Policy statement

GLOBAL POLICY – APPLIES TO EVERYONE ACROSS ALL LOCATIONS

Dealogic is committed to protecting the privacy of individuals; it also has a legal obligation to comply with the various data protection laws in the countries in which it operates. This policy describes Dealogic's main obligations under applicable privacy laws and its approach to compliance in relation to those laws.

The purpose of this policy is to:

- Set out the key principles that relate to the protection of personal information used by Dealogic and its staff;
- Outline what steps Dealogic will take to comply with those principles;
- Describe other sources of information that provide additional guidance and procedures that support this Policy;
- Ensure accountability for compliance is understood and demonstrated across the business; and
- Identify potential penalties and sanctions for failures to comply with this Policy.

Who is covered by the policy?

This policy covers all individuals working for the Company at all levels and grades, including directors, senior managers, officers, employees, contractors, trainees, home-workers, part-time and fixed-term employees, and agency staff (collectively known as "**employees"** in this policy), and third parties who have access to the Company's data and/or electronic systems.

Key privacy principles

Personal information is any data that could be used to identify an individual. This includes information in the public domain and business contact data such as business email address and job title.

The key privacy principles require that personal information is:

- Processed fairly and lawfully and in a way that is transparent to individuals;
- Only collected for specified and explicit legitimate purposes and not further used in a way that is incompatible with those purposes;
- Adequate, relevant and limited to that which is necessary in relation to the purposes for which it is collected and used;
- Accurate and, where necessary, kept up to date;

- Retained in an identifiable form for no longer than is necessary;
- Processed in a manner that ensures the appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by using appropriate technical and organisational measures;
- Processed in accordance with the rights of individuals in relation to their personal information;
- Treated in accordance with any local laws. Where local data protection laws place restrictions on transferring data to other countries, personal information may not be transferred unless the recipient country or territory ensures an adequate level of protection as identified in the relevant applicable law.

Furthermore, any organisation that collects, handles or stores personal information must have in place measures to be accountable for compliance with the privacy principles and be able to demonstrate that compliance.

How Will Dealogic Comply?

Dealogic will, through appropriate management and application of controls:

Fair and lawful processing

- Observe the conditions regarding the fair collection and use of information particularly in respect of any personal information that might be considered sensitive under applicable laws;
- Meet its legal obligations to specify the purposes for which information is used;

Transparency

- Provide individuals with timely and accurate explanations of how their personal information will be used, including the reasons for its use and any additional information to ensure that Dealogic's use of that information is fair and lawful;
- Where appropriate give individuals the opportunity to consent and/or object to the use of their information and ensure that those choices will be respected;
- Where a security incident or other breach of data protection laws might adversely affect individuals, as necessary, take appropriate steps to inform those potentially affected by such events and provide advice and information on how to mitigate such effects;

Data quality and retention

- Take steps to ensure the accuracy and quality of information used;
- Only collect and process information to the extent that it is needed to fulfil operational or business needs or to comply with any legal requirements;

- Apply checks to determine and manage the length of time information is held in a format that allows the identification of individuals and that it is in accordance with Dealogic records management policies;

Security and integrity of data

- Implement and maintain the appropriate technical and organisational policies, procedures and measures to safeguard personal information;

- Maintain a process for identifying breaches of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed and recording details of the same;

- Follow Dealogic's Procurement Policy and procedures for engaging new suppliers and reviewing arrangements with existing suppliers who collect, handle or store personal information for which Dealogic is responsible. Any supplier or third party who handles Dealogic data will be required by written contract to commit to protecting personal information according to Dealogic standards and provide assurances that such protections will be maintained during its relationship with Dealogic;

Individual rights

- Ensure that the rights of people about whom information is held can be fully exercised. These rights may be qualified but will include:
  - the right to be informed that processing is being undertaken;
  - the right of access to their personal information;
  - the right to correct or rectify information that is regarded as wrong;
  - the right to erasure or to restrict processing ('right to be forgotten');
  - the right to object to processing; and
  - the right to data portability;

Transfers of data

- Take steps to ensure that any data that is transferred will be protected in a manner that is compliant with applicable privacy laws and which satisfies any local legal obligations attached to the information in question; and

- Ensure that such compliance obligations are also passed onto those third parties that help Dealogic provide its services.

Training and communication

Training on this policy will be provided. It is the responsibility of employees to ensure they have read and understood this policy. Requests for additional training will be considered.

Who is responsible for the Policy?

Everyone within the business should understand they are responsible for privacy compliance. Dealogic shall provide training and awareness updates. In addition, it will:

- Establish and maintain a description of its processing activities including the reasons for using the data, the lawful grounds for processing, retention periods and any relevant sharing or transfers of data to third countries;
- Utilize tools and methodologies such as Privacy Impact Assessments and Privacy by Design techniques to ensure privacy risks are effectively managed and minimized; and
- Have an officer responsible for oversight of compliance.

Impact of breach of this Policy

Failure to comply with data privacy laws can have severe adverse consequences for Dealogic, including financial penalties and sanctions, reputational damage, hindered competitiveness, and a loss of trust and confidence in Dealogic.

Any employee who breaches this policy may face disciplinary action, which could result in dismissal for gross misconduct. Dealogic reserves its right to terminate its contractual relationship with contractors if they breach this policy.

Who to contact

If you have any queries or concerns relating to this policy, please contact the Legal team: legal@dealogic.com.

Appendix A: Document History

Document History

Version	Amended by	Approved by	Date
1.0	Privacy Partnerships	Legal	23 November 2017

Amendments

Version	Amendments