# Abaco General Data Protection Policy

## 1. Approvals & Review

1.1 This policy was endorsed by Abaco Systems Limited ("Abaco") GDPR Management Committee and approved on behalf of the Abaco Systems Limited Board of Directors ("Board") on 10th May 2018. The policy shall apply from 25th May 2018.

1.2 This Policy shall be reviewed by GDPR Management Committee no later than 1st May 2019.

## 2. Version Control

2.1 The current official issue of this policy shall be located on the Abaco policy portal/s. Users will be advised from time to time where it is located. If this document was found in any location other than that which has been formally notified, the user should check to confirm they are referring to the current issue. The following revision information is provided for reference:

| Issue | Description | Date | Author | Reviewer |
|---|---|---|---|---|
| A | Initial Draft | 01/03/18 | JT | JT |
| B | Final Draft | 24/04//18 | JT | JT |
| 1.0 | Approved for issue | 10/05/18 | JT | GDPR Management Committee |

## 3. Policy Owner

3.1 The Owner of this policy is the Data Protection Officer, the details of whom will be notified to users from time to time.

## 4. Purpose

4.1 An organisation which controls processing activities, involving Personal or Sensitive Data relating to European Union Data Subjects, must comply with the General Data Protection Regulation 2016 ("GDPR") and the Privacy & Electronic Communications Regulation 2003 ("PEER"). This policy sets out the requirements that all those in scope must adhere to.

4.2 This Policy is subject to all the laws, rules and regulations that Abaco is governed by. In the event this policy allows the exercise of discretion, such discretion must be exercised within the confines of the Abaco's statutory obligations and must not contravene any legal, accounting or other regulatory requirements.

## 5. Risk Appetite Statement

5.1 The Boards Risk Appetite for a material breach of GDPR compliance is **LOW.**

5.2 The Board has identified personal data breaches, loss of intellectual property, breach of security requirements, failing to uphold Data Subjects' rights and reputational damage as key data protection risks.

## 6. Glossary of Terms

6.1 A glossary of terms is included in Appendix A to this Policy.

## 7. Scope

7.1 The scope of this policy covers all Processing activities and supporting Information Systems involving Personal or Sensitive Data where Abaco acts as the Controller. This includes Personal or Sensitive data in physical form, stored in a relevant filing system.

7.2 The scope of this policy covers all global geographic territories. For the avoidance of doubt, this includes Third Countries, outside the European Union (EU).

7.3 The scope of this policy covers all Employees, Contractors, Third Parties, Processors, Abaco subsidiaries or other legal persons who process personal or Sensitive Data on behalf of Abaco.

## 8. Requirements

8.1 All processing activities shall be designed to ensure that all data is:

a) Collected for specified, explicit and legitimate purposes only;

b) Accurate and, where necessary, kept up to date;

c) Retained only for as long as necessary;

c) Processed lawfully, fairly and in a transparent manner;

d) Processed securely, in an appropriate manner to maintain security; and

e) Adequate, relevant and limited to only what is necessary to enable the company to operate.

## 9. Data Protection Officer (DPO)

9.1 A Data Protection Officer (DPO) shall be appointed and report directly to the Abaco Board of Directors.

9.2 The DPO shall support Abaco in upholding the rights of Data Subjects as it relates to Abaco's processing activities.

9.3 The DPO shall respond to enquiries from Data Subjects in a timely manner.

9.4 The DPO shall establish and maintain a programme to monitor compliance with this policy.

9.5 The DPO shall establish and maintain a General Data Protection training and awareness programme.

9.6 The DPO shall support compliance with this policy by providing support and advice as it relates to complying with the requirements of this policy.

9.7 The DPO shall be provided timely and appropriate access to information and information systems as it relates to the discharge of their duties.

9.8 Details of the DPO, and their contact details shall be made publicly available.

9.9 The DPO shall maintain the following registers:

i] Register of Processing Activities;

ii] Register of Data Protection Impact Assessments (DPIA);

iii] Register for Data Protection Metrics;

iv] Register for Data Subject Enquiries;

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

## 10 Accountability

10.1 A record of processing activities shall be provided to the Data Protection Officer.

10.2 A System Owner shall be appointed for all Information Systems containing Personal or Sensitive Data. The System Owner shall **not** be from IT unless IT is performing the primary processing activity (e.g. IT operate the Service Desk System and so an IT Manager could be assigned as System Owner).

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

10.4 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.

10.5 A System Owner may delegate responsibility for operational tasks relating to this policy but shall **not** delegate accountability.

10.6 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).

10.7 Processing activities shall be documented and Process Owner/s appointed.

10.8 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.

## 11. Lawfulness of Processing

11.1 Process Owners shall ensure processing is lawful and document the lawful grounds for processing.

11.2 Where processing involves data of Children, parental consent must be sought, provided and documented.

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

11.4 Where Sensitive Data is involved sufficient legal grounds must be established to allow it to be processed. Advice must be sought from DPO regarding such grounds prior to processing of such data.

## 12. Transparency

12.1 Process Owners shall ensure information related to their processing activities is made available to the DPO so an Abaco Data Protection Notice may be published.

12.2 Data Subjects shall be informed of processing activities and provided statutory information at the time data is requested.

12.3 Where data is collected from a source other than the Data Subject, they shall be informed of processing formalities and provided statutory information as soon as practicable but no less than 10 working days from data collection.

12.4 Process Owners shall review the published Data Protection notice quarterly for any inaccuracies relating to processes. The Process Owner shall report inaccuracies to the DPO within 5 working days.

## 13. Protection by Design & Default

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

13.2 Process and System Owners shall implement appropriate technical and organisational measures to ensure that protection is incorporated into processes and systems, by design and default.

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

13.4 All Information Systems shall ensure their systems undergo a Data Protection Impact Analysis (DPIA) which contains at a minimum:

a] a systematic description of the envisaged processing operations and the purposes of the processing.

b] an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c] an assessment of the risks to the rights and freedoms of data subjects;

d] 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.

13.6 The System Owner shall consult with the DPO in relation to the completion of the DPIA.

13.7 The DPO shall, where the risk to Data Subjects' rights is deemed HIGH, consult with the Supervisory Authority.

13.8 System Owners shall ensure systems are explicitly designed to minimise the impact involved in upholding Data Subjects' rights.

13.9 Process Owners shall ensure processes are explicitly designed to minimise the impact involved in upholding Data Subjects' rights.

## 14. Security of Processing

14.1 System Owners shall be accountable for ensuring 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 and Testing
VI. Development and Testing Activities
VII. Security breach monitoring and detection

14.2 Information Systems, containing personal or sensitive data, exposed to the Internet or a Third Party, shall subject to an independent, risk-based penetration test to an agreed scope, no less than annually. System Own shall ensure all issues identified are appropriate treated commensurate with the Board's risk appetite.

14.3 Personal Data Breaches shall be reported to the DPO as soon as possible but no later than 24 hours of detection.

## 15. Accuracy of Processing

15.1 Process Owners shall ensure data remains accurate and where inaccurate corrected as soon as possible but no later than 5 working days from when an error is reported and verified.

15.2 Process Owners of processes involving automated decision making or profiling shall document an alternative manual process and ensure appropriate resources are trained to carry out the manual process if required.

15.3 A Data Subject shall have a right not to be subject to an automated decision or profiling. Process Owners shall ensure this right is respected except where statutory exemptions apply.

## 16. Retention

16.1 With the exception of data held under statutory exemptions, personal data shall not be retained any longer than necessary.

## 17. Data Subject Access

17.1 Process Owners shall ensure those processing data understand how to identify a Data Subject access request.

17.2 Data Subject access requests shall be recorded in a register owned by the DPO.

17.3 Data Subject access requests shall be completed as soon as possible but no more than 30 calendar days following receipt of the request.

17.4 Data Subject access requests shall not incur a charge.

17.5 Data Subject access request shall be processed electronically if this is requested by the Data Subject.

17.6 Reasonable steps shall be taken to verify the identity of the Data Subject prior to providing access to their personal data.

17.7 System Owners shall ensure appropriate resource is made available to support Data Subject access requests.

17.8 Reasonable steps shall be made to seek the permission of third parties prior to including their information an access request. Where permission is not provided, the DPO shall be consulted to determine whether data shall be provided or redacted.

17.9 Requested information shall be communicated to the Data Subject securely.

## 18. Third Party Processing

18.1 Processing activities shall not be outsourced to a third party without a binding written contract that sets out abject-matter and duration of the processing, the nature and purpose of the processing, the type of personal and categories of Data Subjects and the obligations and rights of Abaco.

18.2 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 ensure the protection of the rights of the Data Subject.

18.3 Process and System Owners shall consult with, and attain a written recommendation from the DPO and representatives from Legal, Procurement, Information Security, Business Continuity and Risk 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 Processor's data protection technical and organisational controls.

18.4 Process and System Owners shall, where necessary, engage an independent (internal or external) assessor that is professionally certified to assess the third party Processor's data protection technical and organisations controls.

18.5 Process and System Owners engaging third-party Processors shall ensure ongoing compliance with this policy and maintain accurate records of relevant meetings and compliance visits including supporting evidence of third party Processor's ongoing compliance.

## 19. Roles & Responsibilities

19.1 The Abaco Board of Directors has overall responsibility for this policy, and for reviewing the effectiveness of actions taken in response to concerns raised regarding its provisions.

19.2 Abaco Senior Management ("Senior Management") shall ensure appropriate resources are made available to support the implementation of policy throughout all in-scope areas.

19.3 All those in scope of this policy are responsible for adhering to its requirements.

19.4 The Data Protection Officer (DPO) is responsible for monitoring compliance with this policy and shall provide periodic reporting to the Board and Senior Management on Abaco's compliance with it.

19.5 The Data Protection Office shall be the contact point for all matters relating to the Supervisory Authority ("SA").

19.6 The Chief Information Security Officer ("CISO") is responsible for providing information security support as required to meet the requirements of this policy.

19.7 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.

19.8 The Owners of the policies, detailed in section 10, shall ensure requirements are amended to reflect the requirements of this policy.

19.9 The Head of Human Resources shall ensure Human Resources processing is compliant with the requirements of this policy.

19.10 The Head of Marketing shall ensure processing related to marketing activities is compliant with the requirements of this policy.

19.11 The Head of Sourcing shall ensure procurement processes are compliant with the requirements of this policy.

19.12 Internal Audit shall provide the Board with independent assurance that Abaco is adhering to the requirements of this policy.

## 20. Related Policies and Supporting Documents

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

I. Risk Management Policy
II. Security Policy
III. Incident Response Policy
IV. Records Management Policy
V. HR Policies
VI. Change Management Policy
VII. Project Management Policy
VIII. Outsourcing Policy
IX. Fraud Policy
X. Visitor Policy

20.2 The policies referred to in paragraph 20.1 above and other supporting materials and templates can be found in the relevant Policy Portal on the Abaco Intranet Site and/or the relevant Abaco Towcester Network location. The relevant locations will be notified to all employees and other relevant parties from time to time.

## APPROVALS

Signature: 

Name : ANDY MACCAIG

Title : DIRECTOR

Date: 18th MAY 2018

## Appendix A — Glossary of Terms

**Child:** For the purposes of GDPR is a Natural person who requires parental consent, usually if they are below 16, unless otherwise directed by overriding UK or EU legislation.

**Consent:** Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

**Controller:** The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law.

**Data Protection Impact Assessment (DPIA):** An assessment of the impact of the envisaged processing operations on the protection of personal data and the rights and freedoms of natural persons.

**Data Protection Officer (DPO):** A person with expert knowledge of data protection law and practices who assists the Controller or Processor to monitor internal compliance with GDPR. Such data protection officers, if they are an employee of the Controller, should be able to perform their duties and tasks in an independent manner.

**EU Member State:** Any country party to the founding treaties of the European Union (EU) and thereby subject to the privileges and obligations of membership. Member States are subject to binding laws in exchange for representation within the common legislative and judicial institutions.

**Information Security:** The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

**Natural Person:** Essentially an EU citizen who is alive. A Natural Person may also be referred to as a "Data Subject".

**Personal Data:** Any information relating to an identified or identifiable Natural Person; an identifiable Natural Person is one who can be identified, directly or indirectly, in particular 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 Natural Person.

**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.

**Processing:** 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 collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Processor:** A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

**Profiling:** Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a Natural Person, in particular to analyse or predict aspects concerning that Natural Person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

**Sensitive Data:** Special categories of information relating to an identified or identifiable Natural Person. Examples include but are not limited to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, health data, biometric data, sex life, sexual orientation, criminal records, etc.

**Subject Access Request (SAR):** A request, made by a Natural Person, to access personal data held by a Controller or Processor.

**Supervisory Authority:** The regulator within a European country who will provide regulatory oversight for GDPR, provide guidance and advice and, where necessary, impose corrective actions or administrative fines.

**Third Country:** Any country which is not an EU Member State (e.g. USA, India, China or the other such non-EU country).