General Data Protection Regulation Policy

Auditing Solutions is fully committed to protecting both its own and its client's data, and the rights and freedoms of all individuals in relation to the processing of their personal data.

1 Introduction

Auditing Solutions Ltd ("Auditing Solutions") is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of Auditing Solutions employees in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to an Auditing Solutions Contact (i.e. the Data Subject).

Personal Data is any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person. Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data. An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller: Auditing Solutions as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose Auditing Solutions to complaints, regulatory action, fines and/or reputational damage.

Auditing Solutions' management team is fully committed to ensuring continued and effective implementation of this policy and expects all Auditing Solutions Employees to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction. This policy has been approved by Auditing Solutions Managing Director, Stuart Pollard.

2 Scope

This policy has been designed to establish the standard for the Processing and protection of Personal Data by all Auditing Solutions Employees.

This policy applies to all Processing of Personal Data in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals:

- In the context of the business activities of Auditing Solutions; and,
- During the provision of Auditing Services & related Consultancy.

The protection of Personal Data belonging to Auditing Solutions Employee data is not within the scope of this policy. It is covered in the Auditing Solutions 'Data Protection for Employee Data' policy.

3 Definitions

Employee

An individual who works part-time or full-time for Auditing Solutions under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. This includes temporary employees and independent contractors.

Customer

An external organisation with which Auditing Solutions conducts business, that has contracted with Auditing Solutions as a customer, and that has authorised Auditing Solutions to have access to, and process, Personal Data for the purpose of conducting Internal Audits of both Financial data and Corporate Governance.

Personal Data

Any information (including opinions and intentions) which relates to an identified or Identifiable Living Person.

Contact

Any past, current or prospective Auditing Solutions customer.

Identifiable Living Person

Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or one or more factors specific to the physical, economic, cultural or social identity of that living person.

Data Controller

A living person, Public Authority, Agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. In our case, Auditing Solutions.

Data Subject

The identified or Identifiable Living Person to whom the data refers.

Process, Processed, Processing

Any operation or series of operations performed on Personal Data. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or amendment, retrieval, consultation, use, disclosure and/or dissemination, restriction, erasure or destruction.

Data Protection

The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alternation, Processing, transfer or destruction.

Data Protection Authority

The independent public authority responsible for monitoring the application of the Data Protection regulation. Auditing Solutions is registered with the Information Commissioner's Office under registration reference ZA336348.

Data Processor

A person, public authority, agency or other body that processes Personal Data on behalf of the Data Controller.

Consent

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, signifies agreement to the Process of Personal Data relation to them.

Special Categories of Data

This includes data consisting of information pertaining to:

- Race of the data subject;
- Declared ethnicity of the data subject;
- Political opinions of the data subject;
- Religious beliefs of the data subject;
- Professed opinions or personal beliefs of the data subject;
- Membership of a Trades Union or other society;
- Physical and / or mental health or condition of the data subject;
- Sexual lifestyle of the data subject;
- The commission or alleged commission by the data subject of any offence; and
- Any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Auditing Solutions and its employees are likely to have access to sensitive personal data rarely, if at all.

Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data transmitted, stored, or otherwise Processed.

Encryption

The process of converting information or data into code, to prevent unauthorised access.

Anonymisation

Data amended in such a way that no individuals can be identified from the data, whether directly or indirectly, by any means or by any person.

Confidential data

All data given in confidence, or data agreed to be kept confidential between the originator and Auditing Solutions and that is not in the public domain.

Some confidential data will also be personal data and or sensitive personal data and therefore come within the terms of this policy. All Auditing Solutions Employees will handle confidential data regularly as a function of the Auditing process.

4 Governance

Data Protection Officer

To demonstrate our commitment to Data Protection, and to enhance the effectiveness of our compliance efforts, Auditing Solutions has appointed a suitably skilled Data Protection Officer. Reporting to the Managing Director, the Data Protection Officer's duties include:

- Advising Auditing Solutions and its Employees who carry out Processing pursuant to Data Protection regulations;
- Ensuring the alignment of this policy with the General Data Protection Regulation;
- Undertaking Data Protection Impact Assessments (DPIAs);
- Acting as the point of contact for the Information Commissioner's Office;
- Maintaining a system that provides prompt and appropriate responses to Data Subject requests;
- Informing senior managers of any potential corporate, civil and/or criminal penalties which might be levied against Auditing Solutions and/or its Employees for violation of applicable Data Protection Laws; and
- Establishing procedures and standard contractual provisions for obtaining compliance with this policy by any Employee Processing data on behalf of Auditing Solutions.

Policy dissemination and enforcement

Auditing Solutions management team continue to ensure that all Employees responsible for the Processing of Personal Data are aware of, and comply with, the contents of this policy.

Data Protection by design

To ensure that, as far as it is reasonably possible to do so, all Data Protection requirements are identified and addressed when designing new systems or processes and/or when

reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

A Data Protection Impact Assessment (DPIA) is conducted by the Data Protection Officer for all new and/or revised systems or processes. The subsequent findings of the DPIA must then be submitted to the Management team for review and approval. Likewise, IT systems and applications will be subject to continual review and annual impact assessments completed to assess the impact of any new technology uses on the security of Personal Data.

Compliance monitoring

To confirm that an adequate level of compliance is established and maintained by all Auditing Solutions employees, the Data Protection Officer will carry out an annual Data Protection compliance audit which will assess:

- Compliance with Auditing Solutions' Data Protection and Processing policies;
- Compliance with Auditing Solutions' User Account policy; and,
- Compliance with Auditing Solutions' Information Systems Security policy.

An annual training update will be given to all Employees

5 General Data Protection Regulation principles

Anyone Processing Personal Data must comply with the six data protection principles contained in the General Data Protection Regulation 2016 as they define how personal data can be legally processed: in summary these state that personal data shall:

Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and transparently in relation to the Data Subject. This means that other than in the case of data processed under the Local Audit and Accountability Act 2014, Regulation 5, for the purposes of statutory Internal Audits for Councils and Local Authorities, Auditing Solutions must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness) and it must be for the purpose(s) specified in the applicable Data Protection regulation (Lawfulness).

The Local Audit and Accountability Act 2017 - Legal framework

The Local Audit and Accountability Act 2014, Regulation 5, provides auditors with a; "**right of access to all documents and files relating to a Council Audit that are considered necessary by those conducting the audit**." It is not a requirement to seek the personal consent of the individuals whose personal data is contained within documents or data in order to gain access to these for Internal Audit purposes.

Such documents and files include, but are not limited to, Accounting Systems back up files including cashbooks, financial reports, and associated spreadsheets, payroll records and employment contracts. Additionally, records of services provided to clients of the council are also reviewed. These may include allotment lease records, burial and memorial records, market stall fees records, facilities booking receipts, invoices and other similar items.

Auditing Solutions processes 'personal data' for three reasons:

- For the purposes of conducting statutory Internal Audits on behalf of its Council clients: All data processed by Auditing Solutions is anonymised and only used for reporting the Audit findings to the Client;
- To maintain Client relationships, it collects business address, email and telephone contract information, pertaining to Auditing Solutions Clients, Prospective Clients and Business Contacts; and
- To recruit and pay its Employees.

Auditing Solutions has conducted an extensive data impact audit and has categorised each type of data that it stores by risk and has implemented appropriate protocols to ensure the security of that data.

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes. This means that Auditing Solutions must specify exactly what the Personal Data Collected will be used for and limit the Processing of that Personal Data to only what is required to meet the specified Purpose.

Before commencing any Internal Audit, which will involve obtaining and/or processing personal data, the Auditor must give proper consideration to this policy and how it will be properly complied with.

In particular, Auditors must consider the type of personal data which is to be examined and the extent to which such data is legitimately required for the Audit process. All data and the method used for its collection during the Internal Audit process is defined in the current year's Internal Audit Programme and must be recorded using the digital forms provided or by taking the hard or digital copies of documents that are required to support the Internal Audit conclusions.

Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. This means that Auditing Solutions must not Store any Personal Data beyond what is absolutely required.

Personal data obtained or used during the Audit process is limited to the minimum amount of data which is reasonably required to achieve the Internal Audit objectives and all such personal data is anonymised so that data subjects cannot be identified.

Principle 4: Accuracy

Personal Data shall be accurate and current. This means that Auditing Solutions must continue to maintain high quality processes for the identification and management of out-of-date, incorrect and redundant Personal Data.

Principle 5: Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is Processed. All Personal Data Processed for the purposes of conducting Internal Audits for Councils, Local Authorities and such other bodies with whom contracts exist is held in anonymised format, is only retained for the minimum statutory period prescribed by Law after which it is securely deleted or disposed of. Further detail may be located in Auditing Solutions' Document and Data Retention Policy.

Principle 6: Integrity & Confidentiality

Personal Data shall 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. Auditing Solutions continues to use appropriate technical and organisational measures to ensure that the integrity and confidentiality of Personal Data is maintained at all times.

Accountability

The Data Controller: Auditing Solutions, shall be responsible for, and be able to demonstrate compliance with the General Data Protection Regulation. This means that Auditing Solutions must demonstrate that the six Data Protection Principles, detailed above, are met for all Personal Data for which it is responsible.

6 Data Collection

Personal Data should be collected only from the Data Subject unless one of the following applies:

- The nature of the business purpose necessitates the collection of the Personal Data from other persons or bodies.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed of the collection unless one of the following applies:

- The Data Subject has received information by other means;

- The information must remain confidential due to a professional secrecy obligation; and,
- A national law expressly provides for the collection, Processing or transfer of the Personal Data. Auditing Solutions is permitted to collect, Process and transfer data for the purposes of Internal Audit under the Local Audit and Accountability Act 2014, Regulation 5.

Where it has been determined that notification to a Data Subject is required, notification should occur, but in no case later than twenty-eight days.

7 Data Subject Consent

Auditing Solutions will only obtain Personal Data by lawful and fair means, and where appropriate, with the knowledge and Consent of the individual concerned. Where the need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, Auditing Solutions is committed to seeking such Consent.

The Data Protection Officer in cooperation with the Management team, has established a process for obtaining and documenting Data Subject Consent for the Collection, Processing, and/or transfer of their Personal Data. The process includes the provision for:

- Determining what disclosures should be made in order to obtain valid Consent;
- Ensuring that the request for consent is communicated in plain language in an intelligible and easily accessible form;
- Ensuring that Consent is freely given and not based on a conditional clause(s)
- Documenting the date, method and content of the disclosures made and the scope and validity of the Consent(s) given; and
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

Data Subject notification

Auditing Solutions will, when required by applicable law, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their Personal Data.

When the Data Subject is asked to give Consent to the Processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The Data Subject already has the information;
- A legal exemption applies to the requirements for disclosure and/or Consent, such as Auditing Solutions ability to collect, Process and transfer data for the purposes of Internal Audit under the Local Audit and Accountability Act 2014, Regulation 5; and
- The disclosures may be given electronically or in writing.

8 Data processing

Auditing Solutions will only obtain Personal Data by lawful and fair means, and where appropriate with the knowledge and Consent of the individual concerned.

Data Use

Auditing Solutions uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of Auditing Solutions;
- To provide Internal Audit services to Auditing Solutions customers; and
- The ongoing administration and management of customer services.

The use of a Contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a Contact's expectations that their details will be used by Auditing Solutions to respond to a Contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that Auditing Solutions would then provide their details for any other purpose.

Auditing Solutions will Process Personal Data in accordance with the General Data Protection Regulation. More specifically, Auditing Solutions will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes;
- Processing is necessary to undertake an Internal Audit on behalf of an Auditing Solutions customer under the Local Audit and Accountability Act 2014, Regulation 5; and,
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.

In any circumstance where Consent has not been gained for the specific Processing in question, Auditing Solutions will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

- The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation or Pseudonymisation

Personal data in the public domain

Personal data classified as being in the 'public domain' refers to information which will be publicly available world-wide and may be disclosed to third parties without recourse to the data subject.

Auditing Solutions' practice is to make the following items of employee data freely available unless individuals have chosen to opt out.

- Names of directors and employees;
- Employees' workplace email addresses and telephone numbers;
- Employees' biographies and curriculum vitae from time to time;
- Employees names, academic and professional qualifications and memberships where appropriate; and
- Any additional information relating to Employees that they have agreed to be placed in the public domain, such as portrait photographs.

Similarly, as part of its regular business activities and auditing practice, Auditing Solutions may process personal information about third parties that is already in the public domain where such process is carried out in accordance with the Local Audit and Accountability Act 2014 and the General Data Protection Regulation principles set out below and is unlikely to cause any damage or distress to the data subject.

Special Categories of Data

Auditing Solutions does not Process Special Categories of Data (also known as sensitive data) described in section 3 'Definitions', under any circumstances whatsoever.

Data Quality

Auditing Solutions will adopt all necessary measures to ensure the Personal Data that it collects, and Processes, is complete and accurate. The measures adopted by Auditing Solutions to ensure data quality include:

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, misleading or outdated, even where the Data Subject does not request rectification;
- Keeping Personal Data only for the period necessary to satisfy the permitted uses for Internal Audit purposes or applicable statutory retention period; and,
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.

Digital Marketing

Auditing Solutions does not undertake digital marketing, send unsolicited promotional or direct marketing material either electronically or via hard copy.

Data Retention

To ensure fair Processing, Personal Data will not be retained by Auditing Solutions for longer than necessary in relation to the purposes for which it was originally collected, or for which it was Processed.

The length of time for which Auditing Solutions needs to retain Personal Data is set out in the Auditing Solutions Document and Data Retention Policy. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the Policy. All Personal Data will be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

Data Protection

Keeping personal data properly secure is key in complying with the General Data Protection Regulation. All Employees are therefore responsible for ensuring that if they keep any personal data, it is kept securely and is not disclosed, either orally or in writing, intentionally or accidentally to any unauthorised third party.

Auditing Solutions will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be subject.

The minimum set of security measures to be adopted by each Auditing Solutions is provided in the Auditing Solutions **Information Systems Security Policy**. A summary of the Personal Data related security measures is provided below:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are Processed;
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations;
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation;
- Ensure that access logs are in place to establish whether, and by whom, the Personal Data was accessed, modified on or removed from a data processing system;
- Ensure that Personal Data is protected against undesired destruction or loss;
- Ensure that Personal Data collected for different purposes can and is Processed separately; and
- Ensure that Personal Data is not kept longer than necessary.

9 Data Subject Requests

Individuals are entitled to see all information held about themselves, but personal data should only to be disclosed to third parties under specific conditions.

Wherever possible, Auditing Solutions employees will be open with individuals in relation to information held about them. If an individual wants to make a formal Subject Access

Request under the General Data Protection Regulation, they should be referred to the Data Protection Officer.

Data Subject Rights

The Data Subject has the right to:

- object to Processing of their Personal Data;
- lodge a complaint with the Data Protection Authority;
- request rectification or erasure of their Personal Data; and,
- request restriction of Processing of their Personal Data.

All requests received for access to or rectification of Personal Data must be directed to the Data Protection officer, who will log each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require Auditing Solutions to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If Auditing Solutions cannot respond fully to the request within 30 days, the Data Protection Officer shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request;
- Any information located to date;
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision;
- An estimated date by which any remaining responses will be provided; and
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).

Requests from persons representing the Data Subject

Caution will be exercised if employees are requested to disclose information about an individual to someone else, either within or outside Auditing Solutions. Information may be passed on to other members of staff if it is legitimately required for the completion of an employee's Auditing duties, but in all other cases personal data may not be disclosed without the individual's consent. Even parents, spouses, friends, partners or sponsors are not entitled to information without the Data Subject's consent.

There are times when Auditing Solutions may be required to pass personal information about an individual to a third party. Employees in the Human Resources department may

legitimately disclose relevant data to appropriate third parties to meet statutory requirements. The employee dealing with the request will need to be satisfied as to the legitimacy of the enquirer's identity and request.

Auditing Solutions may also receive requests for information from bodies such as the police and HMRC. Any information disclosure will only take place after Auditing Solutions has satisfied itself, to the extent that it is reasonably possible to do so, that any request made is genuine and legitimate.

Disclosing information in an emergency

Personal information can be disclosed in an emergency. In such a situation, if necessary, personal information can be disclosed without consent. For example, if an employee collapses and is unconscious, it would be permissible to inform medical staff that the individual suffers from a medical condition.

No information about an individual will be disclosed to any other enquirers, without written and signed permission from the individual to release their personal data.

Complaints handling

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is both reasonable and proportionate. The Data Protection Officer will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the Data Protection Officer, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Information Commissioner's Office.

Breach Reporting

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Data Protection Officer providing a description of what occurred. Notification of the incident can me made via e-mail dpo@councilaudit.co.uk.

The Data Protection Officer will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Data Protection Officer will report the Personal Data Breach to the Information Commissioner's Office and advise the parties affected.

10 Responsibilities of Employees

All Employees must:

- Be mindful of the fact that individuals have the right to see their 'personal data'. This may include, but is not limited to, applications for employment submitted by prospective Auditors, or comments written about people in e-mails. No comments or other data should be recorded about individuals which the author would not be comfortable in the individual seeing or being informed of;
- Report immediately the loss or theft of any personal data, contained in a printed document, on a mobile device or storage tool such as a controlled memory stick laptop or similar, to the Managing Director and the Data Protection Officer;
- Report immediately to the Managing Director and the Data Protection Officer if they find any lost or discarded data that they believe contains personal data contained in a printed document, on a mobile device or storage tool such as USB stick or laptop or similar;
- Maintain the contents of all personal data which comes into their possession securely and in accordance with Auditing Solutions' written policies;
- Ensure that all personal data that is provided by them, to Auditing Solutions is accurate;
- Notify Auditing Solutions expeditiously of any changes to their own personal data, i.e. change of address or emergency contact details;
- Only ever obtain and or use personal data relating to third parties for approved auditing purposes;
- Ensure that all personal data processed is done so in accordance with the requirements of the General Data Protection Regulation 2016;
- Familiarise themselves with Auditing Solutions' General Data Protection Regulation Policy and comply with it at all times;
- Familiarise themselves with Auditing Solutions' Remote Working & Mobile Computing Policy and IT Security Policy and comply with them at all times; and,
- Seek advice of the Data Protection Officer whenever you are unsure as to how to process personal data or if you have any data protection concerns whatsoever.

Prohibited activities

The following activities are strictly prohibited:

- Using data obtained for one purpose for another supplemental purpose; i.e. using contact details provided for Human Resources purposes for marketing initiatives; and,
- Disclosing personal data to a third party outside of Auditing Solutions without the consent of the data subject.

Implications of breaching this policy

It is a condition of employment in the case of all employees that they will abide by the policies and rules of Auditing Solutions. Any breach of this policy will be considered a disciplinary offence and may lead to disciplinary action, and/or the individual being held liable in law.

11 Conclusion

Compliance with the General Data Protection Regulation (GDPR) EU 2016/679 which comes into force on the 25th May 2018 is the responsibility of all members of Auditing Solutions, and any questions about this policy or concerning data protection matters should be raised with the Data Protection Officer at dpo@councilaudit.co.uk.

Document Control Information

Owner	Claire Lingard
Version Number	Version 1.1
Approval Date	24th May 2018
Approved By	Stuart Pollard
Date of Last review	25th February 2019
Date of Next review	31st March 2020