

Managed Hosting

G-CLOUD 15 – TERMS AND CONDITIONS





Contents

1.	The Service – Overview	2
2.	Service Term Structure	3
3.	General Conditions on the Buyer	3
4.	Fixed Services Conditions on the Buyer	5
5.	Service Specific Conditions of Use	7
6.	Data Protection	15
7.	Service Level Agreement	17
8.	General Definitions	23

1. The Service – Overview

- 1.1** The Managed Hosting Service (the “Managed Hosting Service”) is a set of data storage and hosting services, which are split into discrete modules. Supplier provides the Service by combining different modules to form a Buyer Solution. The term “Service” or “Services” in these Service Specific Terms means the Private Cloud & Managed Hosting Service and which means the Buyer Solution and includes each Service Element.



1.2 The term “**Service**” or “**Services**” in these Service Specific Terms means the Managed Hosting Service.

2. Service Term Structure

2.1 These Service Terms form part of the Call-Off Contract entered into under the G Cloud 15 Framework.

2.2 The Call-Off Contract comprises the Call-Off Order Form, the Supplier’s Service Terms, Service Definition and Pricing Document, and the applicable Call-Off Terms and Conditions.

2.3 These Service Terms describe how the Service operates and apply in conjunction with the Call-Off Contract.

2.4 In the event of any conflict or inconsistency between these Service Terms and the Call-Off Contract, the Call-Off Contract shall prevail.

3. General Conditions on the Buyer

The Service is available to Buyers that meet and agree the following criteria:

3.1 Additional Service Recipient:

3.1.1. If Buyer wishes to add an Additional Service Recipient, then Buyer shall:

- (a) provide the full corporate details of the Additional Service Recipient;
- (b) seek approval in writing from Supplier;
- (c) inform the Additional Service Recipient of the contractual arrangements; and
- (d) agree to pay such additional Charges as Supplier may reasonably request in relation to the approval of such requests.

3.2 Authorised Users: Access by Buyer to the Services and Equipment is limited to authorised Users. Buyer is responsible for ensuring Users’ compliance with this Agreement.

3.2.1. If Supplier provides each authorised User with User Details, Buyer is responsible for:

- (a) the security of User Details; and
- (b) providing Supplier with the identity of the authorised Users and keeping that information current.

3.2.2. Supplier accepts no liability for any unauthorised or improper use or disclosure of any User Details. Buyer is liable for all acts and omissions relating to the User Details up until the time that it informs Supplier that they are being used without authority or may be compromised.

3.3 AUP: Buyer shall comply with the AUP in using the Services.

3.4 Third Parties: Buyer shall ensure that the Users and all Additional Service Recipients (if any) comply with this Agreement in relation to their use of the Services and Equipment and shall be liable to Supplier for the acts and omissions of the Users and all Additional Service Recipients (if any) in relation to this Agreement. Save as expressly permitted under this Agreement, Buyer shall not resell, distribute, provide or sub-licence the Services or Equipment (except Buyer Equipment) to any third party.

3.5 Terms of Use: Buyer shall not:

- (a) make unauthorised modifications to the Services;
- (b) use the Services as a means to establish permanent servers, relay connections or interconnection services or any similar commercial activities;
- (c) do anything that causes the Network to be impaired;
- (d) use automated means to make calls and/or texts or to send data (including via a GSM Gateway), unless expressly authorised in this Agreement;
- (e) use the Services in a way that:
 - (i) may reasonably be considered to be a nuisance, defamatory, offensive, abusive, obscene or in violation of any person’s rights; or
 - (ii) is illegal, fraudulent or contrary to good faith or commercial practice to Supplier’s detriment; or
- (f) use the Supplier’s SMS service to send mass notification messages, or mass marketing messages, whether or not the messages are unsolicited unless expressly authorised in this Agreement.



- 3.6 Service Monitoring:** Buyer gives express consent for Supplier to monitor Buyer's use of the Service (and disclosing and otherwise using the information obtained) to the extent allowed by Applicable Law to:
- (a) comply with Applicable Law;
 - (b) protect the Network from misuse;
 - (c) protect the integrity of the public internet and/or Supplier's systems and Networks;
 - (d) determine if Buyer has breached any conditions or restrictions on use of the Service;
 - (e) provide the Service; and/or
 - (f) take any other actions agreed or requested by Buyer.
- 3.7 Compatibility:** Buyer shall ensure its systems, equipment and processes satisfy any Technical Prerequisites and if required to be used in conjunction with the Equipment and/or the Services, are in good working order (if applicable) and are compatible for use with the Equipment and/or the Services. Supplier shall use reasonable endeavours to advise Buyer of relevant requirements on request, but in no event shall Supplier be responsible for any performance or non-performance issues with the Equipment and/or the Services, or liable to support the Equipment and/or the Services, if Buyer's systems, equipment, or processes fail to satisfy the Technical Prerequisites or are otherwise incompatible with the Equipment and/or the Services. Supplier may suspend the provision of any Service for which Technical Prerequisites have not been procured within the specified period and charge Buyer any applicable Recovery Charge.
- 3.8 Security and Misuse:** Buyer shall take reasonable steps in line with commercial good practice with entities it controls to limit misuse of or threat to the Service or Network; and address any misuse or threat identified by Supplier through the implementation of appropriate security or user controls. Buyer shall not run any security tests, vulnerability scans or penetration tests on Supplier Equipment or Services without Supplier's prior written approval.
- 3.9 Unauthorised Equipment or Repairs:** Buyer acknowledges that:
- (a) Equipment or Buyer Equipment not authorised for use on the Network; or
 - (b) any unauthorised attempt to repair or tamper with the Equipment,
- may result in an impaired User experience and/or invalidate the manufacturer's warranty.
- 3.10 End of Life**
- 3.10.1. Notification:** Where Equipment is End of Life, Supplier may, on provision of reasonable notice:
- (a) retire the Equipment; and/or
 - (b) provide the Buyer with an option of replacement Equipment which provides equivalent or improved functionality to the extent that alternatives are available.
- 3.10.2. Replacement:** Where End of Life Equipment is replaced in accordance with clause 3.10.1 (Notification), the costs of such replacement shall be charged to Buyer a One-Off Charge and invoiced accordingly.
- 3.10.3. Continued Use:** Where, following receipt of an End of Life notification in accordance with this clause, Buyer continues to use End of Life Equipment, or does not use its best endeavours to allow Supplier to replace the End Of Life Equipment, Supplier:
- (a) shall have no maintenance obligations for the End of Life Equipment;
 - (b) shall not be liable for Buyer's use of the End of Life Equipment;
 - (c) shall not be liable for any service levels relating to the Equipment; and
 - (d) reserves the right to suspend all or part of the affected service.
- 3.11 Buyer Equipment:** Where Buyer provides Buyer Equipment for use with a Service, Buyer shall (and Buyer acknowledges that failure to do so will excuse Supplier from liability for failure to deliver the Service):
- (a) install and configure the Buyer Equipment at Buyer Sites by the date necessary to allow Supplier to perform its obligations;
 - (b) maintain the Buyer Equipment to Supplier's satisfaction, including prompt installation of security patches and updates;
 - (c) immediately replace any Buyer Equipment which is declared by its manufacturer as end-of-life (or otherwise stops marketing, selling or supporting it) and notify Supplier of any such replacement;



- (d) promptly after the Service terminates, give Supplier access to and reasonable help with disconnecting Buyer Equipment from the Service; and
- (e) warrant and undertake that Buyer has full authority to permit Supplier to perform the Service using the Buyer Equipment.

3.12 Exclusions:

- 3.12.1. Supplier does not guarantee that the Services will be continuously available and/or fault-free and Buyer acknowledges that faults may occur from time to time. This acknowledgement is without prejudice to any specific service levels agreed between the Parties in this Agreement.
- 3.12.2. Buyer is responsible for satisfying itself that the Services and any Equipment are suitable for its intended purpose and requirements (including but not limited to any resiliency and/or business continuity requirements). Supplier does not warrant or represent that the Services and Equipment are or will be fit for Buyer's intended purpose and requirements. Supplier recommends that Buyer obtains business continuity (or other) insurance that is appropriate for the nature of its business.
- 3.12.3. Supplier is not responsible for any content, goods or services which are accessed, downloaded or transmitted by Buyer through use of the Services. Supplier accepts no responsibility for any such content, goods or services. Buyer shall take appropriate measures to back up data and otherwise protect against loss of data under this Agreement.
- 3.12.4. Buyer acknowledges that the Service is not intended for use by Consumers in the European Union. Without prejudice to the foregoing, the Buyer shall immediately notify Supplier if it becomes aware that anyone other than Supplier has made available, or intends to make available, the Service to a Consumer in the European Union.

3.13 Termination: Where Buyer terminates the Call-Off Contract during the Call-Off Contract Period, the Buyer agrees to pay Supplier's reasonable, committed and unavoidable losses resulting from the termination of the Call-Off Contract.

3.14 Network Sunset

3.14.1. Buyer hereby acknowledges and accepts that:

- (a) certain Network technologies used to provide the Service on Supplier Equipment or Buyer Equipment may retire prior to the expiry of the contract; and/or
- (b) current Networks may be replaced by further advanced Network technologies during the term of the Call-Off Contract.

3.14.2. As a result, Buyer agrees that maintaining compatibility of its devices with the available Networks from time to time shall be its responsibility.

3.15 Planned Service Changes by Third-Party Providers: Supplier has been informed that BT Openreach (the "Third-Party Provider") for legacy PSTN is withdrawing the service, with full switch off expected to be complete by 31 January 2027. Supplier is entitled to move the Buyer from legacy PSTN to Ethernet Access Method as and when required. Buyer will be advised of an alternative Service Element and the associated Charges, as set out in these Service Terms below. Buyer will have the option to either order an alternative Service Element or to cancel the affected Service Element only in accordance with the terms of these Service Terms and Call-Off Contract.

3.16 Interpretation: In this Agreement, unless the context otherwise requires, words in the singular include the plural and vice versa.

3.17 Format: If Buyer requires this Agreement (or any bills, communications or a document referred to in this Agreement) in a different format, call 03333 043 222 or email disability.access@vodafone.co.uk for a large print, braille version, dyslexia-friendly or audio CD version. These contact details are for accessibility **help** only.

4. Fixed Services Conditions on the Buyer

4.1 Service Commencement Date: Buyer shall notify Supplier within 5 Working Days of the Service Commencement Date if, in the Buyer's reasonable opinion, the Services do not conform to the standard testing criteria and provide sufficient supporting details. Upon receipt of Buyer's notification, Supplier shall take reasonable action to meet the standard testing criteria.

4.2 Supplier-Owned Equipment: The following will apply where Supplier provides Fixed Equipment for Buyer's use with a Service:

4.2.1. **Title:** Title to the Fixed Equipment at all times belongs to Supplier, its suppliers or subcontractors (subject only to any rights which may be granted to Buyer in respect of Supplier Software, as set out in these Service Terms).

4.2.2. **Buyer Obligations:**

4.2.3.1 Buyer agrees to:



- (a) provide secure storage for Fixed Equipment that is sent to Buyer Sites prior to installation;
- (b) use the Fixed Equipment only for the purpose of using the Services, in accordance with Supplier's instructions and Applicable Law;
- (c) allow only Supplier's authorised representatives to add to, move, modify, inspect, test or alter the Fixed Equipment (either on Buyer Site or remotely);
- (d) adequately insure for, and notify Supplier immediately of loss, breach or suspected breach or damage to the Fixed Equipment;
- (e) only connect the Fixed Equipment to the Network using a network termination point that has been approved in advance by Supplier;
- (f) provide Supplier with:
 - (i) adequate power supply, connection, and space for the operation of the Fixed Equipment at Buyer Sites; and
 - (ii) in the case of BPE patch cords and cabling; and
 - (iii) 10 Supplier Working Days' notice of any known disruptive event (such as power disconnection).

4.2.3.2 Additionally, specifically in relation to BPE, Buyer shall:

- (g) appoint a local security representative to ensure the physical security of the BPE who will grant access by approved authorised personnel only and conduct routine physical checks, including ensuring tamper evident labels remain intact; and
- (h) ensure that the physical environment in which the BPE is housed is appropriate for the protective marking of the data being transmitted through such Fixed Equipment. In particular:
- (i) BPE must be located in a communications room or other isolated area that is suitable to limit the occurrence of accidental or malicious damage to the BPE; and
- (ii) if the BPE is located in a shared environment, then it must be kept in a dedicated locked cabinet or rack. If that is not possible, robust access control mechanisms must be implemented by Buyer, with access only available with prior approval from Buyer's local security representative.

4.2.3. **Buyer Equipment:** Where Buyer provides Buyer Equipment for use with a Service Buyer shall (and Buyer acknowledges that failure to do so will excuse Supplier from liability for failure to deliver the Service), Buyer shall:

- (a) install and configure the Buyer Equipment at the Buyer Sites by the date necessary to allow Supplier to perform its obligations;
- (b) Maintain the Buyer Equipment including prompt installation of security patches and updates;
- (c) Promptly after the Service terminates, give Supplier access to, and reasonable help with, disconnecting Buyer Equipment from the Service; and
- (d) Warrant and undertake that Buyer has full authority to permit Supplier to perform the Services using the Buyer Equipment.

4.3 Buyer Sites: For the purposes of preparing for and delivery of the Services, Buyer shall:

- (a) carry out, or permit Supplier or its subcontractors to conduct, a Site Survey;
- (b) prepare the Buyer Site for the Services in accordance with Supplier's instructions;
- (c) allow and/or have in place (or assist Supplier to do so at Buyer's cost) all third-party consents necessary to allow Supplier or its subcontractors and agents (and obtain consents from third parties to allow) to:
 - (i) access the Buyer Sites, and any Buyer Equipment, Fixed Equipment or Equipment, and third-party property located there, as Supplier reasonably requires to perform its obligations under this Agreement (including for the purposes of installing and uninstalling Equipment (whether in the Buyer Sites or outside) and providing and preparing for the provision of, the Services) and including access outside Working Hours; and
 - (ii) ensure that Buyer Sites are safe and have a suitable working environment.

4.4 Emergency Services:

4.4.1. **General:** In the event of a power cut or failure affecting Buyer's fixed line and/or broadband Service, and/or a failure of the internet connection on which the Service relies, Buyer may not be able to make calls including calls to emergency services. This may also affect any calls using the internet including calls to emergency services.

4.4.2. **Buyer Obligations:** Buyer shall:

- (a) provide Supplier with complete and accurate Buyer Site address information; and



- (b) give Supplier at least 30 days' written notice of any change to the location of any Fixed Equipment and to any change to the relevant Buyer Site address information.

4.4.2.1 Buyer acknowledges that any failure to provide the information required in 4.4.2 may render emergency services unable to identify User's location.

4.5 Calls Using the Internet: Where a Service places calls using the internet, Buyer shall:

- 4.5.1. Make Users accessing the Service via a soft client aware that Supplier may be unable to automatically determine their location if they make an emergency services call using the Services.
- 4.5.2. Ensure that such Users provide their location details in the event that they make an emergency services call using the Services. In the event of a power failure, the emergency call placed will be routed over the Network and not through the Service.
- 4.5.3. Provide a registered address where a Buyer or User will make calls over the internet including if there are multiple addresses where such calls will be made and keep information on all such locations up to date.

4.6 Survey: These Service Terms and each Service Element are subject to survey. In the event a Site Survey output results in an increased price from the Call-Off Contract, the Buyer has the right to cancel the affected Service Element only in accordance with the terms of this Service Offer and the Call-Off Contract.

4.7 Third-Party Costs: Unless otherwise agreed and stated in the Buyer's Call-Off Contract, the Buyer will be liable for any additional costs charged to Supplier by third parties in connection with the provision of the Services. Such Charges (often referred to as Excess Construction Charges) are detailed in the Professional Services section of these Service Terms. These Charges will be notified to the Buyer before any construction works take place. In the event this results an increased price from the Call-Off Contract, the Buyer has the right to cancel the affected Service Element only in accordance with the terms of these Service Terms and Call-Off Contract.

5. Service Specific Conditions of Use

5.1 Commencement and Delivery

5.1.1. **ARFS Date and Handover Date:** Supplier will advise Buyer of the Agreed Ready for Service Date ("ARFS Date") following acceptance of the Buyer's Order.

5.1.2. Supplier reserves the right to revise the ARFS Date if:

- (a) Buyer has requested changes to the Buyer Solution or to Buyer's Order;
- (b) any changes have been made to Supplier's programme for delivery of the Buyer Solution; or
- (c) Buyer delays in providing or fails to provide reasonable assistance requested by Supplier.

5.1.3. Supplier will use reasonable endeavours to hand over the entire Buyer Solution to Buyer for Acceptance Testing by the ARFS Date.

5.1.4. If the Handover Date is not on or before the ARFS Date, Supplier will:

- (a) use reasonable endeavours to hand over the Buyer Solution to the Buyer as soon as reasonably practicable after the ARFS Date; and
- (b) escalate within Supplier the factors causing the delay to attempt to resolve the problem and expedite the handover of the Buyer Solution.

5.2 Acceptance: The Acceptance Testing Period begins on the Handover Date.

5.2.1. During the Acceptance Testing Period Buyer has the opportunity to test whether or not the Buyer Solution achieves the Acceptance Criteria.

5.2.2. Buyer must notify Supplier before the expiry of the Acceptance Testing Period whether or not the Buyer Solution or any part of it achieves the Acceptance Criteria.

5.2.3. If, before the expiry of the Acceptance Testing Period, either:

- (a) Buyer does not tell Supplier whether or not the Acceptance Criteria has been achieved; or
- (b) Buyer starts using the Buyer Solution for purposes other than Acceptance Testing; then the Buyer Solution will be deemed to have been Accepted.

5.2.4. In these circumstances the Acceptance Date is the earlier of the date of the expiry of the Acceptance Testing Period or the first date of use for purposes other than Acceptance Testing. If Buyer notifies Supplier before the expiry of the Acceptance Testing Period, that the Buyer Solution or any part of it has not achieved the Acceptance Criteria then the Buyer must provide Supplier with evidence of



such failure. Supplier will then test the relevant Service Element themselves and the Buyer will provide Supplier with reasonable assistance as Supplier requests.

- 5.2.5. If Supplier agrees that the Buyer Solution has not achieved the Acceptance Criteria, then Supplier will use reasonable endeavours to correct it. Supplier will hand the Buyer Solution back to Buyer for a further Acceptance Testing Period once Supplier believes that the cause of the previous failure has been corrected.
- 5.2.6. Buyer is not entitled to withhold Acceptance on the basis of minor defects or defects that cannot be repeated by Supplier. Buyer may not unreasonably withhold or delay Acceptance. If minor defects exist, then the Buyer Solution will be Accepted and Supplier will use reasonable endeavours to correct those defects within a reasonable period following the Acceptance Date.

5.3 The Service and Equipment

- 5.3.1. The Service comprises required core Service Elements and may also include optional Service Elements (detailed below and in the Extra Service Terms) selected by Buyer both of which shall be set out in the Order. Certain Service Elements may also depend upon other specific Service Elements that Buyer must purchase as part of the Buyer Solution.
- 5.3.2. In connection with the Service, Buyer may purchase optional Service Elements including:
 - (a) Network Services;
 - (b) Infrastructure Services including Monitoring and Reporting Services;
 - (c) Operating System Services;
 - (d) Private Cloud Self Service Portal access;
 - (e) Private Cloud Disaster Recovery & Rapid Restore;
 - (f) Database Management Services;
 - (g) Procurement Services; Software Patching and Updates;
 - (h) Anti-Virus Service;
 - (i) Security Services;
 - (j) Shared Backup & Storage Services;
 - (k) Dedicated Backup & Storage Services;
 - (l) Professional Services; Email Protection Services;
 - (m) Managed Cloud Tiering Appliance Services; and
 - (n) Managed Cloud Storage Gateway.
- 5.3.3. Service Elements are available from a number of different Cloud & Hosting Centres. Service availability depends on location and Supplier will notify Buyer which Cloud & Hosting Centre(s) will be used for delivery of the Buyer Solution.
- 5.3.4. Supplier may store backups of the management services referenced in these Service Terms in a Cloud & Hosting Centre in a country different to that from where the management services are being delivered.
- 5.3.5. Fixed Equipment relevant to this Service if applicable will be set out in the Order. The Order will identify which Fixed Equipment, if any, Supplier will supply to the Buyer and which of such Equipment will be purchased by Buyer. Associated Charges shall be set out in the Order.
- 5.3.6. If any other Buyer Equipment is required for use of the Service, it will be identified in the Order.

5.4 Equipment and Software Lifecycle Management:

- 5.4.1. Supplier will provide Equipment Maintenance Services and Software Maintenance Services for any Fixed Equipment specifically notified to Buyer as having Equipment Maintenance Services or Software Maintenance Services available.
- 5.4.2. If Software Maintenance Services no longer applies to a piece of Software after the expiry of the Minimum Term (or when Supplier has deemed the Software has reached the end of its useful life), then the Buyer may continue to use the Software entirely at their own risk. Supplier will no longer be responsible for Software Maintenance Services in respect of that Software and any Service Levels impacted by that Software will no longer apply.



- 5.4.3. Subject to sub clause 5.4.4, Supplier shall cease to be responsible for providing the Equipment Maintenance Services or Software Maintenance Services (as applicable) if any of the following occur:
- (a) the limited availability of replacement Equipment or Software;
 - (b) the Equipment or Software reaching an end of support date with the relevant manufacturer; or
 - (c) the Equipment being deemed by Supplier to be beyond economic repair for any other reason.
- 5.4.4. If Supplier has agreed to have management responsibility in respect of Fixed Equipment, then Supplier shall still use reasonable efforts to maintain the Supplier Equipment during the Minimum Term notwithstanding the occurrence of any of the events listed in sub clause 5.4.3.
- 5.4.5. **The Buyer agrees that:**
- (a) it is the Buyer's responsibility to dispose of (including paying for the disposal of) Buyer Equipment at the end of its useful life in accordance with all Applicable Laws and regulations;
 - (b) where the Buyer does not comply within three months of being requested to do so and the Buyer Equipment remains on Supplier's premises, Supplier reserves the right to dispose of any Buyer Equipment, and charge the Buyer in respect of any reasonable costs Supplier incurs in doing so;
 - (c) any Buyer Equipment provided by the Buyer will be assessed by Supplier to determine if it is fit for purpose and supportable prior to any service commencement. Supplier reserves the right, acting reasonably and having discussed the matter in advance with the Buyer, to refuse to support Buyer Equipment provided by the Buyer which Supplier determine as either not fit for purpose or not supportable; and
 - (d) the Buyer will notify Supplier of any changes the Buyer makes to the Equipment or Software that may impact the Buyer Solution.
- 5.4.6. If Buyer purchases Supplier Equipment and/or Supplier Software that no longer benefits from Equipment Maintenance Services and/or Software Maintenance Service, Buyer acknowledges that the Buyer will not be able to use such Equipment and/or Supplier Software in respect of that Service Element.
- 5.4.7. **Changes:** Buyer is responsible for all Buyers costs, migration of Buyer data and updating of Buyer's systems as a result of any change.
- 5.4.8. **PSTN connection:** Unless it is otherwise permitted by Applicable Law, Buyer and its Users must not
- (a) connect or seek to connect the Service to the public switched telecommunications network ("PSTN") or other fixed voice services (e.g., voice over IP);
 - (b) connect to the public Internet; and/or
 - (c) use the public internet for voice communications services, Buyer will indemnify Supplier for any liability associated with Buyer's impermissible use of the Service.
- 5.4.9. **Software patching, Updates and Anti-Virus:** Where Buyer has ordered the Operating System Services and the Database Services:
- (a) Supplier will not automatically apply any patches, fixes and/or workarounds to the operating system or anti-virus software without the Buyer's agreement except in the event of significant risk to the Buyer, Supplier or any of Supplier's customers. Supplier will use reasonable endeavours to test and communicate the changes to the Buyer. If the risk to Supplier or any of Supplier's customers may not be mitigated by other means, the Buyer may not refuse the change; and
 - (b) Buyer agrees to be responsible for testing to ensure that any applications running within the operating system that are managed by Buyer function correctly after Supplier applies any operating system patches. Buyer must notify Supplier promptly of any faults or problems with any applications. Supplier will not be liable for any costs, loss or damage incurred by Buyer as a result of Buyer's delay or failure to comply with the obligations set out in this clause.
- 5.4.10. **Malware, Viruses and Data:** Supplier assumes no liability for viruses or other malware introduced by Buyer, or for restoration of lost or corrupted data or applications, other than restoration from then-current backups maintained by Supplier if Buyer chooses optional backup and/or archival services (which Supplier recommends).
- 5.4.11. **Loading of Buyer Data and software:** Loading of Buyer data and software is entirely at Buyer's risk. Supplier recommends that all data transmissions to Buyer's servers be encrypted. Supplier has no responsibility or liability for Buyer's transmissions of data. The Service is not intended for and Buyer shall not use the Services to store, transmit or process data for any applications or uses that are prohibited by this Agreement or the AUP.



5.4.12. Data Security and Internet Transmission Buyer acknowledges that the public internet is an inherently insecure environment. The use of the public internet is at the sole risk of Buyer and its Users. Supplier is relieved from all liability in connection with Buyer's and its Users' use of the public internet including liability for any disclosure of Confidential Information transmitted over the public internet.

5.4.13. Email Protection:

- (a) For the avoidance of doubt, the Email Protection Services are not designed to detect phishing emails, a business email compromise (Bec) attack, or such other email borne attack for which the Service is not designed to detect as at the date of these Service Specific Terms and therefore Supplier accepts no liability for any damage or loss resulting directly or indirectly from any failure to detect such attacks.
- (b) No email-protection service can guarantee a 100% detection rate and, therefore, Supplier accepts no liability for any damage or loss resulting directly or indirectly from any failure of the Service to detect viruses, spam or a pornographic image, or for wrongly identifying an email suspected as being infected, spam or containing pornographic images which proves subsequently not to be so.
- (c) Configuration of Email Protection Services (Content Control) is entirely under the control of the Buyer and that the accuracy of such configuration will determine the accuracy of the Content Control service, therefore, Supplier can accept no liability for any damage or loss resulting directly or indirectly from any failure of the Service to detect or wrongly identify an email containing suspected content which proves subsequently not to be so.

5.4.14. General obligations: Buyer must not:

- (a) reverse assemble, reverse compile, otherwise translate, or reverse engineer the Service unless expressly permitted by Applicable Law;
- (b) use the Service Elements, Devices, files, modules, audio-visual content, or related licensed materials separately from the Service;
- (c) use the Services for any content that requires
 - (i) additional Supplier commitments to meet regulatory requirements; or
 - (ii) security measures beyond those provided by Supplier.

5.4.15. Buyer will implement policies, procedures and controls sufficient to fulfil its obligations under this Agreement.

5.4.16. Buyer must:

- (a) ensure all necessary permissions for each Party respectively to use, provide, store and process Buyer data with the Service are obtained.
- (b) nominate a Buyer representative who is able to make financial and contractual decisions relating to the User requirements;
- (c) carry out the tasks allocated to the Buyer under the project plan agreed with the Buyer representative;
- (d) give Supplier (and any Third Party Provider) access to Software and Equipment at reasonable times in accordance with Buyer's normal security procedures to enable Supplier to provide support and/or carry out replacements or repairs in the event of any Service failure;
- (e) ensure that Buyer's systems comply with all pre-requisites for supply of the Service reasonably notified to the Buyer in advance by Supplier;
- (f) complete, return and keep current an authorised contact sheet;
- (g) provide, maintain and regularly review a security policy that covers all Buyer data, applications and systems including those in a Cloud & Hosting Centre;
- (h) control the internal access to key servers and information;
- (i) provide and monitor the internet access of its employees;
- (j) monitor and scan their network and be responsible for application security.
- (k) ensure that the Buyer Solution is protected by one or more of Supplier's managed firewalls
- (l) comply with any other obligations as reasonably notified to the Buyer by Supplier from time to time.

5.4.17. Buyer must get Supplier's written consent prior to carrying out scans of the Supplier Network and Cloud & Hosting Centre.

5.4.18. Supplier may suspend a Buyer Solution or Service Element if the Buyer is subject to a distributed denial of service attack and does not take the "DDoS Mitigation" Service Element from Supplier. Supplier reserves the right to suspend the impacted Service in order



to protect Supplier, Supplier's customers and the wider Internet community. Supplier will notify the Buyer as soon as reasonably practical and seek to reinstate the suspended Service when able.

5.4.19. Relocation

- (a) Supplier may require:
 - (i) Buyer Equipment located in a Data Centre or;
 - (ii) Buyer hosted data in a specific Data Centre specified in the Agreement to be relocated. Such relocation may be within the same Data Centre or to another Data Centre.

5.4.20. Supplier Obligations: In relation to a request under clause 5.4.19, Supplier shall:

- (a) provide no less than three months' notice to the Buyer; and
- (b) pay all pre-agreed reasonable costs and expenses incurred in connection with such relocation of the Buyer Equipment if the Buyer is within the Minimum Term for the affected element of the Service.
- (c) Supplier will, when specifying the timescale for any relocation of the Buyer Equipment or hosted data, use reasonable endeavours to consult with the Buyer to minimise the disruption to the Service.
- (d) Buyer Obligations: Buyer shall cooperate with Supplier requests under this clause in a timely fashion.

5.5 Service Change Request Procedure

5.5.1. Either Party may propose a change to the Service by written request. Upon agreement, the Parties must authorise the change in the form of a change Order or other written amendment to the Agreement (a "Change Order"). Supplier has no obligation to commence work in connection with a change until a Change Order is executed by the Parties.

5.5.2. If within 5 Working Days of the end of a calendar month Buyer request any change which would have the effect of cancelling the whole or any part a Service Element, Buyer may be charged the applicable charges in relation to that Service Element for the full coming month, as determined by Supplier.

5.6 The Network Services: Buyer may order connectivity via the Cloud & Hosting Internet Access service to give Buyer connectivity from Buyer Solution to either the Vodafone Network or to shared Vodafone platforms.

5.7 Operating System Services:

5.7.1. The Operating System Services provide the installation, management, maintenance and support of operating systems running on the Servers included in Buyer Solution. The service options include (i) Buyer Managed Operating System where Buyer takes responsibility for managing the operating system (ii) OS Management which provides for the installation and configuration of the selected operating system on the Servers; backup and restoration of the operating system (excluding Buyer's applications and Buyer's data) by Supplier; and (iii) Web Server Application Management where Supplier provides support to the web Server application in addition to the operating system.

5.7.2. **Conditions of Use:** In order for Supplier to be able to provide the Operating System Services, Buyer agrees that:

- (a) after initial installation of the operating systems, installation of any Buyer Software on a Server by Supplier must be requested as a configuration change;
- (b) any enhancements, upgrades or other modifications to any Buyer Software installed on the Server by Buyer must be requested as a configuration change;
- (c) Supplier reserves the right to charge Buyer for any work that has to be carried out by Supplier as a result of any enhancement, upgrade or other modification made to Buyer's software (including the installation of Buyer Software) by Buyer;
- (d) they will ensure any remote Equipment used to access a Server to modify or upload content or for other similar purposes has a static IP address;
- (e) Supplier will retain root or administrative access to each Server covered by the OS Management service;
- (f) in order to receive the OS Management service, Buyer must purchase the Monitoring and Reporting Service for each Server for which the OS Management service is provided;
- (g) paragraphs 5.7.2 (a), (b), (d) and (e) shall not apply where the Buyer Managed Operating System Service is ordered; and



- (h) the Buyer Managed Operating System Service will be considered Accepted when Supplier are able to demonstrate that the Supplier managed server is ready to have the Buyer Managed Operating System installed on it by the Buyer.

5.8 Private Cloud Self Service Portal Services:

5.8.1. The Private Cloud Self Service Portal allows Buyer to manage Automated Service Requests via a compatible web browser.

5.8.2. **Conditions of Use:** Where Buyer makes a request through an Automated Service Request:

- (a) resource used to process and complete an Automated Service Request will not be counted in the calculation for Inclusive Resource for Change; and
- (b) the service or output resulting from an Automated Service Request will not be eligible for Early Life Support and will be considered automatically Accepted unless Supplier are notified of a non-minor defect.

5.8.3. **Private Cloud Disaster Recovery & Rapid Restore:** Supplier provides two key recovery services capabilities which only apply to private cloud and do not apply to a Buyer Solution which is a managed hosting solution.

5.8.4. “Disaster Recovery” provides Buyers with the ability to failover a single Virtual Machine or groups of Virtual Machines from a private cloud platform in a source (primary) Cloud & Hosting Centre to a private cloud platform in a target (secondary) Cloud & Hosting Centre in the event that the private cloud platform at the primary Cloud & Hosting Centre becomes unusable.

5.8.5. “Rapid Restore” offers the ability to restore a Virtual Machine back to a selected data recovery point whilst retaining the attributes of that failed Virtual Machine.

5.8.6. **Conditions of Use:**

- (a) Supplier will ensure that the necessary data replication agents and supporting Supplier management infrastructure is in place for Buyer to be able to enable recovery services.
- (b) Buyer must have:
 - (i) the required storage compute capacity in place on the private cloud platform at the secondary Cloud & Hosting Centre in order to support the event of a Disaster Recovery failover taking place;
 - (ii) a suitable back-up system in place to protect their environment and data separate from the recovery services that are available. The replication technologies used to deliver recovery services will not protect from virus infection, or other types of data corruption nor loss that could occur in the location of Buyers primary private cloud platform; and
 - (iii) connectivity in order to replicate data between the private cloud platform in the source (primary) Cloud & Hosting Centre to Buyers private cloud platform in a target (secondary) Cloud & Hosting Centre.
- (c) Buyer is responsible for:
 - (i) re-instating applications post completion of a Disaster Recovery failover or the execution of a Rapid Restore request; and
 - (ii) ensuring that there is enough capacity at their site to store the replicated data created through Disaster Recovery and Rapid Restore services
- (d) Supplier is not responsible for any failure of Disaster Recovery and/or Rapid Restore which result from a failure in related or dependent services not provided by Supplier.

5.9 Database Management Services:

5.9.1. The Database Management Services provides provisioning, management, monitoring, diagnostics and support of Buyers database

5.9.2. **Conditions of Use:** In order to receive the Database Management Services, Buyer must order:

- (a) the Backup Services that includes database backup for each Server for which the Database Management Services is provided and;
- (b) the OS Management service for all Servers on which the Database Management Services is to be delivered.

5.9.3. **Monitoring and Reporting Services:** The Monitoring and Reporting Services provides installation, management and support of a variety of monitoring services to support other cloud & hosting Service Elements, such as the OS Management Service, or used on its own.

5.9.4. **Non-Agent Based Monitoring** is an infrastructure and system monitoring service including ping monitoring and TCP monitoring, which is provided over an IP network and without the need for any Agents to be installed on Buyer’s monitored Device(s).



- 5.9.5. **Agent Based OS Monitoring** provides a monitoring service over an IP network requiring a dedicated Agent to be installed on the Devices hosted at Supplier's Cloud & Hosting Centres.
- 5.9.6. **Conditions of Use:** In order for Supplier to be able to provide the Non-Agent Based Monitoring Service Buyer agrees:
- (a) that Supplier will need to work with Buyer in order to design certain protocols that will facilitate the Non-Agent Based Monitoring service;
 - (b) that Buyer will not request or implement a change to Buyer Solution which would result in Buyer Solution not allowing data to be packaged using the protocols specified by Supplier and;
 - (c) data packaged using these protocols must be able to be transferred between Buyer's monitored Device(s) and the Supplier Monitoring Infrastructure.
 - (d) that Supplier will retain exclusive root or administrative access to every Agent on a monitored operating system; and
 - (e) to provide Supplier with all rights on the monitored operating system that are required to enable Supplier to provide the Agent Based OS Monitoring service.
- 5.9.7. Unexpected events detected by the Monitoring and Report Services will cause an Incident to be created and this Incident will be escalated to the Cloud & Hosting Service Desk. The Cloud & Hosting Service Desk will then
- (a) where only the Monitoring and Reporting Services have been ordered notify Buyer and for the avoidance of doubt, such Incident shall not be a Qualifying Incident; or
 - (b) where the source of the Incident is covered by the Service Levels, use reasonable endeavours to resolve the Incident.
- 5.9.8. The Cloud & Hosting Service Desk will automatically close all raised Incident Records:
- (a) for the Non-Agent Based Monitoring Service, as soon as a responsiveness check returns a positive response; or
 - (b) for the Agent Based OS Monitoring Service, as soon as the processes running on the operating system are available and responsive and the monitoring of the operating system returns results that fall below the agreed system parameter thresholds.

5.10 Security Services:

- 5.10.1. **Firewall Management Services** include the provision, installation, Software Patching and Updates and management of firewalls, where physical, virtual or multi-tenanted, configured to Buyer's requirements to provide restrictions on the source and destination TCP/IP addresses and service ports that are allowed to pass through the firewall
- 5.10.2. **Internet VPN Management** Virtual Private Networks (VPN) are networks deployed on a public network infrastructure that employ the same security, management and service policies as are applied in a private network. VPNs connect branch offices and remotes users by utilising a shared or public network, such as the Internet
- 5.10.3. **Intrusion Detection Service (IDS)** provides diagnostics and reporting of intrusion and unauthorised access to Servers and networks through the monitoring of traffic based upon pre-determined criteria. It also monitors the effectiveness of Buyer's security systems by analysing them in real-time against attacks and
- 5.10.4. **Network Admission Control (NAC)** is a service that is intended to compliment Internet VPN Management. NAC is intended to allow a Buyer to perform an assessment of the endpoint that is being used to connect to the Internet VPN Management to determine if it meets the corporate connection policy
- 5.10.5. **Conditions of Use:** Other than in respect of the Supplier Network, network connectivity between Buyer's VPN clients and the Internet VPN Management service and Buyer's VPN clients and the NAC service is the responsibility of Buyer. Buyer must have Firewall Management Service as a pre-requisite to Internet VPN Management and Network Admission Control.
- 5.10.6. Intrusion Detection Service is dependent on Buyer having Security Incident Response or GPG-13 Protective Monitoring as a pre-requisite.
- 5.10.7. NAC is not designed to prevent or capture an endpoint connecting to the Internet VPN Management which has been compromised with any kind of virus or malware and Supplier accepts no responsibility for an endpoint connecting to the Internet VPN Management which has been compromised with a virus or malware.

5.11 Shared Backup & Storage Services:

- 5.11.1. These consist of either
- (a) **Shared Backup Service** a service to backup flat files only; or backup flat and database files; or



- (b) **Shared Storage Service** which provides Buyer with access to a shared storage area network and the storage attached to it.

5.11.2. **Conditions of Use:** In order for Supplier to be able to provide Shared Backup Service:

- (a) Buyer is responsible for initiating requests for a restore and Supplier is responsible for executing the restore.
- (b) if Buyer does not take the Operating System Services, Buyer is responsible for restoring sufficient service to Buyer's system (ensuring that Supplier can install the backup software and connect to the system) to enable the data restore to initiate.
- (c) Buyer must not, and Buyer will ensure that any third party that Buyer appoints will not, modify the backup software configuration files. If Buyer requires changes to the backup software configuration files, these will need to be agreed.
- (d) the Equipment included in Buyer Solution for which Shared Backup Service is provided must be located in a Cloud & Hosting Centre.

5.11.3. **Conditions of Use:** In order for Supplier to be able to provide Shared Storage Service Buyer agrees that:

- (a) Supplier is responsible for the installation of the Equipment and Software for the Shared Storage Services;
- (i) in the event that Buyer manages the operating system on the host operating system, the following additional conditions apply: all hosts requiring connectivity to the shared storage platform must be approved by Supplier; all changes to the host operating system must be agreed by Supplier; and the host operating system must support the technical requirements of the storage platform as provided by Supplier;
- (b) Supplier reserves the right to remove or disable any host system managed by Buyer which is causing or may cause issues with the storage platform for Supplier's other Buyers.
- (c) where any Software or firmware is provided by Supplier to Buyer as part of this Service Element Supplier shall use reasonable endeavours to make required updated versions available to Buyer

5.12 Dedicated Backup & Storage Services

5.12.1. The Dedicated Services consist of either Dedicated Backup Service or Dedicated Storage Service. Dedicated Backup Service provides for the installation of dedicated backup Equipment or software to backup and restore Buyer's data. Dedicated Storage Service provides for the installation, configuration, monitoring, management and support of a dedicated storage solution within one of Supplier's Cloud & Hosting Centres.

5.12.2. **Conditions of Use:**

- (a) Buyer is responsible for initiating requests for a restore and Supplier is responsible for executing the restore;

5.12.3. If Buyer does not take the Operating System Services, Buyer is responsible for restoring sufficient service to Buyer's system to enable the data restore to initiate. Supplier will use reasonable endeavours to assist in the installation of backup software required to initiate the restore;

5.12.4. Where Supplier does not manage the operating system, Buyer is responsible for upgrading the data backup Software and applying any recommended patches.

5.12.5. In order for Supplier to be able to provide the Dedicated Backup Services Buyer agrees that:

- (a) the Server(s) for which Dedicated Backup Services are provided must have a dedicated network interface of a type specified by Supplier;
- (b) Buyer must adhere to Supplier's default backup configuration settings;
- (c) Buyer must not modify the backup software configuration files;
- (d) Supplier must always have reasonable access to Buyer Solution for which the Dedicated Backup Service is provided;
- (e) the Equipment included in Buyer Solution for which the Dedicated Backup Service is provided must be located in a Cloud & Hosting Centre;
- (f) all Buyer Equipment and Buyer Software must meet Supplier's requirements; and
- (g) Buyer must order the Equipment Maintenance Service and the Software Maintenance Service for the dedicated backup Equipment used to provide the Dedicated Backup Service.

5.12.6. In order for Supplier to be able to provide the Dedicated Storage Service:

- (a) Supplier's approval of the design of Buyer's storage solution is required;



- (b) Supplier is responsible for installation of the Dedicated Storage Service; and
- (c) the procurement of the dedicated storage Equipment is not included in this Service Element, although the option for Supplier to procure Equipment for the Dedicated Storage Service for Buyer purchase may be provided in the Order.

5.13 Managed Cloud Tiering Appliance Services

- 5.13.1. Managed Cloud Tiering Appliance Services provide the installation, initial policy configuration, monitoring, management and support of a Cloud Tiering Appliance solution within one of Supplier's Cloud & Hosting Centres.
- 5.13.2. Managed Cloud Storage Gateway Services provide the installation, initial policy configuration, availability monitoring, management and support of a Cloud Storage gateway solution within one of Supplier's Cloud & Hosting Centres.
- 5.13.3. **Conditions of Use:** If Buyer purchases the Managed Cloud Tiering Appliance Services:
 - (a) Buyer will need to order the Cloud Storage Service via a separate Order and agree to the Cloud Storage Service Terms.
 - (b) Buyer must obtain Supplier's approval to the design of these Service Elements.
 - (c) Supplier is responsible for the installation of these Service Elements.
 - (d) These Service Elements do not include the procurement of the Cloud Tiering Appliance or Cloud Storage Gateway or any connections to them. If requested by Buyer, Supplier may procure the Cloud Tiering Appliance or Cloud Storage Gateway and any connections to them on Buyer's behalf and at Buyer's expense.

6. Data Protection

Vodafone as a Data Controller

- 6.1 Vodafone as a Data Controller:** Supplier acts as an independent Data Controller for the Processing activities in these clauses 6.1 to 6.5 (Data Controller role and processing activities) and any additional activities listed in the Service Terms.
- 6.2 Buyer as a Data Controller:** The Parties acknowledge that Buyer will also act as an independent Data Controller for any Personal Data relating to Supplier employees or representatives, for example business contact information.
- 6.3 Processing Activities:** Supplier may process:

- 6.3.1. Personal Data to:
 - (a) manage account relationships;
 - (b) send bills;
 - (c) fulfil an Order or delivery;
 - (d) provide Buyer service; and
 - (e) control access to Supplier's systems that support the Services.
- 6.3.2. As an electronic communications service's provider, Traffic Data in accordance with Applicable Laws to:
 - (a) deliver User communications;
 - (b) calculate Charges for each User;
 - (c) identify threats to the Network or Services and protect against them; and
 - (d) internally develop and improve the Network or Services.

6.4 Data Disclosures: Supplier may disclose Personal Data and Traffic Data:

- (a) to Vodafone Group or third parties for the purpose of supporting the Processing activities described in this clause 6 (Data Protection) or as permitted under Applicable Privacy Law; and
- (b) as required by Applicable Law, court order, or any Authority (including Privacy).

6.5 Privacy Notice: Supplier's privacy notice can be accessed at: www.vodafone.co.uk/privacy.

Vodafone as a Data Processor

- 6.6 Vodafone as a Data Processor:** Supplier acts as a Data Processor for the specific processing as set out in the relevant Service Terms.
- 6.7 Processing Personal Data:** Supplier may only Process Personal Data on behalf of the Buyer:



- (a) to provide and monitor a Service as outlined in the Service Terms; or
 - (b) for any other purpose agreed in writing between the Parties. Additional instructions from Buyer require prior written agreement and may be subject to Charges.
- 6.8 Changes to Sub-Processors:** If Supplier adds or replaces a Sub-Processor, Supplier shall inform the Buyer of changes to Sub-Processors where Supplier is required by Applicable Privacy Law by:
- (a) providing at least 10 Working Days' prior notice; or
 - (b) listing the new or replacement Sub-Processor on www.vodafone.co.uk at least 10 Working Days before Supplier authorises and permits the new or replacement Sub-Processor access to Personal Data in order to give the Buyer the opportunity to reasonably object to such changes.
- 6.9 Sub-Processor Obligations:** Supplier will enter into binding agreements with its Sub-Processors, who will have substantially the same legal obligations for Processing activities as Supplier under these clauses 6.6 to 6.17 (Data Processor role and related requirements). Supplier will be liable to Buyer for the performance of that Sub-Processor's obligations.
- 6.10 Data Retention:** Supplier may keep Personal Data for as long as required to deliver the Service. After this Agreement is terminated, and unless Applicable Law requires otherwise, Supplier will:
- (a) delete the data within a reasonable time frame;
 - (b) return the data if the Buyer provides notification before termination of the Agreement.
- 6.11 Data Access:** Supplier may give access to Personal Data only if necessary to meet its obligations in relation to the Service and will take reasonable steps to ensure that whoever accesses the data:
- (a) is under a statutory or contractual obligation of confidentiality;
 - (b) is trained in Supplier's policies for handling Personal Data; and
 - (c) does not Process Personal Data except as instructed by Buyer, unless Applicable Law requires otherwise.
- 6.12 Data Security:**
- 6.12.1. As required by Applicable Privacy Law, Supplier will:
- (a) provide technical and organisational measures for a level of security appropriate to the risk presented by Processing taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing;
 - (b) comply with Supplier information security policies based on ISO / IEC 27001:2013;
 - (c) give Buyer all information, assistance, and co-operation it may reasonably require to comply with Applicable Privacy Law;
 - (d) notify Buyer without undue delay of any unauthorised access to Personal Data that results in loss or unauthorised disclosure of, or alteration to, Personal Data;
 - (e) provide reasonable assistance to Buyer in relation to any Personal Data breach notification that Buyer is required to make under Applicable Privacy Law; and
 - (f) when requested by Buyer and before any Processing, provide reasonable assistance with:
 - (i) carrying out a privacy impact assessment of the Services; and
 - (ii) consulting the relevant Privacy Authority regarding Processing activities related to the Services.
- 6.12.2. Further information on data security measures can be found at www.vodafone.com/business/Buyer-security.
- 6.13 Audits and Inspections:** If Buyer has a right of audit and inspection under Applicable Privacy Law, it agrees to act as follows:
- (a) Buyer may ask to review Supplier's security organisation, and the good practice and industry standards contained in Supplier's information security policies no more than once each calendar year, and any such review shall relate only to data protection compliance of the Services; and
 - (b) ensure its instructions comply with Applicable Privacy Law. Supplier will inform Buyer if it believes any Buyer instruction infringes Applicable Privacy Law or any confidentiality obligations.
- 6.14 Buyer Responsibilities:** Buyer accepts and agrees that they are responsible for:
- (a) reviewing the information Supplier makes available; and



- (b) determining if the Services meet Buyer's requirements and legal obligations.

6.15 Onward Transfers out of the EEA and UK: Supplier may onward transfer Personal Data to a country outside the European Economic Area, the UK or a country that has not been designated by the European Commission or Secretary of State in the UK as ensuring an adequate level of protection under Applicable Privacy Law, only if:

- (a) the data is transferred in line with the requirements under Applicable Privacy Law;
- (b) the Processing or transfer does not put any Buyer in breach of Applicable Privacy Law; or
- (c) Applicable Law requires it. In this case, Supplier will inform Buyer of that legal requirement before Processing, unless prohibited by Applicable Law.

6.16 Law Enforcement: Supplier:

- (a) may receive legally binding demands from a law enforcement authority for the disclosure of, or assistance with Personal Data, or be required by Applicable Law to disclose Personal Data to persons other than Buyer ("Demand");
- (b) is not in breach of any obligation to Buyer in complying with the Demand; and
- (c) will notify Buyer of the Demand as soon as possible, unless prohibited by Applicable Law.

6.17 Data Subject Enquiries: Taking into consideration the nature of the data processing conducted by Supplier on behalf of the Buyer, Supplier shall assist the Buyer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Buyer's obligation to respond to requests for exercising the data subjects' rights laid down in Applicable Privacy Law.

7. Service Level Agreement

7.1.1. General Support Services Terms

7.1.2. Supplier will provide Buyer with Support Service for the Service Elements ordered by Buyer.

7.1.3. Support Service is available in English only.

7.1.4. Support Service is available as shown below:

Support Service	Service Cover Period
Incident Management for Priority 1 & 2 Incidents	24/7
Incident Management for Priority 3 & 4 Incidents	Working Hours
Service Request Fulfilment	Working Hours

7.1.5. Incidents may be reported at any time during the Service Cover Period; however, Incident resolution will only occur during Working Hours for Priority Level 3 and 4 Incidents.

7.1.6. An Incident may also be a Qualifying Incident.

7.1.7. The Buyer shall appoint primary and secondary central points of contact responsible for accessing the Support Service and communicating with Supplier during the relevant Service Cover Period. Buyer will inform Supplier and keep Supplier up to date with the appointed individuals' identity and level of access.

7.1.8. Buyer will:

- (a) reimburse Supplier for reasonable expenses associated with actions taken when Buyer has reported an Incident caused by an Excluded Event; and
- (b) permit Supplier to interrupt the Service to resolve a Priority Level 1 or 2 Incident (or the Incident will be downgraded to a Priority Level 3 Incident).

7.1.9. Supplier may temporarily interrupt the Service to carry out Planned Works. Supplier will endeavour to notify Buyer in advance of any Planned Works.

7.1.10. Incident Commencement and Resolution Rules: An Incident commences when Supplier creates an Incident Report (being no later than 60 minutes after the Incident has been reported to Supplier) and ends on the earlier of when Supplier advises Buyer of Incident resolution or when the Incident affecting the Service has ceased. In Supplier's discretion or at Buyer's reasonable request, Supplier may continue to investigate via Supplier's Problem Management process; however, this shall not affect the resolved status



of the Incident. Buyer is deemed to have been advised of Incident Resolution if Supplier has made reasonable attempts to contact Buyer and Buyer has not notified Supplier within 24 hours from Supplier's last attempt to contact the Buyer that the Incident resolution is unsuccessful. Supplier's method of Incident resolution is at Supplier sole discretion.

7.2 Early Life Support

- 7.2.1. Early Life Support is limited to supporting Buyer's ability to deploy Buyer applications on the Buyer Solution and to integrating the Buyer Solution into the Buyer's business. Other elements of Early Life Support will vary on a case by case basis.
- 7.2.2. Early Life Support will last for the duration of the Early Life Support Period.
- 7.2.3. Early Life Support is not available in respect of a new single Device being added to the Buyer Solution.
- 7.2.4. During Early Life Support: During Working Hours Buyer will be able to log Incidents solely related to Buyers ability to (i) deploy Buyer's applications on the Buyer Solution and (ii) integrate the Buyer Solution into the Buyer's business.
- 7.2.5. Supplier will use reasonable endeavours to investigate the causes of the Incidents.
- 7.2.6. Buyer will be able to request changes and Supplier will use reasonable endeavours to implement any agreed changes in an agreed time frame.
- 7.2.7. Changes raised during the Early Life Support Period, will consume Inclusive Resource for Change. Should additional hours above the Inclusive Resource for Change be used, Supplier reserves the right to charge for such excess work.

7.3 General Service Level Terms

- 7.3.1. Service Levels and Service Credit terms for the Buyer Solution or applicable Service Element commence on the Service Level Commencement Date.
- 7.3.2. The Service Levels do not apply to Incidents caused by or connected to an Excluded Event or to an output from an Automated Service Request

7.4 Service Availability

- 7.4.1. **Calculation:** Percentage availability is calculated as $P = ((A-B)/A) \times 100$. "A" equals 43200 minutes each full month. "B" equals the number of whole minutes when the relevant Buyer Solution or Service Element is unavailable in the Monthly Measurement Period.
- 7.4.2. **Solution Availability** – The Service Level for Solution Availability is as detailed in the High Level Design. If the Service Levels in the High Level Design exceeds the levels set out in Table 1, or if the High Level Design does not contain Service Levels then Device Availability shall apply:

Table 1 Maximum Solution Availability		
Class of Solution	Maximum Availability	Example
Non-resilient*	97%	Solution provided with one or more single points of failure, such as single server, single firewall.
Resilient	99.9%	Solution provided from a single location, but with no single points of failure, utilising load balancing, N+1 design, etc.
Resilient with Backup Site	99.95%	The same as resilient but also with automated failover to a second location comprising a non-resilient solution.
Distributed resiliency	99.99%	The same as resilient but also with automated failover to a second location comprising another N+1 / resilient solution, with replication between sites.
*The maximum availability where the class of solution is non-resilient excludes the time taken for any replacement Equipment to arrive at the required installation location following a Qualifying Incident.		

(a) Device Availability



- (i) For a single Device, Supplier offers a 97% Availability Service Level. Single Devices are treated as non-resilient as per Table 1. For additional Devices forming part of the Buyer Solution, Table 1 shall apply depending on the design of the Buyer Solution.

(b) **Network Availability**

Network Services Availability (i) If Supplier provide internet access and the service configuration is a single & resilient service dual parent (fully diverse), the Service Level for Availability is 99.99% in a Monthly Measurement Period.

Network Latency and Packet Loss Service Level-Network Latency measures the amount of time that it takes for data to travel between Primary IP Backbone Nodes, and back, on the Supplier IP Backbone within each Region and between Regions.

The Service Level performance for Network Latency is calculated as follows: (x) within a Region - by taking the average monthly Network Latency performance for all routes between Primary IP Backbone Nodes within that Region; and (y) between two Regions - by taking the monthly average Network Latency of the two Primary IP Backbone Nodes with the lowest Network Latency between those Regions.

Packet Loss measures the percentage of data that is lost during the transit of data between Primary IP Backbone Nodes on the Supplier IP Backbone within each Region and between each Region.

The Service Level performance for Packet Loss is calculated as follows: (a) within a Region - by taking an average of the average monthly Packet Loss performance for all routes between Primary IP Backbone Nodes within that Region; and (b) between two Regions - by taking the monthly average Packet Loss for all routes between Primary IP Backbone Nodes between those Regions.

These Service Level targets apply to the Network Latency and Packet Loss performance of the Supplier IP Backbone:

Monthly Average Network Latency and Packet Loss Service Levels		
Region(s)	Parameters	Service Level target
Europe - Europe	Network Latency (ms)	35
	Packet Loss (%)	0.2
Europe – UK	Network Latency (ms)	20
	Packet Loss (%)	0.2
Europe - North America	Network Latency (ms)	90
	Packet Loss (%)	0.2
Europe – Asia	Network Latency (ms)	310
	Packet Loss (%)	0.2
UK – UK	Network Latency (ms)	35
	Packet Loss (%)	0.2
UK- North America	Network Latency (ms)	90
	Packet Loss (%)	0.2
UK – Asia	Network Latency (ms)	210
	Packet Loss (%)	0.2
North America – North America	Network Latency (ms)	65
	Packet Loss (%)	0.2
North America - Asia	Network Latency (ms)	165
	Packet Loss (%)	0.2



Asia – Asia	Network Latency (ms)	90
	Packet Loss (%)	0.2

(c) **Optional Service Element Availability**

(i) Shared Backup Service Levels

Service	Service Availability	Service Performance
Shared Backup Service on a 24/7 basis	99.9% in a Monthly Measurement Period	98% of backups completed successfully in a Monthly Measurement Period.
Buyer must have appropriate backup software installed and configured. Any single storage Device having excessive volumes (as determined by Supplier, in Supplier's reasonable discretion) of data requiring backup will be excluded from any calculation. If Buyer Equipment or Buyer Software accessing the Shared Backup Service fails and such Buyer Equipment or Buyer Software is not managed by Supplier, then such failures are excluded under both the Service Availability and Service Performance Service Levels The Service Levels are measured from the Equipment at the edge of the shared backup platform. If a backup fails on the first attempt but is then successful on a second attempt, the backup is considered successful.		

(ii) Shared Storage Service Level

Service	Service Availability
Shared Storage Service	99.9% in a Monthly Measurement Period
This Service Level is measured from the Equipment at the edge of the shared storage platform and is subject to Buyer having two redundant host bus adapters into the shared storage area network and the required multi-pathing software (or similar) installed and properly configured.	

(d) **Email Protection Services**

The Email Protection Services have an Availability Service Level of 99.95% in the relevant Monthly Measurement Period. This Service Level excludes any Devices dedicated to the Buyer Solution, which are treated separately. Password protected and/or encrypted emails and attachments are excluded from this Service Level.

(e) **Managed Cloud Storage Gateway Service**

The Managed Cloud Storage Gateway Services have an Availability Service Level of 97% (measured as the accessibility of data stored in the gateway's local cache by Buyer) in the relevant Monthly Measurement Period. If the Buyer has a license for the failover virtual Cloud Storage Gateway, the Service Level shall be 99.90% in the relevant Monthly Measurement Period. Any Service Levels contained in the Cloud Storage Service Specific Terms do not apply to the Managed Cloud Storage Gateway Services.

(f) **Private Cloud Self-Service Portal - Virtual Machines**

Buyer has the ability to set different affinity rules as per the table below via the Private Cloud Self Service Portal. The Service Level applicable to the Virtual Machines forming part of the Buyer Solution will vary depending on the affinity rules set by Buyer:

Private Cloud Self-Service Portal – Virtual Machines		
Affinity and anti-affinity rules	Class of Solution	Availability of Virtual Machines in a Monthly Measurement Period



Private Cloud Self-Service Portal – Virtual Machines		
Affinity Must Rule – This allows specific Virtual Machines to reside on a specific underlying physical host however if that physical host fails then the Virtual Machines will NOT failover to another physical server in the Buyer's environment	Non-resilient	97%
Affinity Rule –This allows specific Virtual Machines to reside on a specific underlying physical host but if that physical host fails then the Virtual Machine will failover using HA to another physical server in Buyer's environment.	Resilient	99.9%
Anti-Affinity Rule – This allows users to define that Virtual Machines are kept apart from different underlying physical hosts. Service Level will apply as long as the Buyer has deployed an N+1 architecture		

(g) **SLO- Private Cloud Disaster Recovery & Rapid Recovery**

Supplier will use its reasonable endeavours to deliver the following Recovery Times Objectives and Recovery Point Objectives in respect of Disaster Recovery and Rapid Restore services as set out in the table below.

Disaster Recovery Service	RTO	RPO
Bronze	24 hours (per server)	24 hours (all servers per system)
Silver	4 hours (per server)	12 hours (all servers per system)
Gold	2 hours (per server)	1 hour (all servers per system)
Platinum	1 Hour (per server)	15 minutes (all servers per system)
Rapid Restore	RTO	RPO
Bronze	12 hours (Per server)*	15 minute recovery points available.
Silver	6 hours (Per server)	15 minute recovery points available.
Gold	4 hours (Per server)	15 minute recovery points available.
Platinum	2 hours (Per server)	15 minute recovery points available.

(i) RTO and RPO shall not apply during any planned test of this Service Element.



- (ii) Supplier is not liable for any failure to satisfy the RTO or RPO in the event that the source (primary) private cloud platform has been corrupted, and any standby Virtual Machines on Buyers target (secondary) private cloud platform is not operational post replication.

7.5 Priority of Incidents

7.5.1. The following Priority Levels apply to the Service:

Priority Level	Priority Level Example(s)
1	Total loss of one or more Service Elements that results in the Buyer Solution being unavailable.
2	Intermittent fault or substantial degradation of one or more of the Service Elements that substantially impacts the Buyer Solution.
3	Issue that materially affects the use of the Buyer Solution that is not a Priority Level 1 or 2 issue such as a loss of second site, failure of one or more resilient Devices, failure of a feature of a non-resilient Devices, e.g. a power supply failure in server.
4	Issue that does not materially affect the use of the Buyer Solution such as Total disk usage at 90% Investigations and advice will be given.

7.6 Incident Resolution Times

7.6.1. The Incident Resolution Time is calculated as the number of whole hours between the time Supplier issues a Trouble Ticket and the time Supplier confirms to Buyer that the Incident is resolved.

Priority Level	Incident Resolution Time
1	4 Working Hours
2	8 Working Hours
3	48 Working Hours
4	N/A

7.6.2. When calculating the Incident Resolution Time, any time taken (i) to restore data from backup or (ii) for **Buyer** to carry out any of **Buyer's** obligations is excluded.

7.6.3. The Incident Resolution Time for **Buyer** and third party locations shall be increased to 8 hours in respect of (i) Firewall Management Services and (ii) Internet VPN Management

7.7 Security Incident Response

7.7.1. A Security Incident is raised following initial investigation by Supplier security operations centre (SOC). Where the SOC determines that an alarm should be classified as a Security Incident, the original Incident ticket is closed and the Service Level timer is stopped. The Incident then becomes a Security Incident. A Security Incident Response (SIR) ticket is raised and **Buyer** is contacted. The nature of Security Incident investigation means that SIR tickets have no Service Level for resolution but the following targets will apply:

Priority Level	Priority Level Example(s)	Time to Respond	Time to Conclude Investigation
1	Total loss of one or more Service Elements that results in the Buyer Solution being unavailable.	2 hours	12 hours
2	Intermittent fault or substantial degradation of one or more of the Service Elements that substantially impacts the Buyer Solution.	4 hours	12 hours



Priority Level	Priority Level Example(s)	Time to Respond	Time to Conclude Investigation
3	Issue that materially affects the use of the Buyer Solution that is not a Priority Level 1 or 2 issue such as a loss of second site, failure of one or more resilient Devices, failure of a feature of a non-resilient Devices, e.g. a power supply failure in server.	By end of next working day	12 Working Hours
4	Issue that does not materially affect the use of the Buyer Solution such as Total disk usage at 90% Investigations and advice will be given.	By end of next working day	12 Working Hours
Respond or Responded means Supplier first begins actively working on the matter calculated from the time of the initial alarm. Time to Conclude Investigation means Supplier have concluded their initial investigations and this time commences after Supplier has Responded.			

7.8 Professional Services

7.8.1. Buyer may request Supplier to provide Professional Services to assist the Buyer with deploying applications on the Buyer Solution.

8. General Definitions

8.1 The following definitions apply to the **section 3 - General Conditions** on the Buyer of these Service Terms:

Additional Service Recipient	a Buyer Group entity which is not a direct party to this Agreement, but which is named in this Agreement as a beneficiary of the Services or otherwise approved to receive the Services in accordance with clause 3.1 (Additional Service Recipient).
Agreement	this agreement, consisting of the documents set out in clause 2 (Service Terms Structure).
Applicable Law	law, regulation, binding code of practice, rule or requirement of any relevant government or governmental agency, regulatory Authority, each as relevant to (i) Supplier in the provision of the Services and/or (ii) Buyer in the receipt of the Services or the carrying out of its business.
AUP	Supplier's acceptable use policy set out at http://www.vodafone.co.uk/Acceptable-Use-Policy-Business , as updated by Vodafone from time to time.
Buyer	the entity identified in the Call-Off Order Form as such.
Buyer Equipment	hardware, software or any other tangible material not supplied by Supplier that is used with or to access the Service. Any Equipment Buyer purchases from Supplier shall be considered to be Buyer Equipment once title has passed to the Buyer.
Buyer Group	Buyer and any company in which Buyer has the beneficial ownership of more than 50% of the issued share capital, or the legal power to direct the general management of the company in question, either at or after the date of this Agreement.
Buyer Site	as the context permits a Buyer's premises (either owned by Buyer or a third party) which Supplier needs to access in order to deliver or install Equipment and/or to provide the Services or the location where the Services are to be provided, as set out in the Call-Off Order Form.



Charges	the charges or fees specified in this Agreement as payable by Buyer.
Consumer	means any natural person acting for purposes that are outside the person's trade, business, craft or profession.
End Of Life	where Supplier or a manufacturer of Equipment declares that the type of Equipment is end-of-life (or otherwise stops marketing, selling or supporting it).
Equipment	hardware, Supplier Software, and any other tangible equipment (other than SIMs) supplied by, or on behalf of, Supplier to Buyer for use in receiving the Services. Equipment excludes Buyer Equipment.
European Union (EU)	an economic and political union of 27 countries, as may be updated from time to time. A full list of countries can be found here https://www.gov.uk/eu-eea .
GSM Gateway	any equipment containing a SIM which enables calls from a fixed network (landline) to be routed via a GSM link to a mobile network establishing a mobile-to-mobile ('on-net') call.
Incumbent Provider	a regulated operator who is authorised to provide a Service in a given country.
Intellectual Property Rights	(a) rights in, and in relation to, any patents, registered designs, design rights, trade marks, trade and business names (including all goodwill associated with any trade marks or trade and business names), copyright, moral rights, databases, domain names, topography rights and utility models, and includes the benefit of all registrations of, applications to register and the right to apply for registration of any of the foregoing items and all rights in the nature of any of the foregoing items, each for their full term (including any extensions or renewals) and wherever in the world enforceable; (b) rights in the nature of unfair competition rights and rights to sue for passing off; and (c) trade secrets, confidentiality know how, technical information and other proprietary rights.
Network	the communications network together with the equipment and premises that are connected to such network and which are used by Vodafone to perform the Services.
Non-Recurring Charges	means One-Off Charges.
One-Off Charges	the Non-Recurring Charges payable by Buyer in relation to the Service and/or Equipment as described in the Buyer's Call-Off Order Form, and may include installation Charges for ports, access circuits and routers, charges for set up of Service Elements and configuration changes.
Party or Parties	Buyer and/or Supplier, as relevant.
Recovery Charge	any amount payable by Buyer for early termination or failure to meet commercial commitments as set out in this Agreement.
Service Element	the individual components of a Service (including optional service elements if applicable).
Service Specific Terms	the document(s) identified in this Agreement as the "Service Specific Terms" that set out information such as terms and conditions, specifications and technical information specific to a Service.
Service(s)	the services to be provided by Supplier or a Third Party Provider under this Agreement and as specified in this Agreement. Any reference to Service within this Agreement may be an individual Service or collectively all Services, as appropriate.



SIM	a “subscriber identity module” card is an integrated circuit, whether physical or embedded in a device (and then known as an eSIM Card), storing user specific data and provided by Supplier to allow use of equipment on the Network by Buyer.
Supplier	where used in these Service Terms or the Call-Off Contract means Vodafone.
Supplier Software	any Software supplied by Supplier or its licensors to Buyer (including Software embedded in any Equipment).
Technical Prerequisites	any requirements detailed in the Service Specific Terms or otherwise provided to Buyer in writing relating to a Service or Equipment including notification to upgrade.
Third Party Provider	a third party contracted directly or indirectly by either Supplier (including Vodafone Group) or Buyer that provides a Service, a Third Party Service or that provides a service that connects to a Service. Third Party Providers may include Incumbent Providers.
User	an individual end user of the Services who is approved by Buyer and who must be a permanent or temporary employee or sub-contractor of Buyer or an Additional Service Recipient unless otherwise specified in this Agreement.
User Details	a user name, password, or other access information used by a User to access the Service and/or Equipment.
UK	England, Wales, Scotland, Northern Ireland and adjacent islands (e.g. Isle of Wight) but excluding the Channel Islands and the Isle of Man.
Vodafone	Vodafone Limited, registered number 01471587, and registered office Vodafone House, The Connection, Newbury, Berkshire RG14 2FN.
Vodafone Group	(a) Vodafone Group Plc, Vodafone Limited and any company in which Vodafone Group Plc owns (directly or indirectly) 15% or more of the issued share capital; and (b) any partner market listed on the “Where we are” page at http://www.vodafone.com/ .
Working Days	Monday to Friday inclusive, other than public holidays in the UK.
Working Hours	9.00am to 5.00pm on a Working Day.

8.2 The following definitions apply to the Fixed Services Conditions on the Buyer set out in **section 4** of these Service Terms:

BPE (Buyer premises equipment)	Fixed Equipment on Buyer Site.
Fixed Equipment	hardware, Supplier Software, BPE and any other tangible equipment (other than SIMs and mobility equipment) supplied by or on behalf of, Supplier to Buyer for use in receiving the Services.
Service Commencement Date	the date of completion of Supplier’s testing when the Service is ready for use.
Site Survey	a survey of a Buyer’s Site to assess whether (in Supplier’s opinion) the existing infrastructure is sufficient for providing the Services and detailing what the Buyer needs to do to receive the Service.

8.3 The following definitions apply to the Service Specific Conditions on the Buyer and Service Elements set out in **section 5** of these Service Terms:

Acceptance or Accepted	those parts of the Buyer Solution that have been the subject of Acceptance Testing have achieved, or are deemed to have achieved, the Acceptance Criteria.
-------------------------------	--



Acceptance Criteria	such criteria as established by Supplier to determine whether or not the Buyer Solution is ready for use by the Buyer.
Acceptance Date	means the date on which Acceptance occurs or is deemed to have occurred.
Acceptance Testing Period	a period of testing commencing on the Handover Date lasting: (i) for a continuous period of 10 days in the case of a new Solution; or (ii) for a continuous period of 5 days in the case of a new Device; in each case the "Acceptance Testing Period".
Agreed Ready for Service Date or ARFS Date	the date on which Supplier plan to commence supplying the Buyer's Solution following Supplier's acceptance of the Buyer's Order.
Agent	a software application that can be installed on an operating system
Anti-Virus Service	Supplier will provide anti-virus software and monitor the software for updates ensuring relevant updates are applied on a regular basis. This only applies where Buyer has ordered the Operating System Services.
Automated Service Request	a Service Request which is fulfilled via software instruction and is automatically delivered once successfully completed
Availability	the percentage of time the Buyer Solution or Service Element as applicable is available for use in a Monthly Measurement Period.
Client Software	software that is installed on a Device that allows the Device to access or utilize the Microsoft Products.
Cloud & Hosting Centre	a Supplier or third party data centre with connectivity to the Vodafone Network used to provide the Buyer Solution to the Buyer.
Cloud & Hosting Service Desk	the service desk provided by Supplier for Buyer Solution
Cloud Storage Gateway	the hardware or virtual appliance that presents file storage into Buyer's Solution, providing a local cache for recently written data, whilst protecting all data written to it in the Cloud Storage Service
Cloud Storage Service	the Cloud Storage services to be provided by Supplier to Buyer as set out in separate Cloud Storage Service Specific Terms
Cloud Tiering Appliance	a hardware or virtual appliance that moves files from primary file storage to another storage tier by policy/schedule, replacing the original file with a small stub/pointer. Deployed with a high-availability module that provides read only access to data if the primary device fails.
Buyer Equipment	hardware, software or any other tangible material not supplied by Supplier that is used with or to access the Service. Any equipment Buyer purchases from Supplier shall be considered to be Buyer Equipment once title has passed to the Buyer.
Buyer Software	either: 1) software purchased by the Buyer from Supplier pursuant to these Service Terms or 2) software provided by the Buyer.
Buyer Solution	a set of Service Elements and Devices that together form the Solution for Buyer.
Data Centre	Data Centre a Supplier or Supplier-selected third-party data centre(s), where Supplier provides Buyer with cloud or hosting Services.
DDoS Mitigation Service	is a service designed to detect and mitigate distributed denial of service attacks via the public Internet, for Buyers taking Internet connectivity from Supplier.



Device	any: (a) single manageable piece of Equipment, or (b) piece of Equipment supported by software shared across multiple Buyers such as a server, a router, a switch, a firewall or a storage array; or in the case of the Third Party Provider User Terms, each of a computer, workstation, terminal, handheld PC, pager, telephone, personal digital assistant, “smart phone”, server or electronic device.
Early Life Support	the support provided by Supplier for those parts of the Buyer Solution that Supplier has handed over to the Buyer before those services are Accepted.
Early Life Support Period	the period commencing on the Handover Date and lasting for a continuous period of: (a) 20 days in the case of a new Solution; or (b) 10 days in the case of a new standalone Device that is not part of an existing Solution; or such other period as Supplier may agree with the Buyer.
Email Protection Services	is a service designed to scan emails for (depending on the Email Protection option ordered) viruses, spam, “pornographic images and Buyer own specified content (Content Control).
End User	in the case of the Third Party Provider User Terms, an individual or legal entity that obtains Software Services directly from Supplier, or indirectly through a Software Services Reseller.
Equipment Maintenance Services	maintaining, repairing, and replacing if necessary the Equipment.
Excluded Event	means an Incident caused by: (a) another Supplier service purchased under a separate Buyer Agreement; (b) non-Supplier-supplied power, Buyer Equipment, non-maintained structured cabling or other systems or networks not operated or provided by Supplier (including an Incident relating to consumption of services over the internet); (c) the negligence, act, or omission of Buyer or a third-party not within Supplier’s direct control; (d) Buyer’s delay or non-performance of any of Buyer obligations set out in the Buyer Agreement; (e) Buyer’s request to modify or test a Service Element; (f) a Force Majeure event or Service suspension that is permitted under the Buyer Agreement; (g) the inability or refusal by a Third Party Provider to provide the Mandatory Accompanying Service/access circuit at a Buyer Site; (h) a configuration change during implementation; and (i) service failure at any other Buyer Site; (j) Planned Works; (k) a period of suspension of the Service agreed between the Parties or permitted under the Buyer Agreement, (l) an Incident which arises in Equipment or Software for which Supplier are responsible but which has been modified or changed on the Buyer’s behalf in a manner which has not been accepted in writing by Supplier as having no effect on Supplier’s liability to pay Service Credits; and (m) an Incident which arises as a result of the Buyer failing to agree to the installation of an upgrade, patch or change recommended by Supplier, such as security or other fixes; (n) denial of service attacks (DDoS), where DDoS mitigation services are not provided to Buyer by Supplier; (o) scheduled or Supplier requested maintenance windows; and (p) software or hardware components are no longer supported by the vendor and are therefore considered End of Life or Out of Support.
Extra Service Terms	the additional terms that apply to certain Service Elements ordered by Buyer set out in the Extra Service Terms and/or as Supplier otherwise advises Buyer in writing.



GPG-13 Protective Monitoring Service	is an enhanced version of the Security Incident Response Service designed specifically for the UK Public Sector. It is only available within the UK and is subject to approval of the UK Government.
Handover Date	the date on which Supplier notifies the Buyer that the Buyer Solution, or any part of it, is available for Acceptance Testing.
High Level Design	the document prepared by Supplier to describe, the technical aspects of the Buyer Solution including the Service Level details.
Incident	an unplanned interruption to the Service, a reduction in the quality of a Service, or a failure of a Service configuration item.
Incident Management	the end-to-end management of Incidents by Supplier.
Incident Record	a record of an Incident with a unique reference allocated to it which shall be used for all subsequent updates and communications
Inclusive Resource for Change	the number of free allotted hours of Supplier (including any Third Party Providers) resource available for Buyer to use in implementing changes, as notified to Buyer from time to time.
Infrastructure Services	provide installation, Software Patching and Updates and Monitoring and Reporting Services.
Minimum Term	the minimum term to which Buyer commits to receive a Service (as applicable) as specified in the Call-Off Contract.
Monthly Measurement Period	the period from the Service Level Commencement Date up to the end of the calendar month and then each calendar month thereafter (save for the last month that will end upon the termination date of the Service).
Network Service	the Supplier provided connectivity from the Buyer Solution to either the Vodafone Network or to shared Vodafone platforms
Planned Works	planned Supplier-initiated changes to the Service or Equipment (for example, to carry out essential maintenance or upgrades).
Primary IP Backbone Nodes	the specific nodes on the Supplier IP Backbone that Supplier identifies and notifies to Buyer from time to time.
Procurement Services	provides the Buyer with procurement, configuration and maintenance services for the Equipment
Professional Services	the optional services from Supplier in order to customise the Buyer Solution; obtain additional services based on the Buyer's individual requirements; or obtain project management in respect of the Buyer Solution.
Qualifying Incident	an Incident which has a Priority level of 1 or 2 and which prevents the Buyer from using the Solution or a Service Element in accordance with the service parameters
Recovery Point Objective (RPO)	the maximum rollback point in time to which Buyer's data will be restored during data restoration (e.g. where a RPO of 1 hour applies, and where disruption occurs at noon, data will be recoverable up to 11 am on the same day).
Recovery Time Objective (RTO)	the time taken to restore or reconfigure Equipment and commence the uploading of data to the target systems during the restoration process
Redistribution Software	the software described in the Third Party Provider's User License Terms.
Security Incident	a threat to information or computer security as determined by Supplier.
Security Incident Response	a service that uses a combination of correlation techniques to detect anomalous behaviour including statistical, behavioural and rules base analysis.
Server	a physical and/or virtual device running a hypervisor and/or operating system



Service Credit(s)	the service credit payable by Supplier to Buyer in accordance with these Service Specific Terms.
Service Cover Period	as described in paragraph 1 of the Service Levels.
Service Level(s)	the service levels that apply to the provision of the Service as set out in these Service Specific Terms.
Service Level Commencement Date	the date which is the later of (where relevant) (i) the expiry of the Early Life Support Period (ii) the Acceptance Date and (iii) the Service Commencement Date for the Buyer Solution or individual Service Element as applicable.
Service Level Objective or SLO	the performance Supplier expects to provide, without associated Service Levels or Service Credit.
Software Maintenance Services	maintaining, updating and if necessary replacing the Software.
Software Patching and Updates	as part of this service Supplier will monitor the operating system and database vendor updates and recommend appropriate patches and updates to the Buyer.
Software Services	services that Supplier provides that make available, display, run, access, or otherwise interact, directly or indirectly, with the Products. Supplier must provide these services from data centre(s) through the Internet, a telephone network or a private network, on a rental, subscription or services basis, whether or not Supplier receives a fee. Software Services exclude any services involving installation of a Product directly on any End User device to permit an End User to interact with the Product.
Solution	a set of Service Elements and Devices that together form a Solution.
Trouble Ticket	a record of an Incident with a unique reference allocated to it that is used for all subsequent updates and communications.
Virtual Machine	software container that can run its own operating systems and applications as if it were a physical computer
Supplier Equipment	Equipment supplied by Supplier for Buyer's use and includes hardware and related software that Supplier will use to provide the Buyer Solution exclusively to the Buyer at the Cloud & Hosting Centre.
Supplier IP Backbone	is collectively represented by Supplier autonomous system Networks known as AS1273, AS6660 and AS2529.
Supplier Monitoring Infrastructure	the monitoring infrastructure at a Cloud & Hosting Centre that performs monitoring services in respect of various types of hosting and network equipment.
Supplier Network	the Supplier IP network between the primary backbone nodes, (excluding the connection from the Cloud & Hosting Centre to the Buyer Solution, access facilities, the Equipment) and Buyer Equipment.
Supplier Software	Software that Supplier uses to provide the Buyer Solution exclusively to the Buyer at the Cloud & Hosting Centre where title remains with Supplier or the Third Party Provider.

8.4 The following definitions apply to **section 6 - Data Protection** of these Service Terms:

Applicable Privacy Law	the relevant data protection and privacy law, regulations (including UK GDPR and the Data Protection Act 2018) and other regulatory requirements to which Vodafone Limited is subject.
"Fixed Authority"	means those governments, agencies, courts of law, and professional and regulatory authorities including NRAs that supervise, regulate, investigate, or enforce Applicable Law.



Data Controller	the person that determines the purposes and means for which Personal Data is Processed, as defined under Applicable Privacy Law.
Data Privacy Obligations	in respect of each Party, that Party's obligations relating to the Processing or control of Personal Data as a Data Controller or Data Processor, as expressly set out in clause 6 (Data Protection) of this Agreement.
Data Processor	the person that Processes Personal Data on behalf of the Data Controller as defined under Applicable Privacy Law.
European Economic Area (EEA)	means the Member States of the European Union together with Iceland, Liechtenstein, and Norway, as may be updated from time to time. A full list of countries can be found here https://www.gov.uk/eu-eea .
GDPR	General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data.
Personal Data	shall mean any information relating to an identified or identifiable natural person as defined by the Applicable Privacy Law.
Privacy Authority	the relevant statutory or supervisory authority with responsibility for the Applicable Privacy Law in the jurisdiction of the Data Controller.
Process/Processed/Processing/Processes	obtaining, recording or holding information or data or carrying out any operation or set of operations on it.
Sub-Processor	a sub-contractor who is processing Personal Data on behalf of Supplier.
Traffic Data	any data processed for the purpose of the conveyance of a communication on an electronic communications network and for billing.
UK GDPR	means GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.