1. Introduction

The Brintons Group ("Group") is committed to safeguarding the privacy of all personal and sensitive data held by the Group.

1.2 Purpose

[1.2.1] The Group undertakes and controls activities which involve the processing of Personal and Sensitive Data relating to European Union data subjects. The Group must therefore comply with the General Data Protection Regulation 2016 ("GDPR") and the Privacy & Electronic Communications Regulation 2003 ("PECR"). This policy sets out the requirements all those in scope must adhere to.

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

1.3 Group Risk Appetite Statement

[1.3.1] The Group Board's risk appetite for a material breach of GDPR is LOW.

[1.3.2] The Board has identified the risk of personal data breaches and failing to uphold the rights and data security of its data subjects as being a major risk to the Group's reputation and standing.

1.4 Scope

[1.4.1] The scope of this policy covers all processing activities and supporting information systems involving personal or sensitive data where the organization acts as the data controller. This includes personal or sensitive data in physical form, stored in a relevant filing system.

[1.4.2] The scope of this policy covers all the Group's global activities and territories; including those outside the European Union (EU).

[1.4.3] The scope of this policy covers all Employees, Contractors, Third Parties, Processors or others who process personal or sensitive data on behalf of the Group.

2. Requirements

2.1 Principles

[2.1.1] All processing activities shall be:

- Collected for specified, explicit and legitimate purposes only
- Accurate and, where necessary, kept up to date
- Retained only for as long as necessary
- Processed lawfully, fairly and in a transparent manner
- Processed securely, in an appropriate manner to maintain security
- Adequate, relevant and limited to what is necessary

2.2 Managing Data Protection

[2.2.1] The Company Secretary ("CoSec") will have overall responsibility for the management and implementation of this policy and shall report directly to the Group Board.

[2.2.2] The CoSec shall support the organization in upholding the rights of data subjects as it related to the organization's processing activities.

[2.2.3] The CoSec shall respond to inquiries from data subjects in a timely manner.

[2.2.4] The CoSec shall support compliance with this policy by providing support and advice as it relates to complying with the requirements of this policy.

[2.2.5] The CoSec shall maintain the following registers:

- Register of processing activities
- Register of Data Protection Impact Assessments ("DPIA")
- Register for Data Protection Metrics
- Register for Data Subject Inquiries

[2.2.6] The CoSec shall report personal data breaches to the Supervisory Authority (e.g. the Information Commissioners Office ("ICO") in the UK.

2.3 Accountability

[2.3.1] A record of processing activities shall be provided to the CoSec.

[2.3.2] A System Owner ("SO") shall be appointed for all information systems containing personal or sensitive data.

[2.3.3] System ownership shall not be assigned to a person who does not have management responsibility for that particular information system.

[2.3.4] System ownership shall not be assigned to a person who does not hold formal management authority over those carrying out the processing activity within that information system.

[2.3.5] A SO may delegate authority for operational tasks relating to this policy but they shall and cannot delegate responsibility and accountability.

[2.3.6] A SO may seek advice in the discharge of their duties but remains responsible and accountable for any subsequent decisions taken.

[2.3.7] Processing activities shall be documented and a Process Owner ("PO") appointed.

[2.3.8] Process ownership shall not be assigned to a person who does not hold formal authority over the processing activity within the information system.

2.4 Lawfulness of Processing

[2.4.1] POs shall ensure processing is lawful and document the lawful grounds for processing.

[2.4.2] Processing of children's data is strictly prohibited.

[2.4.3] With the exception of storage, processing shall cease immediately when there are no longer lawful grounds for processing.

2.5 Transparency

[2.5.1] POs shall ensure information related to their processing activities is made available, so that an organizational data protection notice may be published and kept up to date.

[2.5.2] Data subjects shall be informed of our processing activities and provided with statutory information at the time data is collected.
[2.5.3] Where data is collected from a source other than a data subject, the data subject shall be informed of our processing activities and provided with statutory information as soon as practicable but at the latest within 10 working days.
[2.5.4] POs shall review the published data protection notice quarterly for any inaccuracies relating to their processes. The PO shall report any inaccuracies to the CoSec within 5 working days.

2.6 Data Protection by Design and Default
[2.6.1] All Group information systems and processes shall be designed to comply with the requirements of this policy.
[2.6.2] SOs and POs shall implement appropriate technical and organizational measures to ensure that data protection is incorporated into processes and systems, by design and default.
[2.6.3] Processing activities and supporting information systems shall be designed to ensure the minimum personal data is stored and for the minimum period necessary.
[2.6.4] All information systems shall ensure their systems undergo a Data Protection Impact Analysis ("DPIA") which contains as a minimum:

- A systematic description of the envisaged processing operations and the purposes of the processing.
- An assessment of the necessity and proportionality of the processing operations in relation to the purpose.
- An assessment of the risks to the rights and freedoms of our data subjects.
- 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.

[2.6.5] The SO shall consult with the CoSec in relation to the completion of the DPIA.
[2.6.6] The CoSec shall, where the risk to data subjects' rights is deemed HIGH, consult with the Supervisory Body.
[2.6.7] SOs shall ensure systems are explicitly designed to minimize the impact involved in upholding data subjects' rights.
[2.6.8] POs shall ensure processes are explicitly designed to minimize the impact involved in upholding data subjects' rights.

2.7 Security of Processing
[2.7.1] SOs shall be accountable for ensuring systems meet the minimum required standards for security. Including, but not limited to:

- Identity and access management
- Patch and vulnerability management
- Change management
- Backup and restoration
- IT service continuity planning
- Development and testing activities

[2.7.2] 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. SOs shall ensure all issues identified are appropriately treated in line with the Board's risk appetite.
[2.7.3] Personal data breaches shall be reported to the CoSec as soon as possible but no later than 24 hours after detection.

2.8 Accuracy of Processing
[2.8.1] POs shall ensure data remains accurate and, where inaccuracies are identified, corrected as soon as possible but no later than 5 working days from when the inaccuracy is identified and verified.
[2.8.2] POs of processes involving automated decision making or profiling shall document an alternative manual process and ensure appropriate resources available and people trained so that this manual process can be carried out if necessary.
[2.8.3] A data subject shall have the right not to be subject to an automated decision or profiling. POs shall ensure this right is respected except where statutory exemptions apply.

2.9 Retention
[2.9.1] With the exception of data held under statutory exemptions, personal data shall not be retained any longer than is necessary.

2.10 Data Subject Access
[2.10.1] POs shall ensure those processing data understand how to identify a Data Subject Access Request ("DSAR")
[2.10.2] DSAR shall be recorded in a register owned by the CoSec.
[2.10.3] DSAR shall be completed as soon as possible but within 30 calendar days.
[2.10.4] DSAR shall not incur a charge.
[2.10.5] DSAR shall be processed electronically if this is requested by the data subject.
[2.10.6] Reasonable steps shall be taken to verify the identity of the data subject prior to providing access to their personal data.
[2.10.7] SOs shall ensure appropriate resources are made available to support DSARs
[2.10.8] Reasonable steps shall be made to seek the permission of third parties prior to including their information within a DSAR. Where permission is not provided, the CoSec shall be consulted to determine whether data should be provided or redacted.
[2.10.9] Responses to DSARs shall be communicated to the data subject securely.

2.11 Third Party Processing
[2.11.1] Processing activities shall not be outsourced to a third party without a binding written contract 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 the organization.

[2.11.2] POs shall use only their party processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this policy and ensure the protection of the rights of the data subject.
[2.11.3] POs and SOs shall consult with, and obtain a written recommendation from the CoSec and authorization from at least two Directors prior to signing a contract with a third party processor and with sufficient time to carry out an effective due-diligence process on the proposed outsourced process and the third party processors data protection technical and organizational controls.
[2.11.4] POs and SOs shall engage an independent (internal or external) assessor that is suitably qualified to assess the third party processors data protection and organizational controls.
[2.11.5] POs and SOs engaging third party processors shall ensure continuing compliance with this policy and maintain accurate records of relevant meetings and compliance visits including supporting evidence of the third party processors ongoing compliance.

3. Roles and Responsibilities

[3.1] The Group Board has overall responsibility for this policy, and reviewing the effectiveness of actions taken in response to concerns raised in respect of this policy.
[3.2] Senior management shall ensure appropriate resources are made available to support the implementation of this policy throughout the Group.
[3.3] All directors and employees with responsibilities under this policy are required to adhere to the terms of this policy.
[3.4] The CoSec is responsible for monitoring compliance with this policy and shall provide periodic reporting to the Board and Senior Management on the organization's compliance with this policy.
[3.5] SOs and POs are responsible for ensuring their processes and information systems meet the minimum requirements of this policy.
[3.6] The Head of Human Resources shall ensure Human Resources processing is compliant with the requirements of this policy.
[3.7] The Head of Marketing shall ensure processing related to marketing activities is compliant with the requirements of this policy.
[3.8] The Head of Purchasing shall ensure procurement processes are compliant with the requirements of this policy.

4. Ownership and Approval

[4.1] The owner of this policy is the incumbent Company Secretary.
[4.2] This policy was endorsed by the Board on 18 May 2018 and it is effective from that date.