UK GENERAL DATA PROTECTION REGULATION

DATA PROTECTION POLICY

AMENDMENT HISTORY

Date	New Issue No.	Details of Amendment
Feb 2021	1	Draft Policy for Staff Consultation
June 2021	2	Final Policy Document

1. Policy Statement

1.1 Everyone has rights with regard to the way in which their Personal Data is handled. During the course of our activities we will collect, store and process Personal Data about our users, clients, contractors, tenderers, advisors, employees, suppliers and other third parties. Data users are obliged to comply with this policy when processing Personal Data. Breach of this policy may result in disciplinary action.

1.2 This Data Protection Policy applies to all ARC21 personnel. You must read and understand and comply with this Data Protection Policy when processing Personal Data on our behalf and attend training when required. Related policies are available to help you interpret and act in accordance with this Data Protection Policy. You must also comply with all such related policies.

1.3 Please contact the Data Protection Officer (DPO) with any questions about the operation of this policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed

2. About this Policy

2.1 The types of Personal Data that ARC21 may be required to handle include information about current, past and prospective tenderers and subcontractors, advisors, suppliers, employees and others that we communicate with. The Personal Data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 and 2018 (the Acts), the General Data Protection Regulations (GDPR), UK General Data Protection Regulations (UKGDPR) and other regulations. Following the UK's exit from the EU this policy reflects data protection legislation from 1 January 2021 and is tailored to comply with the retained EU law version of the General Data Protection Regulation (EU 2016/679) (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

2.2 This policy and any other documents referred to in it sets out the basis on which we will process any Personal Data we collect from Data Subjects, or that is provided to us by Data Subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

3. Definition of Data Protection Terms – See Appendix 1

4. Data Protection Principles

4.1 Anyone processing Personal Data must comply with the principles of good practice which provide that Personal Data must be:

a) Processed fairly, transparently and lawfully.

b) Processed for specified, limited purposes and in an appropriate way (Purpose Limitation).

c) Adequate, relevant and not excessive for the purpose (Data Minimisation).

d) Accurate and where necessary kept up to date.

e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed.

f) Processed in line with Data Subjects' rights.

g) Secure (using appropriate technical and organisational measures to avoid loss, destruction or damage).

h) Not transferred to people or organisations situated in countries without adequate protection (Transfer Limitation).

4.2 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

4.2 Article 5 of the UK GDPR (applicable since 1 January 2021) contains principles which controllers and processors must comply with when processing Personal Data – lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation, integrity; confidentiality and accountability.

5. Fair and Lawful Processing

5.1 Data protection laws are 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. For Personal Data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Acts/UK GDPR. These include, among other things, the Data Subject's consent to the processing, or that the processing is necessary for the performance of a contract with the Data Subject, for compliance with a legal obligation to which the Data Controller is subject, for the purposes of performing a public task, to protect the Data Subject's vital interests or for the legitimate interest of the Data Controller where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

5.2 When sensitive Personal Data is being processed, additional conditions must be met.

5.3 It is necessary to identify and document the legal ground being relied on for each Processing activity.

6. Consent

6.1 As set out above, a Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent. A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

6.2 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

6.3 Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Categories of Personal Data and Criminal Convictions Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Special Categories of Personal Data and Criminal Convictions Data. Where Explicit Consent is required, we must issue a Privacy Notice to the Data Subject to capture Explicit Consent.

6.4 We will need to evidence Consent captured and keep records of all Consents in accordance with related policies so that ARC21 can demonstrate compliance with Consent requirements.

7. Processing for Limited Purposes

7.1 In the course of our activities, we may collect and process the Personal Data set out in our Data Retention Policy Schedule. This may include data we receive directly from a Data Subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, other public sector bodies, business partners, tenderers, contractors and sub-contractors, advisors, suppliers, payment and delivery services and others).

7.2 We will only process Personal Data for the specific purposes set out in the Data Retention Policy Schedule or for any other purposes specifically permitted by the data protection legislation.

8. Notifying Data Subjects

8.1 The UK GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

8.2 Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the UK GDPR including the identity of the Controller and DPO, how and why we will use, process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

8.3 When Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the UK GDPR as soon as possible after collecting/receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the UK GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

8.4 If we collect Personal Data directly from Data Subjects, we will inform them about:

a) The purpose or purposes for which we intend to process that Personal Data.

b) The types of third parties, if any, with which we will share or to which we will disclose that Personal Data.

c) The means, if any, with which Data Subjects can limit our use and disclosure of their Personal Data.

8.5 If we receive Personal Data about a Data Subject from other sources, we will provide the Data Subject with this information as soon as possible thereafter.

8.6 We will also inform Data Subjects whose Personal Data we process that we are the data controller with regard to that data.

9. Purpose Limitation

9.1 Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

9.2 We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

9.3 We will only collect Personal Data to the extent that it is required for the specific purpose notified to the Data Subject or as required by law.

10. Data minimisation

10.1 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

10.2 Staff may only collect Personal Data that is required for their job duties and should not collect excessive data or Process Personal Data for any reason unrelated to the duties of the job. Staff also need to ensure that any Personal Data collected is adequate and relevant for the intended purposes.

10.3 Staff must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Data Retention Schedule.

11. Accurate Data

11.1 We will ensure that Personal Data we hold is accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

12. Timely Processing

12.1 A Data retention Policy will be maintained to ensure that Personal Data is deleted after a reasonable time unless a law requires that data to be kept for a specified period.

12.2 We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required in accordance with the Data Retention Policy. This includes requiring third parties to delete Personal Data where applicable.

13. Processing in Line with Data Subject's Rights

13.1 ARC21 will process all Personal Data in line with Data Subjects' rights, in particular their right to:

a) Request access to any data held about them by a Data Controller.

b) Prevent the processing of their data for direct-marketing purposes.

c) Ask to have data amended, rectified or erased.

d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

e) Restrict processing in specific circumstances and challenge processing which has been justified on the basis of ARC21's legitimate interests or in the public interest.

f) Object to decisions based solely on Automated Processing, including profiling (ADM).

g) In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

h) Be notified of a data protection breach which is likely to result in a high risk to their rights and freedoms.

i) Receive certain information about the Data Controller's Processing activities.

j) Withdraw consent to processing at any time.

k) Make a complaint to the Information Commissioner's Office (ICO).

13.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

14. Employee Data

14.1 ARC21 obtains, collects and processes Personal Data relating to employees in the course of business in a variety of circumstances e.g. recruitment, training, payment, performance reviews, personnel/HR, administrative and general business and management purposes and to protect the legitimate interests of ARC21. Employee/HR data will only be processed for employment related purposes and, in general, will not be disclosed to third parties, except where required or authorised by law or with the agreement of the applicable employee.

14.2 Personal employee/HR data kept by us will normally be stored on the employee's personnel file or HR electronic database. We will seek to ensure that only authorised personnel have access to an employee's personnel file. The employee's line manager or supervisor will have access to certain Personal Data where necessary and in accordance with operational requirements. We will ensure that appropriate security measures are in place to protect against unauthorised access to employee/HR data.

14.3 ARC21 has a legal obligation to keep certain employee and HR related data for a specified period of time and we will ensure to adhere to such statutory requirements, in addition to the principles and requirements of data protection under the applicable legislation, in respect of such employee and HR data.

15. Data Security

15.1 ARC21 will take appropriate security measures against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

15.2 We will put in place procedures and technologies appropriate to our size, administrative resources and identified risks, to maintain the security of all Personal Data from the point of collection to the point of destruction (including the use of encryption and pseudonymisation). Personal Data may be transferred to a Data Processor if that Data Processor agrees to comply with those procedures and policies, or if that Data Processor puts in place adequate measures him/herself.

15.3 We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

a) **Confidentiality** means that only people who are authorised to use the data can access it.

b) **Integrity** means that Personal Data should be accurate and suitable for the purpose for which it is processed.

c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes.

15.4 Security procedures include:

a) **Entry controls**. Any stranger seen in entry-controlled areas should be reported.

b) **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.)

c) **Methods of disposal**. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

d) **Equipment**. Data users must ensure that individual monitors do not show confidential information to passers-by; that password protection and other restrictive measures are put in place and should log off from their PC/electronic devise when it is appropriate to do so.

15.5 You must comply with and not attempt to circumvent the administrative, physical and technical safeguards implemented and maintained by ARC21 in accordance with the Acts/UK GDPR and relevant standards to protect Personal Data.

16. Reporting a Personal Data Breach

16.1 The UK GDPR requires Controllers to notify any Personal Data Breach to the Information Commissioner and, in certain instances the Data Subject. ARC21 has procedures to deal with suspected Personal Data breaches and will notify Data Subjects or any applicable regulator where we are legally required to do so.

16.2 If you know or suspect that a Personal Data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the DPO or designated key point of contact. You should preserve all evidence relating to the potential Personal Data Breach.

17. Transfer Limitation

17.1 The UK GDPR restricts data transfers to countries outside the UK to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. You transfer Personal Data across borders when you transmit, send, view or access that data in or to a different country.

17.2 We do not anticipate having to transfer data outside the UK. However should it become necessary to do so ARC21 will ensure that one of the following conditions applies:

a) The UK has issued regulations confirming that the country to which the Personal Data is transferred ensures an adequate level of protection for the Data Subjects' rights and freedoms.

b) Appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved for use in the UK, an approved code of conduct or certification mechanism.

c) The Data Subject has given his/her explicit consent to the proposed transfer after being informed of any potential risks; or

d) The transfer is necessary for one of the reasons set out in the Acts/UK GDPR, including the performance of a contract between ARC21 and the Data Subject, or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving consent and, in some limited cases, for ARC21's legitimate interest.

e) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

f) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the Data Subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

17.3 You must consult the DPO before transferring Personal Data outside of the UK.

18. Disclosure and Sharing or Personal Information

18.1 ARC21 may share Personal Data we hold with other councils/public bodies.

18.2 ARC21 may also disclose Personal Data we hold to third parties. If ARC21 or substantially all of our assets are transferred to a third party, Personal Data we hold may be transferred to that third party as required by law or by agreement with the constituent councils.

18.3 If we are under a duty to disclose or share a Data Subject's Personal Data in order to comply with any legal obligation, or in order to enforce or apply any contract with the Data Subject or other agreements; or to protect our rights, property, or safety of our employees or others.

18.4 ARC21 may also share Personal Data we hold with selected third parties for the purposes of carrying out our lawful and legitimate business activities.

19. Dealing with Subject Access Requests

19.1 Data Subjects may make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should inform their Line Manager immediately and then forward it to the Corporate Services Director immediately. There are strict deadlines for dealing with such requests.

19.2 When receiving telephone enquiries, ARC21 will only disclose Personal Data we hold on our systems if the following conditions are met:

a) Check the caller's identity to make sure that information is only given to a person who is entitled to it.

b) Suggest that the caller put their request in writing if unsure about the caller's identity and where their identity cannot be checked.

19.3 Refer a request to the Line Manager or Corporate Services Director for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

20. Accountability

20.1 Article 24(1) UKGDPR requires a controller to demonstrate that data processing activities comply with the UK GDPR's requirements. Together, Articles 5(2) and 24 form the 'accountability principle' which is a key element of the UK GDPR.

20.2 ARC21 will implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. ARC21 as Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles. ARC21 must have adequate resources and controls in place to ensure and to document GDPR compliance including:

20.3 Appointing a suitably qualified DPO;

20.4 Implementing Privacy by Design when Processing Personal Data and completing Data Protection Impact Assessments (DPIAs) where Processing presents a high risk to rights and freedoms of Data Subjects;

20.5 Regularly training staff on the UK GDPR, Related Policies and data protection matters including.

20.6 Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

21. Record keeping

21.1 The UK GDPR requires us to keep full and accurate records of all our Data Processing activities. ARC21 will keep and maintain accurate records reflecting our Processing.

21.2 These records should include, at a minimum, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Data Subject's consents and procedures for obtaining consents, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place.

22. Training and audit

22.1 We are required to ensure that staff have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

22.2 All of the systems and processes will be reviewed to ensure they are compliant and that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

23. Privacy by Design and Data Protection Impact Assessment (DPIA)

23.1 ARC21 is required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles. ARC21 must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

a) the state of the art (i.e. most up-to-date developments)

b) the cost of implementation;

c) the nature, scope, context and purposes of Processing; and

d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

e) Data controllers must carry out a screening exercise to assess risk and to determine whether a DPIA is required. DPIA's must be conducted where screening reveals that the proposed Processing is "***likely to result in a high risk to the rights and freedoms of natural persons***" and in particular in respect to high risk Processing involving:

- use of new technologies (programmes, systems or processes), or changing technologies (programmes, systems or processes);
- Automated Processing including profiling and Automated Decision Making (ADM);
- large scale Processing of Special Categories of Personal Data or Criminal Convictions Data; and
- large scale, systematic monitoring of a publicly accessible area.

23.2 You must notify the Corporate Services Director when screening reveals that a DPIA is required. The DPO must be informed before any DPIA is commenced.

24. Personal Data

24.1 Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place. We may only share the Personal Data we hold with another employee, agent or representative of our organisation if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions. We may only share the Personal Data we hold with third parties, such as our service providers if:

a) they have a need to know the information for the purposes of providing the contracted services;

b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained:

c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place; and

d) the transfer complies with any applicable cross border transfer restrictions.

25. Changes to this Policy

25.1 We reserve the right to change this policy at any time. Where appropriate, we will notify Data Subjects of changes within a reasonable time period including by mail or email.

APPENDIX 1

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data Subjects for the purpose of this policy include all living individuals about whom we holds Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their personal information.

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any Personal Data is processed. They are responsible for establishing practices and policies in line with the Acts. We are the data controller of all Personal Data used in our business for our own operational purposes.

Data users are those of our employees whose work involves processing Personal Data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Data Privacy Impact Assessment (DPIA) are tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data processors include any person or organisation that is not a data user that processes Personal Data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include, for example, tenderers, contractors, advisors, suppliers, other councils, public or government bodies, and other organisations or entities which handle Personal Data on ARC21's behalf.

Data Protection Officer (DPO) is the person required to be appointed in specific circumstances under the UK GDPR. As a public body, arc21 is obliged to appoint a DPO in accordance with UK GDPR.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Special Categories of Personal Data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Special categories of Personal Data can only be processed under strict conditions.

UK GDPR: the retained EU law version of the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the UK GDPR.