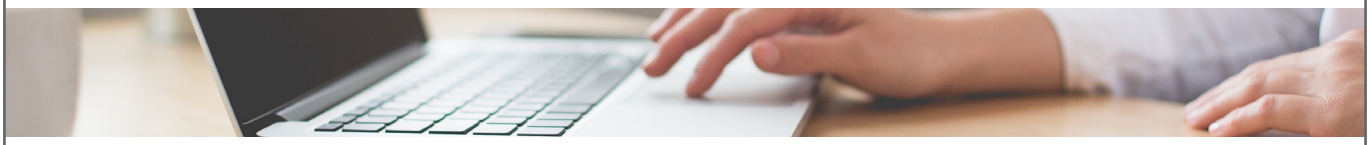

ADAMS HENDRY CONSULTING LIMITED DATA PROTECTION POLICY

Introduction

1. This policy sets out how Adams Hendry Consulting Ltd (AHCL) processes the personal data of data subjects. It applies to all personal data that AHCL process, regardless of the media on which those personal data are stored. AHCL is committed to being clear and transparent about how it collects and uses personal data and to complying with its data protection obligations. Protecting the confidentiality, security and integrity of the personal data it processes is also of paramount importance to business operations. AHCL will process personal data in accordance with this policy, the data protection legislation and the latest applicable privacy notice which has been issued.

2. This policy is non-contractual and does not form part of any employment contract, casual worker agreement, consultancy agreement or any other contract for services.

3. AHCL members of staff – who themselves are data subjects - must always comply with this policy when processing personal data on AHCL's behalf in the proper performance of job duties and responsibilities. The purpose of this policy is to set out what AHCL expects from its staff and to ensure that they understand and comply with the rules governing the processing of personal data to which they may have access in the course of their work, so as to ensure that neither AHCL nor individual members of staff breach the data protection legislation.

4. AHCL takes compliance with this policy very seriously. Any breach of this policy or any breach of the data protection legislation will be regarded as misconduct and will be dealt with under the appropriate disciplinary procedure. A significant or deliberate breach of this policy, such as accessing a data subject's personal data without authority or unlawfully obtaining or disclosing a data subject's personal data (or procuring their disclosure to a third party) without AHCL's consent, constitutes a gross misconduct offence and could lead to summary dismissal.

5. The Board of AHCL has overall responsibility for data protection compliance and should be contacted if there are any questions about the operation of this policy, if further information is required about data protection legislation, data protection matters generally or if there are any concerns that this policy is not being or has not been followed. The Director in charge of data protection is: Philip Rowell p.rowell@adamshendry.co.uk, tel: 01962 877414 – Adams Hendry Consulting Limited.

The data protection principles

6. Under the data protection legislation, there are six data protection principles that AHCL and all members of staff must comply with at all times in their personal data processing activities. In brief, personal data must be:

i. Processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency).

ii. Collected only for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation).

iii. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

iv. Accurate and, where necessary, kept up to date - every reasonable step must also be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy).

v. Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed (storage limitation).

vi. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

Lawfulness, fairness and transparency

7. Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. This principle means that both AHCL and members of staff may only collect, process and share personal data lawfully and fairly and for specific purposes.

Lawfulness and fairness

8. Processing is only lawful in certain circumstances. These include where:

- the data subject has given consent to the processing of their personal data for one or more specific purposes;

- the processing is necessary for the performance of a contract with the data subject, e.g. an employment contract, or in order to take steps at the request of the data subject prior to entering into a contract;

- the processing is necessary for compliance with AHCL's legal obligations;

- the processing is necessary to protect the data subject's vital interests (or someone else's vital interests);

- the processing is necessary to pursue AHCL's legitimate interests as a private business (or those of a third party), where the data subject's interests or fundamental rights and freedoms do not override AHCL's interests; the purposes for which we process personal data for legitimate interests must also be set out in an appropriate privacy notice

9. AHCL and its staff must only process personal data on the basis of one or more of these lawful bases. Before a processing activity starts for the first time, and then regularly while it continues, AHCL will review the purpose of the processing activity, select the most appropriate lawful basis (or bases) for that processing and satisfy ourselves that the processing is necessary for the purpose of that lawful basis (or bases). When determining whether the AHCL's legitimate interests are the only or most appropriate basis for lawful processing, we will record this basis and keep it under review.

10. Where consent is the lawful basis relied upon (which is not envisaged to be very often, if at all), this requires the data subject to have given a positive statement, active opt-in or clear affirmative action. In addition, consent must specifically cover the purposes of the processing and the types of processing activity, so separate consents for different types of processing must be obtained, where appropriate. Data subjects also have the right to withdraw their consent to processing at any time, they must be advised of this right and it must be as easy for them to withdraw their consent as it was to give it.

11. Legislation also provides that the processing of special categories of personal data and criminal records personal data is only lawful in more

limited circumstances where a special condition for processing - set out in Article 9 of the GDPR - also applies (this is an additional requirement; the processing must still meet one or more of the conditions for processing set out above).

12. AHCL may need to process special categories of personal data and criminal records personal data. AHCL and its members of staff must only process special categories of personal data and criminal records personal data where there is also one or more of these special lawful bases for processing. Before processing any special categories of personal data and criminal records personal data, staff must notify the Director in charge of data protection so that they may assess whether the processing complies with one or more of these special conditions.

13. A clear record must be kept of all consents, including explicit consents, which covers what the data subject has consented to, what they were told at the time and how and when consent was given. This enables AHCL to demonstrate compliance with the data protection requirements for consent.

Transparency

14. The transparency principle requires AHCL to provide specific information to data subjects through appropriate privacy notices. These must be concise, transparent, intelligible, easily accessible and use clear and plain language. The information to be included in a privacy notice includes that set out in Article 13 of the Regulations.

15. AHCL will issue a privacy notice when it first collects a data subject's personal data from them. If the personal data have been obtained from third parties, we will provide the privacy notice information within a reasonable period of having obtained the personal data and no later than one month. However, if the personal data are to be used to communicate with the data subject, the privacy notice information is to be provided when the first communication takes place. If disclosure of the personal data to another recipient is envisaged, the notice is to be provided, at the latest, when the data are first disclosed. Members of staff must comply with these rules on privacy notices when processing personal data on AHCL's behalf in the proper performance of job duties and responsibilities.

16. Privacy notices will be available on AHCL's website, and it is envisaged that the issuing of privacy notices as outlined above will be via a link to the AHCL webpage provided within email footers, on letter heads, or within terms of business. Hard copies of the privacy notices will also be available in AHCL's meeting room.

17. AHCL will also issue privacy notices to members of staff from time to time. Privacy notices can also be obtained from the Director in charge of data protection.

Purpose limitation

18. Personal data must be collected only for specified, explicit and legitimate purposes and they must not be further processed in any manner that is incompatible with those purposes.

19. Personal data cannot be used for new, different or incompatible purposes from those disclosed to the data subject when they were first obtained, for example in an appropriate privacy notice, unless the data subject has been informed of the new purposes and the terms of this policy are otherwise complied with, e.g. there is a lawful basis for processing. This also includes special categories of personal data and criminal records personal data.

Data minimisation

20. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

21. AHCL will only collect personal data to the extent that they are required for the specific purposes notified to the data subject. AHCL staff must only process personal data where job duties and responsibilities require it and must not process personal data for any reason which is unrelated to your job duties and responsibilities. In addition, staff must ensure that any personal data collected are adequate and relevant for the intended purposes and are not excessive.

22. When personal data are no longer needed for specified purposes, members of staff must ensure

that they are destroyed, erased or anonymised in accordance with AHCL's rules on data retention and destruction set out in subsequent paragraphs.

Accuracy

23. Personal data must be accurate and, where necessary, kept up to date. In addition, every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

24. It is important that the personal data AHCL holds about its members of staff is accurate and up to date. Members of staff must keep AHCL informed if personal data changes, e.g. you change your home address, so that records can be updated.

25. Staff must also ensure as far as they are able that the personal data held about other data subjects is accurate and up to date where this is part of job duties or responsibilities. The accuracy of any personal data must be checked at the point of their collection and at regular intervals thereafter. All reasonable steps must be taken to destroy, erase or update outdated personal data and to correct inaccurate personal data.

Storage limitation

26. Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data are processed.

27. AHCL will only retain personal data for as long as is necessary to fulfil the legitimate business purposes for which they were originally collected and processed. AHCL's rules on data retention and destruction set out below, must be complied with.

Retention: job applicants

28. If a job applicant's application for employment is unsuccessful, AHCL will generally hold their personal data, including special categories of personal data and criminal records personal data, for up to one year after the end of the relevant recruitment exercise but this is subject to: (a) any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and (b) the retention of some types of personal data for up to seven years to protect against legal risk, e.g. if they could be relevant to a possible legal claim in a tribunal, County Court or High Court.

29. If the job applicant has consented to AHCL keeping their personal data on file in case there are future suitable employment opportunities, it will hold their personal data for a further one year after the end of the relevant recruitment exercise, or until consent is withdrawn.

Retention: Members of staff

30. AHCL will generally hold personal data, including, as necessary, special categories of personal data and criminal records personal data, for the duration of a member of staff's employment or engagement. The exceptions are:

- any personal data supplied as part of the recruitment process will not be retained if they have no bearing on the ongoing working relationship;
- criminal records personal data (if collected) collected in the course of the recruitment process will be deleted once they have been verified through a DBS criminal record check, unless, in exceptional circumstances, the information has been assessed by AHCL as relevant to the ongoing working relationship;
- it will only be recorded whether a DBS criminal record check has yielded a satisfactory or unsatisfactory result, unless, in exceptional circumstances, the information in the criminal record check has been assessed by AHCL as relevant to the ongoing working relationship;
- if it has been assessed as relevant to the ongoing working relationship, a DBS criminal record check will nevertheless be deleted after six months or once the conviction is "spent" if earlier (unless information about spent convictions may be retained because the role is an excluded occupation or profession), and
- disciplinary, grievance and capability records will only be retained until the expiry of any

warning given (but a summary disciplinary, grievance or performance management record will still be maintained for the duration of employment).

31. Once a member of staff has left employment or their engagement has been terminated, AHCL will generally hold their personal data, including special categories of personal data and criminal records personal data, for one year after the termination of their employment or engagement, but this is subject to: (a) any minimum statutory or other legal, tax, health and safety, reporting or accounting requirements for particular data or records, and (b) the retention of some types of personal data for up to seven years to protect against legal risk, e.g. if they could be relevant to a possible legal claim in a tribunal, County Court or High Court. AHCL will hold payroll, wage and tax records (including salary, bonuses, overtime, expenses, benefits and pension information, National Insurance number, PAYE records, tax code and tax status information) for up to seven years after the termination of their employment or engagement.

32. Overall, this means that we will "thin" the file of personal data that we hold on members of staff one year after the termination of their employment or engagement, so that we only continue to retain for a longer period what is strictly necessary.

Retention: other third parties, including clients, advisors and suppliers

33. AHCL will generally hold personal data belonging to clients, advisors, suppliers and external bodies. Personal data of members of the public – provided to AHCL during 'planning consultations' – may also be held.

34. Once our business relationship with the relevant party has been terminated, we will generally hold personal data for ten years after the termination of the relationship. This timeframe takes account of the requirements of Town Planning and related law, as well as other legal obligations under which AHCL operates.

Destruction and erasure

35. All personal data must be reviewed before destruction or erasure to determine whether there are special factors that mean destruction or erasure should be delayed. Otherwise, they must be destroyed or erased at the end of the retention periods outlined above. If staff are responsible for maintaining personal data and are not clear what retention period should apply to a particular record, please contact the Director in charge of data protection for guidance.

36. Personal data which are no longer to be retained will be permanently erased from our IT systems or securely and effectively destroyed and we will also require third parties to destroy or erase such personal data where applicable. Staff must take all reasonable steps to destroy or erase personal data that is no longer required.

37. In some circumstances we may anonymise personal data so that they no longer permit a data subject's identification. In this case, we may retain such personal data for a longer period.

Integrity and confidentiality

38. Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

39. AHCL takes the security of personal data seriously and has implemented and maintains safeguards which are appropriate to the size and scope of our business, the amount of personal data that we hold and any identified risks. Steps have also been taken to ensure the ongoing confidentiality, integrity, availability and resilience of our processing systems and services and to ensure that, in the event of a physical or technical incident, availability and access to personal data can be restored in a timely manner. AHCL tests and evaluates the effectiveness of its technical and organisational safeguards to ensure the security of our processing activities.

40. In turn, staff are responsible for protecting the personal data that AHCL holds, and staff must implement reasonable and appropriate security measures against unauthorised or unlawful processing of personal data and against their accidental loss, destruction or damage. Staff must be particularly careful in protecting special categories of personal data and criminal records personal data. Staff must follow all procedures, and comply with all technologies and safeguards, that are put in place to maintain the security of personal data from the point of collection to the point of destruction.

41. Where AHCL uses third-party service providers to process personal data on our behalf, sufficient security arrangements will be implemented in contractual arrangements with those third parties to safeguard the security of personal data. AHCL staff can only share personal data with third-party service providers if authorised to do so and provided that certain safeguards and contractual arrangements have been put in place, including that:

- the third party has a business need to know the personal data for the purposes of providing the contracted services;
- sharing the personal data complies with the privacy notice that has been provided to the data subject (and, if required, the data subject's consent has been obtained);
- the third party and has put adequate measures in place in ensure the security of processing;
- the third party only acts on our documented written instructions;
- a written contract is in place between AHCL and the third party that contains specific approved terms;
- the third party will assist AHCL in allowing data subjects to exercise their rights in relation to data protection and in meeting our obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the third party will delete or return all personal data to AHCL at the end of the contract; and
- the third party will submit to audits.

42. Before any new agreement involving the processing of personal data by a third-party service provider is entered into, or an existing contract is amended, the approval of its terms from a Director must be obtained.

43. Staff may only share personal data with other members of staff if they have a business need to know in order to properly perform their job duties and responsibilities.

44. Hard copy personnel files are confidential and must be stored in locked cabinets. Only authorised members of staff, who have a business need to know in order to properly perform their job duties and responsibilities, have access to these files. Files will not be removed from their normal place of storage without good reason. Personal data stored on removable storage media must be kept locked away within an AHCL office when not in use by authorised members of staff. Personal data held in electronic format will be stored confidentially by means of password protection, encryption or pseudonymisation, and again only authorised members of staff have access to those data.

45. Hard copy data must be stored in project files retained within the AHCL office (which has restricted access and which is alarmed and monitored). Verbal approval for the removal of project files from the office – for instance for home working or attendance at meetings – must be secured in advance of the file being removed from the office. Staff are responsible for ensuring the security of such files when they are away from the office.

46. AHCL has network backup procedures in place to ensure that personal data held in electronic format cannot be accidentally lost, destroyed or damaged. Personal data other than that found in emails or project documents, must not be stored on local computer drives or on personal devices. Personal data must not be stored on portable USB or external hard drives.

47. The data protection legislation requires AHCL to notify any relevant personal data breach to the Information Commissioner's Office within 72 hours of becoming aware of the breach and, where there is a high risk to the rights and freedoms of data subjects, to the data subject themselves. AHCL has procedures

in place to deal with any suspected personal data breach and staff are required to comply with these. If you know or suspect that a personal data breach has occurred, you must immediately contact the Director in charge of data protection – or appointed representative, retain any evidence in relation to the breach and follow AHCL's data breach policy and response plan.

Accountability

48. AHCL is responsible for, and must be able to demonstrate compliance with, the data protection principles. This means that it must implement appropriate and effective technical and organisational measures to ensure compliance and also require staff to fully assist and co-operate with it in this regard. In particular, AHCL has:

- appointed a Director in charge of data protection to be responsible for data protection compliance and privacy matters within the business;
- keeps and regularly reviews written records of personal data processing activities;
- implements a privacy by design approach when processing personal data;
- integrated data protection requirements into our internal documents other related policies and privacy notices;
- introduced training for all members of staff on the data protection legislation and on their data protection duties and responsibilities;
- introduced regular reviews of privacy measures, policies, procedures and contracts and regular testing of our systems and processes to monitor and assess our ongoing compliance with the data protection legislation and the terms of this policy in areas such as security, retention and data sharing.

Privacy by design and data protection impact assessments

49. AHCL implement privacy by design measures when processing personal data by implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the data protection legislation. Staff must assess what privacy measures can be implemented on all processes or systems that process personal data where this is part of their job duties or responsibilities.

50. Where a new business activity or process is considered likely to result in a high risk to the rights and freedoms of data subjects, AHCL will seek to undertake a Data Protection Impact Assessment (DPIA) of that new activity or process.

51. A DPIA will comprise a review of the new activity or process and it must contain a description of the processing operations and the purposes, an assessment of the necessity and proportionality of the processing in relation to those purposes, an assessment of the risks to individuals and the measures in place to address or mitigate those risks and demonstrate compliance.

Automated processing and automated decision-making

52. Automated processing is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, and automated decision-making occurs when an electronic system uses an individual's personal data to make a decision without human intervention. The Company does not carry out any automated processing and does not take any decisions based solely on automated decision-making, including profiling.]

Direct marketing

53. AHCL is subject to certain rules when directly marketing to our clients and customers. Before undertaking any such activity, staff must discuss matters with the Director in charge of data protection and follow any guidelines provided.

Transferring personal data outside the European Economic Area

54. The data protection legislation restricts transfers of personal data to countries outside the European Economic Area (EEA) in order to ensure that the level of data protection afforded to data subjects is maintained. The Company does not

transfer personal data to countries outside the EEA and you must ensure that you comply with this rule.

Data subject rights to access personal data

55. Data subjects have the right, on request, to obtain a copy of the personal data that AHCL holds about them by making a written data subject access request (DSAR). This allows the data subject to check that AHCL are lawfully processing their personal data. The data subject has the right to obtain:

- confirmation as to whether or not their personal data are being processed;
- access to copies of their specified personal data; and
- other additional information.

56. The other additional information (which should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language) are detailed in Article 15 of the GDPR.

57. When a data subject makes a DSAR, AHCL will log the date on which the request was received and confirm their identity. Where there are reasonable doubts concerning the data subject's identity, we will request them to provide such additional information necessary to confirm their identity before complying with their DSAR. AHCL will then search databases, systems and other places where the personal data which are the subject of the DSAR may be held. Where AHCL process a large quantity of personal data about a data subject, we may ask them to first specify the information that their DSAR relates to.

58. If the data subject makes their DSAR electronically, AHCL must provide a copy of the personal data in a commonly used electronic format, unless they specifically request otherwise. If the data subject wants additional copies of the personal data, the Company will charge a reasonable fee, which is based on our administrative costs of providing the additional copies.

59. AHCL will normally respond to a DSAR and provide copies of the personal data within one month of the date of receipt of the request. However, it may extend this time limit for responding if the request is complex or there are a number of requests made by the data subject. If AHCL intend to extend the time limit, it will contact the data subject within one month of the DSAR's receipt to inform them of the extension and to explain why it is necessary.

60. Before providing the personal data to the data subject making the DSAR, AHCL will review the personal data requested to see if they contain the personal data of other data subjects. If they do, AHCL may redact the personal data of those other data subjects prior to providing the data subject with their personal data. AHCL will also check whether there are any statutory exemptions from disclosure that apply to the personal data that are the subject of the DSAR. If a statutory exemption applies to any of the personal data, those personal data may not be disclosed.

61. Whilst AHCL will normally provide a copy of the personal data in response to a DSAR free of charge, it reserves the right to charge a reasonable fee, based on our administrative costs of providing the personal data, when a DSAR is manifestly unfounded or excessive, particularly if it repeats a DSAR to which AHCL have already responded. Alternatively, where a DSAR is manifestly unfounded or excessive, we reserve the right to refuse to respond altogether. Where AHCL refuse to act on a request in this way, it will set out its written reasons why to the data subject within one month of receipt of their DSAR. AHCL will also inform them of their right to complain to the Information Commissioner's Office or to seek a judicial remedy in the courts.

62. If a data subject wishes to exercise its data subject access rights, please put the request in an e-mail, and send it to our Director in charge of data protection as follows: Philip Rowell, p.rowell@adamshendry.co.uk – tel: 01962 877414. AHCL will inform you if it needs to further verify your identity.

63. If staff receive a DSAR from another data subject, it must immediately be forwarded to our Director in charge of data protection and they will deal with responding to it.

Other data subject rights in relation to their personal data

64. Data subjects have a number of other rights in relation to their personal data. When AHCL process data subjects' personal data, it will respect those rights. It is AHCL's policy to ensure that requests by data subjects to exercise their rights in respect of their personal data are handled in accordance with the data protection legislation.

65. Subject to certain conditions, and in certain circumstances, data subjects have the right to:

- be informed;
- request rectification of their personal data;
- request the erasure of their personal data;
- restrict the processing of their personal data;
- object to the processing of their personal data;
- data portability;
- not be subject to automated decision-making, including profiling;
- prevent direct marketing; and
- be notified of a data breach which is likely to result in a high risk to their rights and freedoms.

66. If a data subject invokes any of these rights the following response procedures will be applied as appropriate and applicable:

- requests to rectify personal data - unless there is an applicable exemption, AHCL will rectify the personal data without undue delay and we will also communicate the rectification of the personal data to each recipient to whom the personal data have been disclosed unless this is impossible or involves disproportionate effort;
- requests for the erasure of personal data - AHCL will erase the personal data without undue delay provided one of the grounds set out in the data protection legislation applies and there is no applicable exemption (and, where the personal data are to be erased, a similar timetable and procedure to that applying to responding to DSARs will be followed). AHCL will also communicate the erasure of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort. Where AHCL has made the personal data public, it will take reasonable steps to inform those who are processing the personal data that the data subject has requested the erasure by them of any links to, or copies or replications of, those personal data
- requests to restrict the processing of personal data - where processing has been restricted in accordance with the grounds set out in the data protection legislation, AHCL will only process the personal data (excluding storing them) with the data subject's consent, for the establishment, exercise or defence of legal claims, for the protection of the rights of another person, or for reasons of important public interest. Prior to lifting the restriction, we will inform the data subject that it is to be lifted. AHCL will also communicate the restriction of processing of the personal data to each recipient to whom the personal data have been disclosed, unless this is impossible or involves disproportionate effort
- response to objections to the processing of personal data - where such an objection is made in accordance with the data protection legislation and there is no applicable exemption, we will no longer process the data subject's personal data unless we can show compelling legitimate grounds for the processing which overrides the data subject's interests, rights and freedoms or we are processing the personal data for the establishment, exercise or defence of legal claims.
- response to requests for data portability - unless there is an applicable exemption, we will provide the personal data without undue delay if the lawful basis for the processing of the personal data is consent or pursuant to a contract and our processing of those data is carried out by automated means (and a similar timetable and procedure to that applying to responding to DSARs will be followed)

67. If data subjects wish to make any of the above requests staff should contact the Director in charge of data protection.

Obligations in relation to personal data

68. AHCL staff must comply with this policy and the data protection principles at all times in any personal data processing activities undertaken on behalf of the Company and in the proper performance of job duties and responsibilities.

69. AHCL staff are aware that they are personally accountable for their actions and can be held criminally liable. It is a criminal offence to (i) knowingly or recklessly obtain or disclose personal data (or to procure their disclosure to a third party) without the consent of AHCL (ii) knowingly or recklessly re-identify personal data that has been anonymised without the consent of AHCL, where it has de-identified the personal data, and (iii) to alter, block, erase, destroy or conceal personal data with the intention of preventing their disclosure to a data subject following a data subject access request. Where unlawful activity is suspected, AHCL will take appropriate steps. Such conduct would also amount to a gross misconduct offence under AHCL's disciplinary procedure and could lead to summary dismissal.

70. AHCL staff must also comply with the following guidelines at all times:

- only access personal data that they have authority to access and only for authorised purposes, e.g. if you need them for the work you do for AHCL, and then only use the data for the specified lawful purpose for which they were obtained
- only allow other members of staff to access personal data if they have the appropriate authorisation and never share personal data informally
- do not disclose personal data to anyone except the data subject. In particular, they should not be given to someone from the same family, passed to any other unauthorised third party, placed on the Company's website or posted on the Internet in any form. unless the data subject has given their explicit consent to this
- be aware that those seeking personal data sometimes use deception to gain access to them, so always verify the identity of the data subject and the legitimacy of the request
- where AHCL provides passwords to be used before releasing personal data, you must strictly follow AHCL's requirements in this regard
- only transmit personal data between locations if the method of transfer is secure
- if you receive a request for personal data about another member of staff or data subject, you should forward this to Director in charge of data protection
- ensure any personal data you hold are kept securely, either within the office or for justifiable reasons taken out of the office if in hard copy, or password protected or encrypted if in electronic format, and comply with AHCL's rules on computer access and secure file storage
- do not access another member of staff's personal data, e.g. their personnel records, without authority as this will be treated as gross misconduct and it is a criminal offence
- do not obtain or disclose personal data (or procure their disclosure to a third party) without authority or without AHCL's consent as this will be treated as gross misconduct and it is a criminal offence
- do not remove personal data, or devices containing personal data, from the workplace with the intention of processing them elsewhere unless this is necessary to enable you to properly carry out your job duties and responsibilities, you have adopted appropriate security measures (such as password protection, encryption or pseudonymisation) to secure the data and the device and it has been authorised by your project manager
- ensure that, when working on personal data as part of your job duties and responsibilities when away from your workplace and with the authorisation of your project manager, you continue to observe the terms of this policy and the data protection legislation, in particular in matters of data security
- do not store personal data on local computer drives, your own personal computer or on other personal devices
- do not make unnecessary copies of personal data and keep and dispose of any copies

securely, e.g. by disposing within the confidential waste
- ensure that you attend all mandatory data protection training
- refer any questions that you may have about the data protection legislation or compliance with this policy to the Director in charge of data protection
- remember that compliance with the data protection legislation and the terms of this policy is your personal responsibility.

Changes to this policy

71. The Company will review this policy at regular intervals and we reserve the right to update or amend it at any time and from time to time. We will circulate any modified policy to members of staff and, where appropriate, we may notify you of changes by e-mail.

72. It is intended that this policy is fully compliant with the data protection legislation. However, if any conflict arises between the data protection legislation and this policy, AHCL will comply with the data protection legislation.

73. This policy may also be made available to the Information Commissioner's Office on request.

Adams Hendry Consulting Ltd
22 May 2018

Definitions

In this policy, the following words and phrases have the following meanings:

"Consent" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them.

"Criminal records personal data" means personal data relating to criminal convictions and offences and personal data relating to criminal allegations and proceedings.

"Data protection legislation" means the EU General Data Protection Regulation (GDPR), the Data Protection Act 2018 and any other applicable primary or secondary legislation as may be in force in the UK from time to time.

"Data subject" means a living identified or identifiable individual about whom the Company holds personal data.

"Members of staff" is any director, employee, worker, agency worker, apprentice, intern, volunteer, contractor and consultant employed or engaged by the Company.

"Personal data" is any information relating to a data subject who can be identified (directly or indirectly) either from those data alone or by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that data subject. It excludes anonymised data, i.e. where all identifying particulars have been removed.

"Processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disclosing, disseminating, restricting, erasing or destroying. It also includes transmitting or transferring personal data to third parties.

"Special categories of personal data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data, data concerning the physical or mental health of a data subject or data concerning a data subject's sex life or sexual orientation.