The Corda Network

Service Level Agreement

and

Support Services Handbook

October 29, 2018

Service Level Agreement

1.0 Introduction, Scope & Assumptions

This is a Service Level Agreement ("SLA") for the R3 Doorman, R3 Network Map Service and R3 Notary Service provided by R3 to document the appropriate service levels for each Covered Service and penalties for non-performance.

This SLA defines support for the Services provided by R3, but does not cover the Third Party Doorman or Third Party Notary Service. It also does not cover support for the Corda Software. Support for the Corda Software, if any, is provided under a separate agreement.

All time definitions are made in accordance to UTC +0.

Capitalized terms used herein and not otherwise defined shall have the meanings ascribed to them in the Participant Terms of Use.

Documentation:

User Guide: Joining The Corda network

Service Definition - The Network Map

Service Definition - The Notary

Service Definition - The Doorman

1.1 Assumptions and Certain Definitions

- The Corda network is a shared system, and other Corda Network Participants may be accessing the Services. Therefore, SLAs that refer to the processing of requests or transactions within a specified time period refer to all requests from all Corda Network Participants in all Business Networks. While R3 will endeavour to treat requests from all Business Networks equally, at times requests related to certain Business Network may experience different levels of service than requests related to other Business Networks.
- R3 reserves the right to suspend some or all Services if and to the extent that any Corda Network Participant violates the Participant Terms of Use or such Participant's use of the Services materially and adversely affects R3 operations or delivery of the Services (for example, by causing virus outbreaks or security issues). Requests from suspended Participants will not be counted towards determination of service levels.

1.2 Nominated Individuals

Either party may replace nominated individuals by providing notice in accordance with the Participant Terms of Use.

2.0 Service Level Agreement

2.1 General

Reporting and Measurement

R3 will periodically report on the average service levels for each of the Services across all Business Networks.

Downtime

Scheduled Downtime / Service Window ("Scheduled Downtime")

- Maintenance windows for all Services will be scheduled each Saturday from 10:00 UTC+0 until 18:00 UTC+0 (adjusted for British Summertime BST)
- R3 may from time to time announce additional maintenance windows for upgrades or service migrations. These will be published in advance along with the release schedule.
- A reminder for a maintenance window will be sent to relevant Corda Network Participants, via email, 24 hours prior to the start of the maintenance window, including a schedule of works that will be performed

Unscheduled Service Downtime/Outage

- In the unlikely event that a Service is not available for normal business access by at least a majority of Corda Network Participants during operational hours, then the event will be treated as an Incident and will be classified as per the standard severity definitions provided in the Support Services Schedule. R3 will subsequently follow its defined Incident management process.

Excused Failures

Failure to meet any service level will be excused to the extent the following circumstances are present:

1. The failure of, or problems relating to the Services, connections, software, firmware or equipment not under the control of R3;
2. Actions or inactions of any Corda Network Participant, or third-party vendor thereto (other than R3 and its subcontractors);
3. Misuse of any of the Services, or use of any Services other than as permitted in the Participant Terms of Use or the Documentation;
4. Failure of Participant to meet any of its obligations set forth herein;
5. Migration or upgrades;

6. R3's exercise of its rights to suspend or revoke any of the Services as permitted pursuant to the Participant Terms of Use;
7. Any action of any governmental authority requiring the suspension of any Service; or
8. Any Force Majeure event (as defined in the Participant Terms of Use), so long as R3 complies with reasonable disaster recovery procedures and provides to Participant at least the same level of service during such Force Majeure event as provided to other Corda Network Participants.

2.2 Performance Levels

R3 Doorman

Turnaround of certificate signing requests ("CSRs") is measured from time of the acknowledged receipt by R3 of a correctly formatted CSR and all other required information (including confirmation that the requestor has executed the Participant Terms of Use) to the time at which R3 makes a new certificate available to the node requesting access to the Corda Network. The R3 Doorman process can handle multiple certificate signing requests in parallel. Upon receipt of a CSR, R3 will send a confirmation email to the email address contained in the CSR. A response will be required before the CSR progresses further.

The service levels below are dependent on receiving a correctly formatted CSR. The R3 Doorman may reject a CSR if the data is not constructed according to the standards set out in the User Guide: Joining The Corda network. If a CSR must be resubmitted, the time to completion will be measured from the time the revised CSR is submitted.

- 95% of Certificate Signing Requests will be completed within two (2) Business Days of R3's receipt of a properly formatted and accepted CSR and the provision of all information required in connection therewith as per User Guide: Joining The Corda network.
    - If R3 requires further information from Participant regarding a properly formatted CSR, that information must be provided before the two (2) Business Day time period begins.
- A maximum of fifty (50) CSRs can be handled in parallel without impacting the above service level.
    - Should the number of outstanding CSRs exceed fifty (50) at any time (including CSRs for all Business Networks) the corresponding service level for that period will increase to four (4) Business Days.

CSRs received outside of supported hours of business (see section 2.3) will be deemed received at 08:30 UTC+0 on the following Business Day.

R3 Network Map Service

Turnaround of network map updates as a result of successful certification of a new node is measured from the time a new node.info file is received by the R3 Network Map Service to the time at which the updated network map is placed upon on the distribu-

tion site(s) maintained by R3. Corda Network Participants are responsible for updating their own nodes with the revised information.

- 95% of R3 Network Map updates for new nodes will be completed within 1 hour of the network map receiving an updated node.info file.

Turnaround for R3 Network Map updates received during Downtime will be deemed to begin from the cessation of Downtime. "Downtime" means Scheduled Downtime and Unscheduled Downtime.

R3 Notary Service

The turnaround time for transaction notarization request is measured from the point that an inbound request is received on R3 infrastructure to the point at which the reply leaves R3 infrastructure. The turnaround time will only be applicable to correctly formatted and structured notarization requests from a Corda Network Participant that has a properly issued Participation Certificate. Turnaround times are applicable up to a rate of 1 notarisation (with 10 or fewer input states) request per second as an aggregate of all nodes.

Notarization requests are treated individually, in sequence of receipt, by the R3 Notary Service working from an inbound queue. The speed of processing of requests depends on the complexity of the transactions received, in particular the number of input states.

- 95% of transactions (with 10 or fewer input states) will be notarised within sixty (60) seconds of being received by the R3 Notary Service.

Turnaround for notarization requests received during Downtime will be deemed to begin from the cessation of the Downtime.

2.3 Availability Levels

R3 Doorman Service

- The R3 Doorman Service will be available to receive new CSR's and associated technical messaging from Monday through to Friday, where Monday begins at 0:30 UTC+0 and Friday ends at 21:30 UTC+0, apart from Scheduled Downtime windows.
- The service will operate with 99% availability during these times
    - Uptime will be measured using DataDog Manage Monitors.
    - As a secondary check point, in case of dispute, ticket data from Jira will be used to verify uptime.

R3 Network Map Service

- The R3 Network Map will be available Monday through to Friday, where Monday begins at 0:30 UTC+0 and Friday ends at 21:30 UTC+0, apart from Scheduled Downtime windows.
- Each service will operate with 99% availability during these times
    - Uptime will be measured using DataDog Manage Monitors

R3 Notary Service

- The R3 Notary Service will be available 99% of the time apart from Scheduled Downtime windows.
- It will operate with 99% availability during these times
    - Uptime will be measured using DataDog Manage Monitors
    - As a secondary check point, in case of dispute, ticket data from Jira will be used to verify uptime.

Corda Network Support Services Handbook

1.0 Introduction & Scope

This is a handbook for support of the Corda Network Services to document such support services ("Support").

This handbook shall be effective throughout the term of the Participant Terms of Use and may be updated by R3 upon notice to Participant from time to time. All time definitions are made in accordance to UTC +0. "Normal Business Hours" are from Monday 00:30 UTC+0 to Friday 21:30 UTC+0. A "Business Day" is between 9:00 UTC+0 and 17:00 UTC+0 during Normal Business Hours.

1.1 Types of Support

Support is only provided for unexpected errors, exceptions or behaviour applicable to the Services in the Corda Network and is not provided for Participant's individual Business Networks.

1.2 Participant Responsibilities

Participant is responsible for the obligations set out below and acknowledges that the commitments provided by R3 are dependent on the performance of those obligations.

- Designate nominated individuals (employees of Participant) who will be responsible for engaging the Support Services by contacting R3 via designated methods of accessing Support using their pre-authorised credentials. Individuals who are not nominated individuals are not permitted to engage the Support Services.
- Ensure that nominated individuals are suitably qualified and experienced, and are familiar with the Corda Network.
- Provide access to required diagnostic information such as log files, configuration files, crash dumps, etc.
- Provide R3 with a list of contacts for escalations and emergencies. It is recommended that this list includes email groups with more than one individual.
- Meet the minimum technical requirements to use the Corda Network and the Corda Software and properly install the Corda Software, as set forth in the Corda documentation.
- Provide relevant training to individuals who will be using the Corda Network.
- Provide R3 with all reasonable co-operation to facilitate the efficient discharge of its obligations under this Agreement.
- Apply all patches and upgrades in a timely fashion after testing in a non-production environment.
- Perform quarterly forecasts of volumes for use of Support upon which R3 can reasonably rely in capacity planning.

To the extent possible, and as requested by R3, Participant may also be required to provide R3 or its authorized technical representative access to its source code in order to diagnose an Incident or otherwise provide Support. Participant acknowledges that if access is not provided as requested by R3, response times, Incident determination and Incident resolution will be slower, impaired or impossible. R3 will treat all source code as confidential and will not share it with anyone outside of R3's firm. R3 will also take reasonable steps to ensure only engineers designated to investigate the Participant's Incident or provide Support to Participant request are given access to Participant's source code. R3 will not, under any circumstances, access or take action within Participant's own environments but may provide guidance, advice, workaround suggestions or code fixes to Participant's own support personnel who do have such access and rights.

From time to time R3 may request that nominated individuals carry out procedures or changes to source or configuration to establish a diagnosis or test a potential fix. These procedures and changes may be destructive in nature or have unexpected adverse effects, and while the R3 support team will take every reasonable effort to advise of any impact, it is the nominated individuals' responsibility to apply due-diligence and ensure they are complying with their organisation's change and backup policies.

Nominated Individuals - Participant

Participant may replace nominated individuals by providing notice in accordance with the underlying agreement.

Stakeholder Role	Current Incumbent	Email Address	Main Responsibilities

2.0 Support

An "Incident" is a Participant problem caused by a malfunction in the Corda Network Services where the Services do not operate in the way stated in the SLA.

R3 is not in control of how Participant's CorDapp manages workload on its and other CorDapp users' hardware and operating systems, and so issues of performance or capacity overload caused by the CorDapp's use of the Corda Software are explicitly excluded from the definition of "Incident," as long as the Corda Services are working in accordance with the SLA.

2.1 Before contacting Support

To resolve a request for Support in the most expedient way possible, the nominated individual will need to gather sufficient information about the problem before engaging the R3 support team.

Defining the Problem

It is important to be as specific as possible when describing a problem or question in a support ticket. At a minimum, the questions below should be answered with as much detail as necessary:

- What were you expecting to happen, and what happened instead?
- What is the impact to your CorDapp and your application or service as a whole?
- Is there a workaround available and, if so, what is it?
- Can the problem be re-created easily in a test or development environment? If so, what steps are required?
- Are you seeing any exception messages or other diagnostic information and, if so, what are they? (include full stack traces of all exceptions)
- For how long has this problem been occurring?
  Has the problem happened before? What was the previous resolution or workaround?
- What recent changes have been made to the application and/or its environment?

Gather Relevant Technical Information

To analyse and diagnose problems effectively, the support team needs to have as much technical information about the problem as possible. Large or numerous files (e.g. logs) can be zipped together and attached to the ticket separately. At a minimum, the following items should be included on the support ticket:

- Corda version number
- Operating system and version
- Java version
- Full trace of any exceptions output to the console or terminal
- All relevant node logs which can be found in the logs directory of each node
- Any available code

- How the Corda node(s) was deployed
- How the Corda node(s) is being started and stopped (e.g. through batch files, shell scripts, containers, systemd)
- Screen-shots, if available
- Any other logs (e.g. network traces/vmstat output)

2.2 Incident Classifications

Incident will be classified by R3, in discussion with Participant, in accordance with the following levels of severity applicable to each Service:

Doorman Service

Severity 1: N/A

Severity 2: Major Impact. A detrimental situation caused by an error in the Corda Foundation Doorman Service in which the performance for responding to Certificate Signing Requests is above four (4) Business Days; or key functionalities of the Doorman Service are not accessible without manual workarounds, thereby causing a significant impact on business operations. Severity 2 applies strictly to a commercial production environment and for the Doorman Service run by the Corda Foundation only.
Severity 3: Moderate impact. The service's impairment is caused by unexpected behaviour in the Corda Foundation Doorman Service, but still maintains its key functionalities; for example, the impairment could be caused by unusually high volumes of certificate signing requests. The service impacted is not critical, thereby causing little, or having limited, impact on business operations.
Severity 4: Little Impact. A noticeable situation, caused by an error in the Corda Foundation Doorman Service, in which use of the service is affected in some cosmetic or ergonomic way and has minimal impact causing no significant impact on business operations, or an issue which is reasonably correctable by a documentation change or by a future, regular release from the Corda Foundation.

Network Map Service

Severity 1: N/A
Severity 2: Major Impact. A detrimental situation caused by an error in the Corda Foundation Network Map Service in which the performance for updating the network map takes more than two (2) hours during Normal Business Hours; or key functionalities of the Network Map Service are not accessible without manual workarounds, thereby causing a significant impact on business operations. Severity 2 applies strictly to a commercial production environment and for the Network Map service (and associated infrastructure) run by Corda Foundation only.
Severity 3: Moderate impact. The service's impairment is caused by unexpected behaviour in the Corda Foundation Network Map, but still maintains its key functionalities; an example would be an impairment caused by receiving higher volumes of requests to update the Network Map. The service impacted is not critical, thereby causing little or having limited impact on business operations.

Severity 4: Little Impact. A noticeable situation, caused by an error in the Corda Foundation Network Map, in which use of the service is affected in some cosmetic or ergonomic way and has minimal impact causing no significant impact on business operations, or an issue which is reasonably correctable by a documentation change or by a future, regular release from the Corda Foundation.

Notary Service

Severity 1: Critical Impact. An emergency situation caused by an error in the Corda Foundation Notary Service which critically impairs more than 25% of the total network participants to conduct business until it is rectified, or a workaround is in place. Such incidents are typically characterised by the loss of entire application systems, infrastructure components or data sets and will cause material financial, reputational, compliance, or customer service impact (or significant increase in risk of impact) if not resolved quickly. Severity 1 applies strictly to a commercial production environment and for Notaries run by the Corda Foundation only.
Severity 2: Major Impact. A detrimental situation caused by an error in the Corda Foundation Notary Service in which the application performance degrades substantially below 95% of transactions being notarised within 60 seconds (for flows with less than 10 input states); or key functionalities of the Notary Service not being accessible without manual workarounds, thereby causing a significant impact on business operations. Severity 2 applies strictly to a commercial production environment and for Notaries run by the Corda Foundation only.
Severity 3: Moderate impact. The Corda network is impaired caused by unexpected behaviour in the Corda Foundation Notary Service, but still maintains its key functionalities, and the impairment is caused by an error in the Notary. The component impacted is not critical to the application, thereby causing limited impact on business operations.
Severity 4: Little Impact. A noticeable technical impairment caused by a minor error in the Corda Foundation Notary Service, in which use of the service is affected in some cosmetic or ergonomic way and has minimal impact causing no significant impact on participant operations, or an issue which is reasonably correctable by a documentation change or by a future update to the Corda Foundation Notary Service by the Corda Foundation.

Accessing Support

Submitting Support Requests

a. R3 shall provide Participant with a web link to make requests for Support and report errors, which shall be the primary method for reporting errors. R3 will also provide a method for escalating errors via a dedicated telephone number and email address for Support should the response fall outside the stated service levels. For clarity, the telephone number and email is not a substitute for the primary contact method, which is essential to ensuring that the error is properly reported and classified, and for the commencement of support activities.

b. Participant agrees that all errors and Support requests will be reported via the channels described in item a above, and any attempts to use other channels (e.g. direct contact with R3 employees or over public internet forums and chat channels) may trigger delays in response and resolution of the error.

Through R3 Support Portal or R3 Services site(s), you may post support incidents electronically to the R3 support specialists. This service desk portal allows you to put all of the pertinent information about your problem into the problem record via the Internet without having to wait for someone to call you back. This should save you time and help with problem resolution time.

If you are submitting or updating a severity one problem or raising the severity of an existing problem to severity one and it is outside of Normal Business Hours in your country you should open your problem by voice or follow-up your web submission with a call to your local support center referencing the problem number you receive on the web. We want to ensure that your emergency call will be handled appropriately.

2.2 Response Targets

R3 shall use commercially reasonable efforts to respond to all Incident reports and requests for support as provided below.

Severity 1: After R3 acknowledges that an Incident qualifies as a Severity 1 issue, R3 and Participant will work diligently to resolve it. R3 shall acknowledge Severity 1 calls within two (2) hours from the time the issue was reported. In addition, R3 shall, at R3's expense, (a) immediately assign an appropriate number of qualified resources to reasonably work towards correction of the Incident 24-hours a day, 7-days a week until R3 has provided a functional workaround or permanent fix or the issue is no longer defined as Severity 1; and (b) regularly report on the status of the corrections if the issue remains after four (4) hours at a schedule agreed with the Participant. An appropriate number of Participant resources must be made available in Severity 1 situations and reasonably cooperate to help resolve the issue.

A Severity 1 issue may be immediately downgraded if one of the following occurs: (i) a functional workaround has been implemented that has enabled the application to restart and continue normal service; (ii) during the course of the investigation R3 determines that R3's systems are not the cause of the issue; or (iii) Participant confirms the severity can be reduced for other reasons; or (iv) Participant fails to provide appropriate resources to work with R3 at any time.

Severity 2: After R3 acknowledges that an Incident qualifies as a Severity 2 issue, R3 shall acknowledge Severity 2 calls within four (4) Normal Business Hours from the time the issue was reported. In addition, R3 shall, at R3's expense, (a) promptly assign an appropriate number of qualified resources to work towards correction of the Incident until R3 has provided a functional workaround or permanent fix; and (b) report on the status of the corrections not less than every Business Day.

A Severity 2 issue may be upgraded if the workaround no longer hides the impact of the issue, or if the workaround does not work. A Severity 2 issue may be downgraded if one of the following occurs: (i) a permanent fix has been implemented to remove the need for the workaround; or (ii) during the course of the investigation it has been determined that R3's systems are not the cause of the issue; or (iii) Participant confirms the severity can be reduced for other reasons; or (iv) Participant fails to provide appropriate resources to work with R3 at any time.

Severity 3: After R3 acknowledges that an Incident qualifies as a Severity 3 issue, R3 shall acknowledge Severity 3 calls within twenty-four (24) Normal Business Hours from the time the issue was reported. In addition, R3 shall, at R3's expense, then assign an appropriate number of qualified resources to work towards correction of the Incident until R3 has provided a functional workaround or permanent fix.

A Severity 3 issue may be upgraded if the impairment spreads to key functionalities of the application. A Severity 3 issue may be downgraded if one of the following occurs: (i) during the course of the investigation it has been determined that R3's systems are not the cause of the issue; or (ii) Participant confirms the severity can be reduced for other reasons.

Severity 4 or Information Requests: After R3 acknowledges that an Incident qualifies as a Severity 4 issue, R3 shall acknowledge Severity 4 calls within two (2) Business Days from the time the issue was reported. R3 would normally undertake to address such issues in future releases. R3 shall respond to enquiries that do not involve the report of an Incident as soon as is practical, taking account of volumes of such queries and incidents in process at the time. R3 will take all reasonable steps to provide an answer to the request.

A Severity 4 may be deemed to be closed or unresolved if one of the following occurs: (i) during the course of the investigation it has been determined that R3's systems are not the cause of the issue; or (ii) Participant confirms the severity can be reduced for other reasons.

2.3 Escalation

R3 will provide to Participant contact information for its support escalation team, which may be contacted only in the event a Severity 1 or Severity 2 Incident not being handled according to the service levels described above.

2.4 How your service request is handled by R3 Software Support

Submitted incident requests are logged into the R3 problem management system. Once logged, a unique service request record ("ticket") is created. Please make note of the ticket number and use it in any future communication on this issue with the support center. Your service request is routed to a resolution team for handling. A resolution team is simply a group of software support specialists and software engineers. You will

be contacted by a specialist in the appropriate resolution team as described in section 2.2.

Your service request is researched, resolved, or escalated as appropriate. In order to investigate the issue, R3 may need to access information on your system relative to the failure or may need to recreate the failure to get additional information. Should the problem be configuration related, it is possible you may need to recreate the problem to get that required information. Our support specialists may request that you send in the problem information or test cases or that they be able to view it with you electronically.

2.5 How technical questions (how-to/install) are handled by support

Technical question support allows you to obtain assistance from R3 for questions regarding connecting to and using Corda Network Services. In the course of providing answers to your technical questions, we may refer you to product documentation or publications, or we may be able to provide a direct answer to assist you in the following areas:

Short duration problems involving

- Installation
- Usage (how-to)
- Specific usage/installation questions for documented functions
- Product compatibility and interoperability questions
- Technical references to publications such as user guides and technical manuals
- Providing available configuration samples
- Planning information for software fixes

The following are examples of areas that are out of scope:

- Analyzing performance
- Writing, troubleshooting or customizing code for a customer
- Answering extensive configuration questions
- Recovering a database, or data recovery
- Consulting
- Interpretation or triage of Participant or third party generated defect scanning reports
- Training

3.0 Exclusions

3.1 Exclusions

Support does not include provision of new or separate products, or major features, which R3 offers for an additional fee to its customers generally.

Support does not include customized or bespoke modifications created by R3 for a single third party or group of third parties.

No on-site Support will be provided.

- Support will not be provided with respect to any services other than the Corda Network Services, and will not be provided with respect to incidents caused by or incurred in connection with an unauthorized or unspecified use of the Corda Software.
- Support will not include general training on use of the Corda Software.
- Support will not be provided with respect to Incidents caused by any reason external to the Corda Software, including failure or fluctuation of electrical supplies, inadequate cooling, or equipment.

4.0 Your responsibilities

R3 does not warrant that the Services products are defect free, however we do endeavor to fix them to work as designed. Our remote Support is available to provide you assistance and guidance, however we assume that you will provide information about your system and the failing component, information that is key to resolving the problem.

This information includes capturing documentation at the time of a failure, applying a trap or trace code to your system, possibly formatting the output from the trap or trace, and sending documentation or trace information, in hardcopy or soft copy, to the remote support center. You are also responsible for obtaining fixes, by downloading or by receiving ones that have been shipped to you on media, applying the fixes to your systems and testing the fixes to ensure they meet your needs. Occasionally, removal of installed fixes may be necessary in the process of isolating problems. And sometimes fixing a problem will mean the installation of a later release of the software as some fixes cannot be retrofitted into earlier code.

Both parties acknowledge and agree that they will comply with all the provisions of the EEA Data Protection Addendum attached hereto as Exhibit A.

EXHIBIT A

EEA Data Protection Addendum

Scope

The terms in this EEA Data Protection Addendum ("Addendum") apply to all services in Appendix A (the "Services") which involve processing of personal data by R3 which is subject to GDPR. This Addendum forms part of the agreement (the "Agreement") between the customer (the "Participant") and R3. This Addendum applies to the processing of Personal Data, with subject to the EU General Data Protection Regulation 2016/679 (hereinafter "GDPR"), by R3 LLC ("R3") on behalf of Participant. Terms used herein and not otherwise defined shall have the meanings ascribed to them in the GDPR.

Processing of Participant Data; Ownership

R3 and Participant agree that with regard to the processing of Personal Participant Data, Participant is Controller and R3 is Processor. R3 will process the personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

R3 is not responsible for any personal customer data stored or otherwise used with any R3's proprietary software or on any network provided by R3.

Disclosure of Participant Data

R3 will not disclose Personal Participant Data outside of R3 and its affiliates and third-party vendors facilitating business for R3 except (1) as Participant directs, (2) as set forth in the Agreement, or (3) as otherwise required by law.

If a law enforcement agency or other third party contacts R3 with a legally binding demand for Personal Participant Data, R3 will attempt to redirect the third party to request that data directly from Participant (and for this purpose, R3 may disclose Participant's basic contact information to that third party). If compelled to disclose Personal Participant Data to a law enforcement agency or other third party, R3 will as soon as reasonably practicable notify Participant and provide it with a copy of the demand unless legally prohibited from doing so.

Processing Details

The parties acknowledge and agree that:

- The subject-matter, nature and purpose of the processing is limited to Personal Participant Data as defined by and within the scope of the GDPR;
- The duration of the processing shall be for the duration of the Participant's right to use the Service and until all Personal Data is deleted or returned in accordance with Participant instructions or the terms of the Agreement;
- The nature and purpose of the processing shall be to provide the Service pursuant to the Agreement;
- The types of Personal Data processed by the Online Service include those expressly identified in Article 4 of the GDPR; and
- The categories of Data Subjects are Participant's representatives and end users, such as employees, contractors, collaborators, and customers.

If R3 receives a communication from a Data Subject seeking to exercise any of his or her rights under articles 12 to 23 of the GDPR, R3 will redirect the Data Subject to make its request directly to Participant. R3 will comply with reasonable requests by Participant to assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the Processor.

Cooperation

R3 will assist with any audits conducted by the Controller or another auditor mandated by the Controller. The Participant shall reimburse R3 for any reasonable and demonstrable expenses relating to any such audit. Participant and R3 shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate.

Data Security

Security Practices and Policies

R3 will maintain appropriate technical and organizational measures to protect Personal Participant Data. R3 reserves the right to amend the security measures that it has in place to protect Personal Participant Data (or equivalent), and/or its description of them, by amending the relevant web pages from time to time, provided that it does not materially reduce the level of security provided.

Participant Responsibilities

Participant is solely responsible for making an independent determination as to whether the technical and organizational measures set out in Appendix B ensure a level of security appropriate for the Personal Participant Data, including meeting any of Participant's security obligations under the GDPR or other applicable data protec-

tion laws and regulations. Participant will indemnify, defend, and hold harmless R3 from and against any and all losses (i) in respect of or arising out of any third party claim against R3 alleging that the measures set forth in Appendix B are insufficient or otherwise fail to comply in any respect with the requirements of the GDPR or (ii) arising or resulting from any breach of the GDPR by R3 in connection with the measures set forth in Appendix B. Participant acknowledges and agrees that taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Persona Participant Data as well as the related risks to individuals the technical and organizational measures implemented and maintained by R3 provide a level of security appropriate to the risk with respect to its Personal Participant Data. Participant is responsible for implementing and maintaining privacy protections and security measures for components that Participant provides or controls.

Security Incident Notification

If R3 becomes aware of a personal data breach which are likely to result in a risk to the rights and freedom of natural persons while processed by R3 (each a "Security Incident"), R3 will without undue delay (1) notify Participant of the Security Incident and provide Participant with detailed information about the Security Incident; (2) investigate the cause of the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Participant's administrators by any means R3 selects, including via email. It is Participant's sole responsibility to ensure Participant's administrators maintain accurate contact information on each applicable Service portal. Participant is solely responsible for complying with its obligations under incident notification laws applicable to Participant and fulfilling any third-party notification obligations related to any Security Incident, but R3 shall give Participant such assistance as Participant reasonably requests and R3 is reasonably able to provide in relation to the performance of any such third party notification obligations which arise as a result of a breach by R3 of this Addendum.

R3's obligation to report or respond to a Security Incident under this section is not an acknowledgement by R3 of any fault or liability with respect to the Security Incident.

Participant must notify R3 promptly about any possible misuse of its accounts or authentication credentials or any security incident related to a Service.

Data Transfers and Location

Personal Participant Data that R3 processes about the Participant may be transferred to, and stored and processed in, the United States or any other country in which R3 or its affiliates or sub-contractors ("Subprocessors") with access to Personal Participant Data operate. Participant appoints R3 to perform any such transfer of Personal Participant Data to any such country and to store and process Personal Participant Data to provide the Services. All transfers of Personal Participant Data to a third country or an international organization will be subject to appropriate safeguards as described in Article

46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

Data Retention and Deletion

After Participant disables its account and upon expiration of the applicable retention periods, unless R3 is required to retain Personal Participant Data under European Union or Member State laws, R3 shall delete Participant Data.

Processor Confidentiality Commitment

R3 will ensure that its personnel engaged in the processing of Personal Participant Data will be obligated to maintain the confidentiality and security of such data, including after their engagement ends.

Notice and Controls on use of Subprocessors

R3 may hire third parties to provide certain limited or ancillary services on its behalf. Participant consents to the engagement of these third parties and R3 affiliates as Subprocessors. Agreement to these terms constitutes Participant's prior written consent to the subcontracting by R3 of the processing of Personal Participant Data to its Subprocessors, if such consent is required. R3 shall ensure that each Subprocessor is bound by a written contract imposing on the Subprocessor materially the same data privacy and data security obligations as are accepted by R3 in this Addendum (as applicable to the Subprocessor) or other obligations which similarly meet the requirements of article 28(3) of the GDPR. A list of third party Subprocessors can be found in Appendix A.

From time to time, R3 may engage new Subprocessors. R3 will give Participant notice by updating the www.corda.net website and providing Participant with a mechanism to obtain notice of that update of any new Subprocessor other than an affiliate of R3 at least 14-days in advance of providing that Subprocessor with access to Personal Participant Data.

If Participant does not approve of a new Subprocessor receiving Participant Personal Data, then Participant may terminate any subscription for the affected Online Service. If the affected Online Service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. To terminate a service, please send a written notice to legal@r3.com. All fees paid will be forfeited by Participant.