ADVANCED
BUILDING CONTRACTORS LIMITED

Data Protection Policy

Purpose

Any organisation which collects, stores or processes Personal or Sensitive Data relating to any UK or EU data subject must comply with the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), EU General Data Protection Regulation (EU GDPR) and the Privacy Electronic Communications Regulation 2003 ('PECR'). This policy has been established to lay out how we comply with the requirements of these regulations.

Advanced Building Contractors Ltd has identified Personal Data Breaches, Failing to Uphold Data Subjects Rights and Reputational damage as key Data Protection Risks for our business, our employees and our customers. As such our Risk appetite for material breach of GDPR compliance is Low.

This policy aims to identify and understand the key principles of GDPR and the Rights of Data subjects and support training and awareness across our organisation.

Scope

This policy relates to all processing activities and supporting information systems involving personal or sensitive personal data where Advanced Building Contractors Ltd acts as a controller. This policy includes data held in physical form and stored in a relevant filing system.

This policy should be reviewed by all Employees, Contractors, Third Party Processors, Managers and Directors of Advanced Building Contractors Ltd.

Roles & Responsibilities

Advanced Building Contractors Ltd has overall responsibility for this policy, and for reviewing the effectiveness of actions taken in response to concerns raised in this policy.

The business shall ensure appropriate resources are made available to support the implementation of this policy throughout all in-scope areas.

All those in scope of this policy are responsible for adhering to the requirements herein.

Fraser Cattanach is responsible for monitoring compliance with this policy and shall provide periodic reporting for the organisation on compliance with this policy.

Fraser Cattanach shall be the contact point for all matters relating to the Supervisory Authority (SA)

Fraser Cattanach is responsible for providing or accessing information security support as it relates to this policy.

Those described as owners of this policy are responsible for ensuring their processes, and information systems meet the minimum requirements of all in-scope policies.

The owners of the policies detailed in **Related Policies,** shall ensure requirements are amended to reflect the requirements of this policy.

Related Policies & Procedures

This policy should not be read in isolation. The following policies also include specific and supporting requirements:

- Information Security Policy
- Records Management & Retention Policy & Procedures
- Data Sharing & SAR Policy & Procedures
- Breaches Policy & Procedures

These policies can be found in the central documentation folder located in Microsoft 365 under > Operations > 'Data Protection'.

Definitions and Key Terms

A Glossary of Terms is included under Appendix A of this policy and includes definitions of Data Subjects, Personal Data, Sensitive Personal Data, Controllers and Processors.

Principles

Advanced Building Contractors Ltd are committed to meeting the 7 Principles of GDPR. When handling Personal Data or Sensitive Personal Data, you must adhere to the 7 Principles of GDPR. These state that all Data Must be:

1. Processed Lawfully, Fairly and in a Transparent Manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, Relevant and Limited to what is necessary
4. Accurate and, where necessary, kept up to date
5. Retained only for as long as necessary
6. Processed Securely, in an appropriate manner to maintain security

The 7th Principle of GDPR is **Accountability**, which links all other principles together. We must be accountable for ensuring that our organisation honours all Principles.

As Part of our commitment to meet these principles, we have the following measures in place:

Accountability

Fraser Cattanach has been appointed as owner for all Information Systems containing Personal or Sensitive Data.

System Ownership shall not be assigned to a person who does not have budgetary responsibility for the Information System.

System Ownership shall not be assigned to a person who does not hold Formal Authority over those carrying out processing activity within the Information System.

A system owner may delegate responsibility for operational tasks relating to this policy but shall not delegate accountability

A system owner may seek advice in the discharge of their duties but remains accountable for any subsequent decisions taken (e.g. acceptance of risk).

A record of processing activities is maintained and held by Fraser Cattanach.

Processing activities shall be documented, regularly updated and a process owner appointed.

Process ownership shall not be assigned to a person who does not hold formal authority over those carrying out processing activity within the Information System.

Lawfulness of Processing

Fraser Cattanach shall ensure processing is lawful and document the lawful grounds for processing.

With the exception of some essential storage, processing shall cease immediately where there are no longer lawful grounds for processing.

Transparency

Data Subjects shall be informed of processing activities and provided statutory information at the time data is collected by means of our Privacy Notice

Where data is collected from a source other than the Data Subject, they shall be informed of processing activities and provided with statutory information as soon as practicable but no less than 1 month.

Fraser Cattanach shall regularly review the published Privacy Notice annually for any inaccuracies relating to their processes. The business shall rectify inaccuracies within 5 working days of discovery.

Data Subject Rights

Any Data Subject has the following rights which must be upheld when processing their personal data. A Breach of these rights can result in the maximum fine:

The Rights are:

1. The Right to be Informed
2. The Right of Access
3. The Right to Rectification
4. The Right to Erasure
5. The Right to Restrict Processing
6. The Right to Data Portability
7. The Right to Object
8. Rights in relation to automated decision making and Profiling

Data Protection by Design & Default

Information Systems and Processes shall be designed to comply with the requirements of this policy.

Fraser Cattanach shall implement appropriate technical and organisational measures to ensure that data protection is incorporated into processes and systems by design and default.

Processing activities and supporting Information systems shall be designed to ensure the minimum personal data is stored and for the minimum period necessary.

Fraser Cattanach shall ensure any envisaged new processing systems undergo a Data Protection Impact Analysis (DPIA) which contains at a minimum:

I. A systematic description of the envisaged processing operations and the purposes of the processing
II. An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
III. An assessment of the risks to the rights and freedoms of data subjects
IV. The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this policy, taking into account the rights and legitimate interests of data subjects and other persons concerned.

Fraser Cattanach shall consult with external consultants in relation to the completion of the DPIA

Fraser Cattanach shall, where risk to data subjects is deemed HIGH, consult with the Supervisory Authority.

Fraser Cattanach shall ensure systems are explicitly designed to minimise the impact involved in upholding Data Subjects Rights.

Security of Processing

Fraser Cattanach shall be accountable for ensuring that systems meet the minimum required standards for security, including but not limited to;

I. Identity & Access Management
II. Patch & Vulnerability Management
III. Change Management
IV. Backup & Restoration
V. IT Service Continuity Planning & Testing
VI. Development and Testing Activities
VII. Security Breach Monitoring & Detection

Information Systems, containing Personal or sensitive data, exposed to the Internet or a Third Party, shall be subject to an independent, risk-based penetration test to an agreed scope, no less than annually. Fraser Cattanach shall ensure all issues identified are appropriately treated to commensurate with the organisations risk appetite.

Personal Data Breaches shall be logged, assessed and notified where required immediately upon discovery, but no later than 72 hours after detection / discovery.

Accuracy of Processing

Fraser Cattanach shall ensure data remains accurate and where inaccurate corrected as soon as possible but no later than 5 working days from when the error is reported and verified in accordance with the organisation's Records Management and Retention Policy. All processing shall be suspended from the point of notification until the records have been updated.

Retention

With the exception of data held under statutory exemptions, personal data shall not be retained any longer than necessary and in accordance with the company's record management and retention policy.

Individual Responsible for Data Protection

Fraser Cattanach will be the individual responsible for Data Protection

Fraser Cattanach shall represent the organisation in upholding the rights of Data Subjects as it relates to the organisations processing activities

Fraser Cattanach shall respond to enquiries from Data Subjects in a timely manner.

Fraser Cattanach shall establish and maintain a programme to monitor compliance with this policy.

Fraser Cattanach shall establish and maintain a Data Protection Legislation Training and Awareness Programme.

Fraser Cattanach shall report personal data breaches to the Supervisory Authority no later than 72 hours after the breach has been detected.

Data Subject Access Requests

Fraser Cattanach shall ensure that all of those in scope, understand how to identify a Data Subject Access Request

Data Subject Access Requests shall be recorded in a Register owned by Fraser Cattanach

Data Subject Access Requests shall be completed as soon as possible but no more than 30 calendar days.

Data Subject Access Requests shall not incur a charge

Data Subject Access Requests shall be processed electronically if this is requested by the Data Subject.

Reasonable steps shall be taken to verify the identity of the Data subject and where relevant the third party requesting the information on the Data Subject's behalf prior to providing access to the personal data.

Reasonable Steps shall be made to seek the permission of third parties prior to including their information within an access request. Where permission is not provided, a consultant shall be contacted to determine whether data should be provided or redacted.

Requested information shall be communicated to the Data Subject securely.

Third Party Processing

Processing activities shall not be outsourced to a third party without a binding written agreement that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of Data Subjects and the obligations and rights of this organisation.

Process Owners shall use only third-party processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this policy and ensure protection of the rights of the data subject.

Process and System owners shall review all agreements and where in doubt obtain external advice / recommendations from consultants and representatives from Legal, Procurement, Information Security, Business Continuity prior to signing a contract with a third party Processor and with sufficient time to carry out effective due-diligence on the proposed outsourced process and the third party Processors data protection technical and organisational controls.

ADVANCED
BUILDING CONTRACTORS LIMITED

Personal Data Breach

If any person within the scope of this policy believes that there has been or could be a breach of any Data Protection Regulation in respect of personal data, they should follow the breaches process with immediate effect to assess the severity and adhere to all requirements.

Approvals & Review

This policy was endorsed and approved by Fraser Cattanach on 10th November 2021. The Policy shall apply with effect from and will be enforced from that date.

This policy was reviewed on 5th November 2023 and no changes were identified. The policy shall be reviewed by Fraser Cattanach no later than 4th November 2024.

Version Control:

The current official Copy of this policy shall be located in Microsoft 365 Operations folder under subfolder 'data protection'. If this document was found in any other location, the reader should check and confirm they are reading the current requirements. The following Version information is as follows:

Version No	Description	Date	Author	Reviewed
01	ABC/DPP/001	10th November 2021	All In Business Solutions Ltd	Fraser Cattanach
02	ABC/DPP/002	5th November 2022	All in Business Solutions Ltd	Fraser Cattanach
03	ABC/DPP/002	5th November 2023	All in Business Solutions Ltd	Fraser Cattanach

Policy Owner

The owner of this policy is Fraser Cattanach.

Signature:

Director

Dec 5, 2023

7. Data Protection Policy

Final Audit Report 2023-12-05

Created:	2023-12-05
By:	Joanna Keogh (joanna.keogh@abcltd.net)
Status:	Signed
Transaction ID:	CBJCHBCAABAApSY4GbYr3JWC41wHzM9TQHURcqMTXq85

"7. Data Protection Policy" History

Document created by Joanna Keogh (joanna.keogh@abcltd.net)
2023-12-05 - 12:59:11 PM GMT

Document emailed to Fraser Cattanach (fraser.cattanach@abcltd.net) for signature
2023-12-05 - 1:01:43 PM GMT

Email viewed by Fraser Cattanach (fraser.cattanach@abcltd.net)
2023-12-05 - 5:34:18 PM GMT

Document e-signed by Fraser Cattanach (fraser.cattanach@abcltd.net)
Signature Date: 2023-12-05 - 5:34:33 PM GMT - Time Source: server

Agreement completed.
2023-12-05 - 5:34:33 PM GMT