DEALOGIC SECURITY AND PRIVACY MEASURES

Objective

The key objectives of Dealogic's Information Security Program and Privacy Framework are to ensure clients' continued confidence in the Dealogic platform and its associated services by maintaining a risk-based culture and a dedicated focus on comprehensive security controls. Information Security and Privacy are the responsibility of the whole organization.

The key elements of Dealogic's Information Security Program include: a clearly defined security strategy; a certified Information Security Management System (ISMS); documented policies, processes and standards together with guidelines and plans. The Dealogic Information Security Program is certified against the current ISO27001 standard for its ISMS. ISO27001 is a globally recognized standard that defines international best practice for managing the security of information. Dealogic's Information Security Program is subject to regular external/independent review.

The Dealogic Privacy Framework includes a Data Protection Policy as well as guidelines to ensure employees are aware of their obligations and know where to go for additional support. Privacy Impact Assessments will be undertaken where the processing is considered to present a high risk to individuals or the numbers of individuals whose data is to be processed is significant. The business will adopt Privacy by Design and Default principles to ensure privacy risks are understood and, as far as possible, mitigated. Accountability for compliance with general privacy principles is shared across the whole company and appropriately senior individuals are tasked with ensuring their area of operations follow best practice and relevant regulatory requirements and guidance.

1. Personnel

Dealogic personnel are obliged to maintain the confidentiality of any third party and Dealogic data and are required to conduct themselves in a manner consistent with Dealogic's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Reasonably appropriate backgrounds checks (to the extent legally permissible and in accordance with applicable local law and regulation) shall be made before personnel are granted access to data.

All Dealogic employees receive training on their obligations under data protection legislation and additional guidelines are in place and continue to be developed to provide practical assistance to employees in carrying out their duties. They are also reminded that failure to comply with the Dealogic Privacy Policy may lead to disciplinary actions.

2. Technical and Organizational Measures

Dealogic has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect different types of personal data (for example, client data, data of users of Dealogic systems and employee data) including, but not limited to:

- Personally identifiable information (name, email, telephone number and login credentials)
- Government and state provided unique identification (social security / national insurance)
- Financial data (bank details, dealings and investments)
- Identity (physical, physiological, mental, economic, cultural or social identity)

Protection controls shall include (but not be limited to):

- Role-based access
- Data loss protection through copy restrictions and email filtering
- Vulnerability and patch management
- Use of encryption and pseudonymisation
- Resiliency and Business Continuity Plans (BCP)

3. Application Security & Delivery

(a) Physical Security

Critical information processing facilities (cloud and hosted datacentres) that are used to store production data are geographically distributed and have been selected based upon their ability to protect systems against damage or disruption resulting from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster to a level defined by a risk assessment.

Physical protection of sites and availability of services are protected through various means, which may include the following:

- physical security – barriers, cages, cabinets, intruder detection/alarms, door access controls, shutter doors, bomb-proof glass, CCTV, on-site security staff
- connectivity – primary and backup telecommunications via multiple ISPs
- monitoring – power, communications, environment
- environmental – redundant cooling and environmental systems (e.g., humidity, filtration)
- lighting – provided from multiple power sources
- water – early notification of water leakage or infiltration
- fire and smoke – early detection and suppression systems

Power systems have been designed to provide redundant and maintainable supplies for continued operation. All power provision has been architected with redundant power supply including multiple power sources including:

- N+1 redundancy on power
- Redundant UPS
- Diesel generators with on-site fuel supply and extended fuel re-supply contracts

Critical infrastructure systems have been architected to eliminate single points of failure and allow for synchronisation of data between multiple information processing facilities in disparate regions. All systems are designed to allow the preventative and corrective maintenance with minimal interruption and are subject to preventative maintenance procedures in accordance with the manufacturer's or internal specifications.

Dealogic utilise Microsoft operating software. It maintains a formal evaluation, testing, and authorisation process to apply regular updates to all operating systems and key software applications in line with the vendor. Where external cloud-based services are used, additional controls are applied in terms of data protection, data destruction and single/multi- tenanted environments.

All data storage systems are architected to allow synchronization of between two or more locations in order to ensure the shortest recovery time and closest recovery point. Failover and testing of systems is performed regularly to ensure recovery within required recovery time objectives.

(b) Delivery Networks & Transmission

The connectivity, in both cloud and datacentre environments is managed to protect against threats and to maintain security for the systems and applications, including protecting information in transit.

Physical or virtual firewalls are deployed at appropriate points within the infrastructure. Alerts and logs from all components are exported to, and reviewed, by Dealogic's security operations centre. Firewall platform operating system releases and software patches are reviewed and assessed on a quarterly basis in line with current vendor recommendations. Dealogic maintains a resilient network consisting of multiple enforcement and load-balancing elements. The systems infrastructure is regularly scanned to look for vulnerabilities and a Web Application Firewall (WAF) is in place as additional protection.

Changes to the security operations tools and infrastructure are performed according to documented change management procedures.
All application connections to Dealogic use defined protocols and ports. Data is protected through the application of encryption and transport technologies such as the latest versions of HTTPS protocols TLS connections.

(c) Physical Access and Site Controls

Dealogic Office, datacentres or cloud facilities are subject to perimeter security controls, including:

- Security boundaries are defined, and the location and strength of each of the perimeters depends on the security requirements of the assets within that perimeter.
- Critical information processing equipment (equipment necessary to provide a managed service), are housed in secure areas that are protected by appropriate barriers and entry controls. They are physically protected from unauthorised access, damage, and interference. Reviews of physical security are part of the Dealogic internal, and independent external audit functions, carried out on not less than an annual basis.
- Access to Dealogic offices and buildings is restricted to authorised personnel only and controlled accordingly. Access is logged.
- Access to third-party sites utilised by Dealogic for the processing of data is highly controlled through defined processes by the site owner. These controls are audited at regular intervals.

- Permanent and contract staff are provided with an electronic access card that includes photographic identification where possible. Access is restricted to relevant areas of the building.
- Equipment rooms and any areas where sensitive information is stored are subject to additional controls. Utility access panels are locked at all times.
- Visitors to any Dealogic facility are provided with a temporary access pass that is valid only for the date of the visit and always accompanied and/or monitored by a Dealogic staff member until leaving the premises.
- Where access is required to high-security areas, visitors are required to provide photographic identification and be escorted at all times.
- Cloud and Dealogic managed Datacentre facilities are protected through the implementation of barriers, cages, cabinets, intruder detection/alarms, door access controls, shutter doors, bomb-proof glass, CCTV and on-site security staff.

(d) Logical Access Control

To prevent unauthorised logical access to the Dealogic infrastructure and applications, access control standards and procedures are established, documented, and reviewed to control assigned privileges based on role and security requirements.

In accordance with the Dealogic logical access control policies, only authorised Dealogic staff are granted access to the production services in order to provide support. Individual access is via a unique username or ID that is traceable to an individual to ensure accurate logging of activities. Multifactor authentication is enforced for all administrators and access to different tiers controlled by role-based access controls (RBAC). Password management and multifactor authentication systems used within the organisation provide an effective, interactive facility that ensures that quality passwords are employed. Policy and procedures are based upon a least-privileged principle.

4. Data

(a) Data Storage, Isolation & Authentication

Information assets are protected from unauthorised access, use, disclosure, disruption, modification, or destruction. In general, information is distributed only on a "need-to-know" basis.

Dealogic classifies information with regard to legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification by using of the following two information classifications:

i. **Confidential** - default restriction for disclosure to staff; this classification shall have three sub-levels:
    - **Dealogic**: Any non-public information where Dealogic is the information owner.
    - **Personal**: Personal information as defined by the General Data Protection Regulation (GDPR), other privacy regulations, and in line with the Dealogic Privacy Policy.
    - **Client**: Any information where Dealogic clients are the information owner and Dealogic is the custodian.

ii. **Public** - unrestricted for disclosure to anyone
    All Dealogic information classified as Public must be reviewed and authorised as such before release. All Public information must be marked as such.

Protection measures take into consideration the format in which the information is stored (e.g., electronic, physical) and the environment in which the information is used (e.g., electronic storage device, media, printed matter, verbal).

(b) Disc Decommissioning and Data Destruction

Magnetic media (e.g., hard disk, backup tape) that has ceased to function normally or no longer meets operational requirements (e.g., legacy version) is physically destroyed (e.g., shredded). Prior to disposal or re-use, all data on hard disk drives is eradicated using a Dealogic-approved zeroization application. Cloud based data is made unrecoverable by revoking the encryption key and the service provider zeroing the disk space.

5. Sub processor Security

Dealogic maintains an information security policy for suppliers of goods and services, along with procedures to assess and manage ongoing risks associated with providing suppliers access to Dealogic information assets, as classified by Dealogic. Suppliers handling personal information on behalf of Dealogic will be subject to contract terms which broadly reflect those

to which Dealogic agrees to when it is acting as a data processor for a client. Where Dealogic acts as a data controller and engages a supplier, it will ensure that the requirements of Article 28 of the GDPR are satisfied.

A supplier risk assessment is completed by Dealogic prior to implementing a service, as appropriate. The risk assessment reviews controls relating to:

- physical and/or logical access to Dealogic data
- acceptable use of Dealogic controlled equipment, network, facilities, etc.
- acceptable behaviour when on a Dealogic site or a Dealogic client site
- legal and/or regulatory requirements
- engagement of sub-contractors/fourth-parties
- requirement for oversight, monitoring, and audits of controls

Suppliers engaged by Dealogic are subject to ongoing oversight, monitoring, and regular review as appropriate which include:

- managing the ongoing relationship with the supplier
- managing and resolving incidents
- setting and reviewing Key Performance Indications (KPIs) and/or Service Level Agreements (SLAs)
- negotiating and reviewing contracts
- communicating supplier-related issues to relevant stakeholders within Dealogic

Changes to the services provided by a supplier are subject to and managed through contract re-negotiation and/or formal redefinition of the services which includes legal and compliance review. If you would like to know more about our supplier management, please contact privacy@dealogic.com.

6. Breach Notification

Dealogic has implemented a formal Incident Management programme. Every employee has access to the service management portal (i.e. ticketing system) so that issues can be identified and managed appropriately including reporting to the relevant parties where necessary.

7. Privacy Compliance

As it operates in a number of jurisdictions, Dealogic has adopted a global Privacy Policy which reflects the standards found in the European General Data Protection Regulation and this Policy must be complied with unless it is not possible owing to other local legal obligations.

(a) Data Subject Rights

As Dealogic mainly acts as a processor in respect of the data that it handles on behalf of clients, it is anticipated that most data subjects will, in the first instance, seek to exercise their rights by directly engaging with the client. Dealogic will however, take all reasonable steps to assist its clients in delivering compliance with any access or similar requests.

(b) PIAS/PBD/Risk Management

Privacy risk within Dealogic is managed in line with generally accepted risk management principles with the addition of the use of Privacy Impact Assessments where high-risk processing is envisaged and the incorporation of Privacy by Design and Default principles when new systems or products are being developed.

(c) International Data Transfers

Dealogic has put in place an Intra-Group Agreement based on the Standard Contractual Clauses approved by the European Commission. These clauses have been signed by members of the Dealogic Group and demonstrate a commitment to ensuring appropriate protections are in place for personal data that is subject to overseas transfer restrictions.

(d) Data Privacy Contact:

General Counsel
Dealogic Limited
10 Queen St Place
2nd Floor
London
EC4R 1BE
United Kingdom