Dialog Finance PLC

Information Security Clauses

Table of contents

1 Purpose

The purpose of this document (please refer to as Schedule [x] in the legally binding contract) is to establish minimum information security requirements to be followed by any supplier of Dialog Finance as defined in the agreement between Dialog Finance and supplier.

2 Definitions

In this document, the following definitions apply, unless the context otherwise requires:

Terms	Definitions
Dialog Finance PLC (DF) / Dialog Finance	Shall mean and include Dialog Finance PLC and any of its Affiliates.. "Affiliate" means in relation to a party any entity which, directly or indirectly, controls or is controlled by, or is under common control with, that party, where control is the possession, directly or indirectly, of (a) alone or pursuant to an agreement with other members, a majority of the voting rights in it, (b) the power to direct or cause the direction of the management or operating policies of the entity through the exercise of voting rights, contract, trust or otherwise, or (c) a right to appoint or remove the majority of the directors of the entity, and "Affiliates" means any of them.
Dialog Finance Data	Data relating to DF (including financial, operational, supply chain, customer, employee and all other related forms of data) or any supplier of any DF provided or made available to Supplier or any other Supplier Group Company under this Agreement or any Local Service Agreement and shall include all data generated pursuant to this Agreement. For the sake of clarity, Dialog Finance Data includes Confidential Information as defined in the Agreement and Personal Data as defined in this Schedule [x].
Personal Data	Any information provided by or on behalf of Dialog Finance to Supplier relating to an identified or an identifiable natural person ("data subject") being one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity, or as otherwise defined under applicable Data Protection Legislation.
ISO 27001	Means ISO 27001:2013, an information security standard that was published on 25 September 2013, published by the International Organization for Standardization and the International Electrotechnical Commission (as may be updated from time to time);
PCI DSS	Means Payment Card Industry Data Security Standard version 3.2 and / or (as may be amended from time to time); *[Note – Only relevant to suppliers who process payment card information e.g. e-commerce merchants. Delete if not applicable]*
Security Incident	Occurs where (i) Dialog Finance Data is intentionally or unintentionally disclosed to an unauthorized environment or recipient, or (ii) there is an unauthorized access of Dialog Finance Data and/or to Dialog Finance Systems including but not limited to

	applications, services, networks, and /or devices, or there is an attempt to do (i) or (ii).
Dialog Finance Network	All information technology equipment owned or licensed by Dialog Finance, including desktop and laptop computers, telephones, mobile phones, networks, software, email, data and intranet;
Dialog Finance Systems	The software and other electronic, computer and information communications technology devices and equipment owned, supplied, operated and/or developed for Dialog Finance, or its Affiliate and/or any of its Sub-contractors as varied, updated and renewed from time to time including all networks, servers, hosted applications or data centres and any equipment contained therein.
Dialog Finance's Threat & Vulnerability Standard	The controls relating to the management of threats & vulnerabilities that have the potential to disrupt Dialog Finance IT systems and business processes; plus compromise the confidentiality, integrity and availability of Dialog Finance Data.

3 Order of Precedence

In case of a conflict or inconsistency between the provisions of this Schedule and the main terms of the Agreement, the provisions contained in this Schedule shall prevail in relation to the subject matter to the extent of the inconsistency, provided always that nothing in this Schedule shall permit Supplier (or any Subcontractor) to access Dialog Finance Data and/or Dialog Finance Systems in a manner which is prohibited by the Agreement.

4 Standards Compliance

a. Supplier shall have appropriate information security policies, standards and procedures documented which align to industry best practice as set out in the relevant parts of ISO 27001 and ISO 27002 (or any standards replacing and or updating the same).

b. Where Dialog Finance has concerns in relation to the security of the Services or activities of the Supplier's personnel, Supplier agrees to attend review meetings with Dialog Finance to discuss such issues, in the event Dialog Finance requests the removal of any Supplier personnel from providing the services or having access to such services, the Supplier shall immediately comply with such request.

c. Supplier shall continuously assess security risks in relation to their products and services and report promptly any issues identified which may impact the security of Dialog Finance Data or Dialog Finance Systems.

5 Organizational Compliance

The Supplier shall implement, maintain and operate (i) information security policies and standards; and (ii) information security functions and processes, including the publication of such information security policies to ensure compliance with the requirements of this Schedule across the Supplier Group and applicable Subcontractor(s).

6 Governance

The Supplier shall appoint a single point of contact for information security (the "**Supplier Information Security Representative**") The Supplier Information Security Representative must:

a. arrange security governance reviews with Dialog Finance at the agreed frequency, where required by Dialog Finance;

b. clearly communicate points of contact and escalation to ensure priority security concerns are addressed;

c. provide security reports to Dialog Finance across the services at a mutually agreed frequency. These shall provide an executive summary level view, details of areas of concern and supporting remediation and action plans. The format of these reports will be agreed with the Dialog Finance security team.

7 Confidentiality

a. The Supplier shall keep confidential the terms of this Agreement and all information and documentation including information concerning the business or trade secrets, know-how or methods obtained from Dialog Finance in connection with this Agreement both before and after the effective date of the Agreement.

b. The Supplier shall not use any Confidential Information for any purpose other than in complying with its obligations under the Agreement.

c. The Supplier shall not disclose any Confidential Information to any person other than its officers and employees, except to the extent it is necessary for the purpose of performing its obligations under the Agreement.

d. The Confidentiality provisions shall not apply to Confidential Information which:

I. was known to the Supplier (without obligation to keep the same confidential) at the date of its disclosure

II. is after the date of disclosure lawfully acquired by the Supplier in good faith from an independent third party who is not subject to any obligation of confidentiality in respect of such Confidential Information

III. in its entirety was at the time of disclosure or has become public knowledge otherwise than by reason of the Supplier's neglect or breach of the restrictions set out in this Agreement or any other agreement

IV. is independently developed by the Supplier without access to any or all of Dialog Finance’s Confidential Information

V. is required by law, judicial action, governmental department or agency or other regulatory authority to be disclosed in which event the recipient shall take all reasonable steps to consult and consider the reasonable requirements of Dialog Finance in relation to such disclosure.

8 Data Protection

a. Supplier shall collect, store, access, process, transmit Personal Data of Dialog Finance, only if such Personal Data is required for performance of the Services, and subject to prior approval of Dialog Finance if not clearly required for the performance of the Services;

b. Supplier shall collect, store, access, process, transmit Personal Data only to the extent it is strictly necessary for the performance of Services;

c. Supplier shall maintain the original version of, and integrity of, Personal Data, unless otherwise required given the nature of Services required or requested by Dialog Finance;

d. To the extent that the Supplier collects, stores, accesses, transmits, or acts as data processors for Dialog Finance, the Supplier shall, at all times act only in accordance with the Supplier Applicable Laws , rules, regulations, and any written instructions of Dialog Finance that have been communicated to the Supplier provided that any such written instructions by Dialog Finance that requires efforts/expenses beyond those normally invested by Supplier in the provision of its services to Dialog Finance shall be subject to the Parties first agreeing to a change request.

e. Upon Dialog Finance's reasonable request provide regular reports to Dialog Finance regarding its compliance with the provisions of this Agreement (the extent of the content of such report shall be agreed between the Parties or shall otherwise be subject to a change request);

f. The Supplier shall promptly notify Dialog Finance of any notice, enquiry, enforcement proceedings or other correspondence with any Government Official that is pertaining to the Services;

g. The Supplier shall segregate and refrain from co-mingling Dialog Finance's Personal Data with Suppliers own or its customer's, or supplier's information. For such purpose, Supplier storing Dialog Finance Personal Data in separate files/directories from its own or its customer's, or supplier's data shall be considered acceptable.

9 Information System Acquisition, Development and Maintenance

[Only relevant to suppliers who provide software development and / or maintenance services to Dialog Finance. Delete if not applicable]

Supplier shall:

a. employ an effective application management methodology that incorporates information, technical and organizational security measures into the software development process, and ensure that information, technical and organizational security measures, are implemented in a timely manner.\

b. follow standard development procedures, including separation of access and code between production and non-production environments and associated segregation of duties between such environments.

c. ensure internal information security controls for software development are assessed regularly and reflect industry best practices, and revise and implement these controls in a timely manner.

d. manage security of the development process and ensure secure coding practices are implemented and followed, including appropriate cryptographic controls, protections against malicious code, and a peer review process.

e. conduct or arrange for conduction of penetration testing on functionally complete applications, at least once every year and after any significant modifications to source code or configuration.

f. Identify through relevant tools / measures (such as performing static and dynamic application security testing) and remediate any exploitable vulnerabilities prior to deployment / providing the code to Dialog Finance stakeholders for deployment to the production environment.

g. use anonymized or obfuscated (making data difficult / confusing to understand for users of data other than intended parties) data in non-production environments. Never use plain text production data in any non-production environment, and never use Personal Information in non-production environments for any reason. Ensure all test data and accounts are removed prior to production release.

h. Ensure Supplier's Third Parties using open source code, software, applications, or services maintain due diligence in reviewing such resulting code for flaws, bugs, or security issues that may impact data integrity, availability, or confidentiality of Dialog Finance or Dialog Finance's clients.

i. Ensure Supplier Third Parties will not, under any circumstances, share any code created under the Agreement, regardless of the stage of development, in any shared or non-private environment, such as an open access code repository, regardless of password protection.

10 Infrastructure Security & Assurance

a. Supplier shall continuously assess security risks to the Services and report any changes in such risk status, along with a detailed assessment and recommended mitigation controls and actions, without undue delay to the Dialog Finance security team. Any urgent risks to Dialog Finance Data and/or Dialog Finance Systems must be highlighted by the Supplier Information Security Representative to Dialog Finance immediately on identification.

b. Supplier shall procure that Products are tested as follows:

   I. IT and IT related Product elements are tested as per industry standards (such as ISO/IEC 15408, etc.); and
   II. telecommunication infrastructure Products are tested as per industry standards (such as 3GPP (or 3GPP2), etc.).

c. Supplier shall:

   I. ensure that it has documentation which includes a consolidated list of all the security related features in Products it supplies to Dialog Finance; and

II. provide Dialog Finance with a written list (on Dialog Finance's request) of all software, firmware and hardware security related features that are implemented (clearly indicating those that are enabled) in the applicable Product where Supplier installs, support or maintains the applicable Product.

III. provide all documentation in English;

IV. maintain records of those parties involved in the supply chain relating to the Products and provide such records to Dialog Finance on request;

d. During the term of the Agreement, Supplier shall arrange for all testing as detailed in this clause to be undertaken by a mutually agreed industry best practice independent third party ("Third Party") or by Dialog Finance. To the extent that Supplier accesses Dialog Finance Data to provide Services, the security tests referred to in this clause shall include the following:

A. Vulnerability Scanning:

I. Supplier shall permit all scans originating from Dialog Finance's scanner IP address and / or provide its own vulnerability scan reports to Dialog Finance upon request.

II. Upon identification of vulnerabilities on the Supplier' maintained IT Systems, the Supplier will remediate such vulnerabilities in accordance with a mutually agreed remediation schedule. A decision not to remediate any vulnerabilities must be subject to mutual agreement with Dialog Finance.

B. Penetration Testing:

I. Upon notifying the Supplier) either Dialog Finance or the Third Party may perform penetration testing on the Supplier's systems as per mutually agreed frequencies. In the event that the penetration testing conducted discovers vulnerabilities in the Supplier's system, resulting in the Supplier's level of compliance to this Schedule to be unacceptable, Dialog Finance or the Third Party shall be permitted to perform a second penetration test following the remediation of these vulnerabilities focusing on those vulnerabilities discovered from the initial penetration testing.

II. All public facing systems and services including but not limited to applicable web application, database and operating system used for providing Services to Dialog Finance must be penetration tested before going live, and as per mutually agreed frequencies thereafter.

C. Infrastructure and Application Testing:

I. Supplier shall arrange for appropriate infrastructure and application security tests to take place and the scope and frequency of such tests shall be agreed between the Supplier and Dialog Finance in line with the risk profile of the Dialog Finance Systems in scope of the Agreement and documented as a formal testing schedule.

II. Supplier shall also ensure that the underlying infrastructure supporting Dialog Finance is hardened as per industry standards (based on SANS, NIST, CIS,

etc.) where the minimum baseline security standards shall be agreed with Dialog Finance and such hardening is reviewed periodically.

11 Incident Management

The Supplier shall:

a. operate its own documented incident management and investigation processes as updated from time to time

b. formally inform Dialog Finance of any known or suspected Security Incident, that affects, or has the potential to affect, the security of Dialog Finance Data within 24 hours of identification of incident;

c. ensure that all known or suspected Security Incidents are reported while documenting all actions taken to contain, investigate and remediate the Security Incident (including dates, times and individuals involved);

d. ensure it conducts incident handing and investigation on a confidential and 'need to know' basis;

e. provide all reasonable co-operation with any Security Incident investigation by a DF, including (i) making personnel available; (ii) providing data and other information; and (iii) providing subcontractor cooperation; and

f. where requested by Dialog Finance, provide express confirmation to Dialog Finance from its subcontractors acknowledging they must comply with the requirements of this section regarding reporting, managing and investigating Security Incidents.

g. Following any known or suspected Security Incident, Supplier shall notify Dialog Finance within 24 hours of becoming aware of such Security Incident. The Supplier shall investigate and report to Dialog Finance on the cause of the breach, including proposed corrective action within 36 hours of the Security Incident. Dialog Finance shall, where reasonably requested by Supplier (or, if not so requested, at its discretion), provide reasonable co-operation and assistance in connection therewith.

12 Payment Card Information (duty to notify)

[Only relevant to suppliers who process payment card information e.g. e-commerce merchants. Delete if not applicable]

a. Supplier must notify Dialog Finance and/or the relevant DF immediately if it knows or suspects that payment data belonging to Dialog Finance consumers (“Cardholder Data”) held by it, or its Sub-contractors, has been accessed or used other than in accordance with this Agreement (“Unauthorized Use”).

b. Supplier shall promptly provide to Dialog Finance and/or the relevant DF, the full details of the Unauthorized Use (including, without limitation, a breakdown of all information lost if taken) and audit reports of the Unauthorized Use.

c. Supplier shall, at its own cost, prepare and implement, with Dialog Finance, a mitigation plan to rectify any issues arising from Unauthorized Use, including, without limitation, obtaining Dialog Finance's and/or the relevant DF's advance input into and written approval of Supplier's communications to cardholders affected by the Unauthorized Use and providing to, or procuring for, Dialog Finance and/or any DF (and obtaining any waivers necessary to provide or procure) all relevant information to verify their ability to prevent future Unauthorized Use in a manner consistent with the Agreement and this Schedule [x].

d. Supplier must engage, at its sole cost, an independent forensic investigator to conduct a thorough audit of any such Unauthorized Use, or Supplier must provide (and obtain any waivers necessary to provide) to Dialog Finance and/or the relevant DF, its forensic investigators and auditors, on request and at Supplier's sole cost, full cooperation and access to conduct a thorough audit of such Unauthorized Use. Audits conducted by Supplier must include forensic reviews and reports on compliance, as well as any and all information related to the Unauthorized Use and must identify the cause of the Unauthorized Use and confirm whether or not Supplier was in compliance with the PCI DSS at the time of the Unauthorized Use.

e. Without prejudice to the other rights and liabilities under the Agreement, the Supplier indemnifies Dialog Finance and/or any DF for all fraudulent transactions related to such Unauthorized Use and all costs, fees, and expenses, including claims from other third parties and all costs incurred by Dialog Finance and/or any DF as a result of the Unauthorized Use.

13 Access Management

The supplier shall ensure:

a. it validates the identity of any Supplier Personnel (including Subcontractor personnel) authorized to access Dialog Finance Systems/Data - providing, on request by Dialog Finance, their names plus the required and actual levels of access.

b. Supplier personnel have the minimum required system/data access, read and change rights to carry out their duties (with any changes in rights subject to change management). Supplier shall not permit use of shared accounts.

c. access to the Dialog Finance Systems/Data are governed by the security controls set out or derived from Supplier security policies and standards and that breach of these controls policies leads to appropriate personnel disciplinary action.

d. if remote access to Dialog Finance Data and/or Dialog Finance Systems is required, it uses a Dialog Finance approved method, when connecting. Dialog Finance reserves the right to monitor all systems used by Supplier to connect to Dialog Finance networks or access Dialog Finance Data.

14 Asset Management

The Supplier shall in relation to the Services:

a. maintain a secure inventory of all media on which Dialog Finance Data is stored.

b. classify Dialog Finance Data and ensure access is appropriately restricted (e.g. through encryption).

c. impose restrictions on printing Dialog Finance Data and operate secure procedures for disposing of printed materials that contain Dialog Finance Data.

d. ensure Supplier Personnel obtain Supplier authorization prior to storing Dialog Finance Data on portable devices, remotely accessing Dialog Finance Data, transporting or processing Dialog Finance Data outside Supplier's facilities.

15 Security Review

a. Supplier shall permit Dialog Finance personnel, authorized representatives and any party to whom Dialog Finance is legally obliged to provide access or audit rights, to review and assess Supplier's compliance with this Schedule ("Security Review"). Security Reviews may involve access to Supplier controlled premises (including those of Subcontractor(s)), extracting or examining Dialog Finance Data, inspecting security risk management controls and procedures, and interviewing Supplier personnel.

b. Supplier shall permit Dialog Finance authorized representatives to conduct a security assessment to identify, analyze and evaluate the Supplier information security procedures/processes that reduces risks related to confidentiality, availability, and integrity of information in an organization ("Security Assessment") in accordance with the requirements of this clause [x].

c. A Security Review and/or a Security Assessment shall be conducted no more than once per annum, except for instances where there are reasonable grounds to suspect unauthorized use or breaches to the security of Dialog Finance Data and/or Dialog Finance Systems, in which case supplementary Security Reviews may be conducted upon no less than 24 hours advance, written notice

16 Subcontractor(s)

a. Supplier shall not subcontract, assign, or otherwise delegate any of its responsibilities of this Schedule unless agreed with Dialog Finance in writing, in advance. Where Supplier is permitted to subcontract, the Supplier remain Dialog Finance's sole point of contact and responsible for ensuring the Subcontractor comply with this Schedule.

b. Supplier shall ensure that the Sub-contractor complies with and is bound by the requirements of this Schedule [x] as they apply to Supplier. Supplier shall be responsible for all acts and omissions of each of its Subcontractor(s) which shall be treated as if they were the acts or omissions of Supplier itself.

c. Dialog Finance may revoke its prior approval of a Subcontractor (including any approved Subcontractor) where, in Dialog Finance's reasonable opinion, the performance of the Subcontractor is materially inconsistent with the terms of this Schedule.

17 Shared Services

Supplier shall ensure logical separation of (i) Dialog Finance Data from all other data and information held by the Supplier and its Subcontractors; and (ii) the network that processes Dialog Finance Data, including printing facilities, from the Supplier's other networks.

18 Business Continuity Management

a. The Supplier shall have a documented business continuity and disaster recovery plan ("BC DR Plan") to maintain emergency and contingency plans for the facilities in which Supplier information systems that process Dialog Finance Data are located, which shall be tested at least annually. The results of testing along with summary gaps, corrective action plan and timelines for action shall be shared with Dialog Finance.

b. Supplier's redundant storage and procedures for recovering data shall be designed to attempt to reconstruct Dialog Finance Data in its original state from before the time it was lost or destroyed.

19 Obligations on Termination

a. Upon termination or expiry of the Agreement, Supplier shall promptly and securely, within 15 business days of that termination/expiry date, either (as directed by Dialog Finance):

   I. destroy Dialog Finance Data in the Supplier's (including Subcontractors') possession or control. However, Supplier shall retain and properly store during the term of the Agreement and following termination or expiry for at least seven years thereafter, all financial or other information where required by applicable law; or

   II. purge Supplier (and Subcontractor) systems of, and deliver to Dialog Finance, in Dialog Finance's chosen format, on media free of viruses, all copies of Dialog Finance Data in its (including sub-contractors') possession or control;

providing written confirmation of having completed the above (including with respect to its subcontractors) within that timeframe.

b. The Supplier shall also ensure upon such termination or expiry that no Dialog Finance asset is retained by the Supplier or any subcontractor, unless approved by Dialog Finance in writing.

c. In the case of termination or expiry of a purchase order, statement of work or equivalent (an 'order') the above requirements of this section shall apply to all Confidential Information, assets, desktops and servers specific to that order.

End of document.