Data Protection Policy

(inc. management and disclosure of employee and customer data)

National World plc

1. Introduction

Data protection legislation regulates the way in which companies may use (process) the personal information of individuals (including customers, staff, suppliers or other third parties) and protects them from unauthorised use or disclosure of their personal details e.g. name, address, telephone number, email address etc. ("Personal Data").

National World plc ("the Group") and any other companies within its group of companies aims to fulfil its obligations under the UK General Data Protection Regulation ("UK GDPR"), Data Protection Act 2018 ("DPA 2018") as amended or superseded and any other applicable privacy legislation (collectively the "Legislation"), and recognises the need to balance the Group's legitimate need to run its business with that of an individual's legitimate right to respect for their private life. The purpose of this policy is to provide guidance on management and disclosure of personal data and is not intended to confer any additional rights or contractually bind the Group.

1.1 Responsibilities

Compliance with the Legislation is the responsibility of all individual employees of the Group. Employees are expected to familiarise themselves with, and observe at all times the Group's policy and procedures relating to data protection, together with any additional instructions which may be introduced from time to time.

The person having overall responsibility for data protection within the Group is the Data Protection Officer.

The Data Protection Officer should be the first point of contact on all legal and policy matters relating to data protection and privacy. Should external legal advice on data protection issues be required then this will be arranged through the Data Protection Officer and should not be taken locally.

All correspondence and training documentation relating to data protection and privacy must be approved by the Data Protection Officer prior to circulation.

Each Manager or Supervisor will have responsibility for data protection matters in their own immediate area of work and for the actions of their team.

It is the responsibility of all employees to ensure that all Personal Data provided by them to the Group is accurate and kept up to date.

The Group must comply with the six data protection principles contained in the Legislation. The principles of data protection state that the processing of Personal Data must be:

1. Fair and lawful
2. Purposes must be specified, explicit and legitimate
3. Personal Data must be adequate, relevant and not excessive
4. Personal Data must be accurate and kept up to date
5. Personal Data must not be kept for longer than is necessary
6. Personal Data must be processed in a secure manner

1.2 Non-compliance

Failure by the Group to comply with any of the requirements of the Legislation could result in serious consequences for the Group, including being prevented from using the Personal Data, possible personal criminal liability for staff, the likelihood of damaging media attention and the possibility of an investigation followed by sanctions being imposed by the Information Commissioner.

2. Policy

It is the policy of the Group to comply with the letter and spirit of the Legislation. In specific terms, this means the Group:

- Operating within the confines of its privacy notices and policies
- Operating in compliance with the six data protection principles
- Providing appropriate data protection training to all staff
- Ensuring any exemptions are applied consistently and accurately in accordance with the law
- Taking note of the guidance and standards issued by the Information Commissioner from time to time
- Ensuring that any external parties we contract with are appropriately registered with the Information Commissioner and comply with the Legislation, as applicable
- Implementing appropriate mechanisms and safeguards for any international transfers
- Taking note of applicable industry codes of practice, for example:
    - the Direct Marketing Association
    - the British Codes of Advertising and Sales Promotion
    - the Independent Press Standards Organisation (IPSO)

  These are codes of practice in the UK. Other codes may apply to other specific areas of the business.

2.1 Standards

The Group undertakes to follow the Data Protection Policy and to establish adequate compliance arrangements, including adequate business processes and training schedules, to implement that policy.

The Data Protection Officer and other relevant internal audit functions will conduct an ongoing review of compliance with the Data Protection Policy.

3. Collection and Retention

The Group collects and uses Personal Data about living individuals in order to carry on its business and meet its customers' requirements effectively. The Group recognises that the lawful and correct treatment of Personal Data is very important for maintaining trust between the Group and its customers.

Any Personal Data which are collected, recorded or used in any way (whether held on paper, computer or other media) will have the appropriate safeguards applied to it in order to ensure compliance with the Legislation.

3.1 Collection

The Group will only collect Personal Data that is relevant to the carrying out of the legitimate purposes and functions of the Group, in a way that is not prejudicial to the interests of individuals. All employees involved in the collection, processing or administration of Personal Data are responsible for ensuring that this happens. The Group will ensure that all data collection is accurate and as up to date as possible.

The Group will obtain employees' consent prior to the commencement of employment as part of the Group's ongoing data protection compliance. Employees will be informed if their Personal Data requires to be processed for any additional purposes.

3.2 Data Retention

All Personal Data will be kept up to date and when no longer required for the legitimate purposes of the Group, will be disposed of in accordance with the provisions of the Legislation.

3.3 Sensitive/Special Category Personal Data

Sensitive Personal Data include data about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental condition, sexual life, details of the commission or alleged commission of any offence and any court proceedings relating to the commission of an offence.

The Group will handle sensitive or special category personal data with particular care. Before collecting or processing sensitive or special category personal data, the Group will ensure that the appropriate notifications to the individuals have been given and any required consents obtained.

4. Disclosures

The Group will not allow data collected from individuals to be disclosed to third parties except in circumstances which meet the requirement of the Legislation. For example:

- The individual has consented to the disclosure; or
- The Group is legally obliged to disclose the data; or
- There is a business requirement to disclose the data which is within the remit of the Legislation and is not prejudicial to the interests of the individual.

5. Processing

Data processing will be allowed only where there is a clear purpose for the activity, which meets the requirement of the Legislation. If the purpose of the processing of the data is unclear, the Group will notify the individual concerned, who in turn, will be given the opportunity to object to this type of processing.

Employee Personal Data may be processed for the purposes of salary administration, pension administration, health administration, health insurance/benefits, training and appraisal including performance records, disciplinary and grievance records, Group car fleet/leasing administration, any Group benefit administration, marketing of products and services to employees, for diversity and inclusion monitoring purposes or for the purposes of any potential sale of over 50% of the shares of the Group or other changes of control or any potential transfer of an employee's employment under the Transfer of Undertakings (Protection of Employment) Regulations 1981. Disclosure may also be made in the case of sale, change of control or transfer, of the Group (to the potential purchaser or investor and their advisors).

Where Personal Data are passed to a third party for processing, the Group will ensure that a written contract is put in place by the Data Protection Officer, that requires the data processor to act only on the instructions of the Group, and to specifically not disclose Personal Data without specific authority. Such contract should also include appropriate operational and technical security measures and allow the Group to audit adherence to the contract.

6. Editorial Exemption

Under the Legislation, journalism is defined as a 'special purpose' to which an exemption applies. However, in order to claim the exemption the processing of Personal Data must be undertaken with a view to publication and the publication must be in the public interest. The exemption states that any processing satisfying these two criteria does not then have to comply with the Principles of the Legislation other than the sixth Principle which relates to

keeping Personal Data physically and technically secure. The exemption also removes the individual's right to access a copy of their Personal Data and to have their Personal Data deleted, blocked and/or corrected.

It should be noted that this exemption does **not** include the offences under the Legislation, for example it is an offence to buy illegally obtained Personal Data. Journalists should be aware of this and ensure that any Personal Data purchased is procured from a legal source. For further guidance on data protection journalists should refer to the IPSO Editors' Code of Practice' and the Editorial Data Protection Briefing.

7. Transfers or Joint Venture Arrangements

It is essential that any transfers of personal data outside the Group are subject to safeguards to ensure continued compliance with the Legislation. Such transfers must comply with established internal guidelines to ensure that appropriate notifications have been given, a comprehensive data processor contract must be put in place if required and any required consents should be obtained or rights to object provided. In particular, the Group will require third parties to agree to comply with appropriate privacy and information security standards designed to ensure an adequate level of protection.

8. Transfers Outwith the Jurisdiction

Any transfers of Personal Data outside of the UK must be protected via appropriate security and transfer mechanisms, where appropriate.

However, Personal Data must **not** be transferred to a country or territory outside the UK unless the country or territory ensures an adequate level of data protection. Therefore the Data Protection Officer will assess whether the country provides this level of protection and provide an appropriate contract with such a third party and implement any necessary safeguards to ensure compliance.

9. Subject Access

Employees are entitled to access their Personal Data and may do so by contacting the HR Team, who will respond to the request with a confirmation of receipt. Within 30 days of receipt HR will supply all relevant information to which the individual is entitled under the Legislation. The information will be provided in a format agreed with the individual.

Employees should inform HR immediately if they believe that any Personal Data held by the Group is inaccurate.

In the event of a dispute between an employee and the Group regarding Personal Data, the matter should be raised with the Data Protection Officer and be processed in accordance with the Group's grievance procedure.

10. Marketing

The Group will act on any request from an individual to cease processing their Personal Data for the purpose of direct marketing.

The Group will adhere to all other relevant legislation governing marketing by electronic means.

11. Security

The appropriate technical, physical and operational security measures must be put in place to ensure the security of Personal Data against the unauthorised or unlawful processing of the Personal Data and against the accidental loss or destruction of, or damage to, Personal Data.

Employees who are required as part of their job description to process Personal Data about employees or customers will receive training and guidance on the appropriate security of Personal Data to ensure that all data is processed fairly and lawfully. However, the Group expects all of its employees to be aware of the basic principles as set out in this policy. In particular, employees should be aware of the following:

- The Data Protection Officer must be the first point of contact on all legal and policy matters relating to data protection;
- All Personal Data held by the Group must be treated as strictly confidential;
- Personal Data must not be disclosed to anyone outside the Group unless the individual concerned has consented to such disclosure and/or the Data Protection Officer has given specific instructions to do so;
- The Personal Data must be kept secure at all times. It must not be left unattended unless it has been placed in a secure location. Group companies will be advised by the Data Protection Officer of the physical security or arrangements to be adopted appropriate to the level of confidentiality of the Personal Data concerned;
- Personal Data must not be removed or transferred from the Group's premises without documented authorisation from the Data Protection Officer,
- It is the responsibility of all employees to report all security breaches or suspected security breaches or disclosure of Personal Data to the Data Protection Officer.

Any breach of these guidelines may lead to disciplinary action and depending on the seriousness of the breach may lead to summary dismissal.

12. Contact

If you have any enquiry or concern about the Group's Data Protection policy, please contact the Data Protection Officer email: data.protection@nationalworld.com