Supplemental terms DORA

between TellusTalk, LEI.no 89450035BKH9VKE92U17 and Financial entity under Article 2 of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, as amended from time to time.

These supplemental terms (the “Supplemental Terms”) refer to the Service Agreement entered into by and between

(1) The party who orders and uses TellusTalks services, and thereby confirms that they accept our General terms & conditions, and to whom DORA is directly applicable, ”the Customer”, and

(2) TellusTalk AB, corporate identity number 556429-8213, LEI 89450035BKH9VKE92U17, Kungsgatan 37, 8 tr, 111 56 Stockholm, Sweden “the Supplier”,

hereinafter jointly referred to as the “Parties” and separately as a “Party”,

as may have been amended, updated, or restated from time to time, collectively referred to as the “Agreement”.

Unless separately defined in these Supplemental Terms, words, phrases and expressions defined in the Supplemental Terms shall have the meaning as set out in the Agreement.

The governing law and dispute resolution provisions of the Agreement shall apply mutatis mutandis to the terms of these Supplemental Terms.

Except as set out in these Supplemental Terms, the Agreement shall continue in full force and effect.

The Supplemental Terms come into effect on 17 January 2025 and shall as of this date form an integral part of the Agreement.

Definitions
In these Supplemental Terms, the following terms and expressions will have the following meaning unless the context otherwise requires:

“Competent Authority”	means any court, governmental body, regulatory authority in Sweden or the European Union.
“DORA”	means Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, as amended from time to time.
“ICT”	means information and communication technology.
“Lead Overseer”	means the European supervisory authority appointed in accordance with Article 31(1), point (b) of DORA.

between TellusTalk, LEI.no 89450035BKH9VKE92U17 and Financial entity under Article 2 of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, as amended from time to time.

“Resolution Authority”	means an authority designated by a member state in accordance with Article 3 in Directive 2014/59/EU (Bank Recovery and Resolution Directive). In Sweden; the Swedish National Debt Office (Swe: Riksgälden).
“Services”	means the services, which support relevant functions at the Customer, provided by the Supplier as agreed by the Parties in the Agreement.

Supplemental Terms according to DORA Article 30.1 and 30.2

30.1 Background, purpose and structure

The Parties entered into the Agreement on the date stated above.

DORA is applicable in the European Union as of 17 January 2025. DORA is directly applicable to the Customer.

The supplier has not been identified by the Lead Overseer as a supplier of ICT services supporting critical or important functions.

These Supplemental Terms reflect the requirements stated in Article 30(1) and 30(2) of DORA. The Supplier does also comply with some of the requirements stated in Article 30(3) of DORA.

If the Services are supporting a critical or important function, the Customer must have a separate agreement with the supplier stating the requirements of the Service.[1]

The Parties have agreed to these Supplemental Terms to clarify their respective responsibility pursuant to the Agreement in the light of the introduction of DORA.

The purpose of these Supplemental Terms is to describe the requirements that the Supplier shall comply with in relation to the Customer, in general as well as specifically relating to the Services.
To the extent any of the terms contained in these Supplemental Terms conflict and/or are inconsistent with the terms of the Agreement, unless otherwise specifically stated herein, the provisions in these Supplemental Terms shall prevail.

Notwithstanding any provision in the Agreement regarding the choice of law, the interpretation, validity, and enforcement of these Supplemental Terms shall be governed by and construed in accordance with DORA. In the event of any conflict between the

1 DORA Art. 29.1

applicable law chosen for the Agreement and DORA, DORA shall prevail as regards these Supplemental Terms.

30.2

2.a Subcontractors[2]

The Supplier agrees to notify the Customer before using a subcontractor, or implementing material changes to a pre-existing subcontracting arrangement, for the performance of the Services under the Agreement. If applicable, the Supplier agrees to promptly inform the Customer of any preexisting subcontractor that has not yet been notified to the Customer before the entry into force of these Supplemental Terms. For the sake of clarity, it is noted that only subcontractors who are necessary for the delivery of the Service are covered by the current definition of subcontractor. This excludes for example suppliers of consumables.

For the Customer to be able to assess the impact of the risks it is or might be exposed to, the Supplier is responsible for notifying the Customer 30 days in advance of new subcontracting arrangements or material changes thereof. For the avoidance of doubt, it is hereby clarified that, if a longer notification period has been previously agreed upon within the terms of the Agreement, such longer period shall supersede and be applied in lieu of the 30 days period expressly mentioned herein. The Customer shall have the right to request a subcontractor to be excluded from the processing of the Customer´s data should the Customer object to a subcontracting arrangement. The Supplier shall inform the Customer if such exclusion is possible or will affect the scope of the Services. The Customer shall also have the right to terminate the Agreement pursuant to section 8 should the Customer object to a subcontracting arrangement. Such objection and notice of termination by the Customer shall be based on factual ground and provided in writing to the Supplier within thirty (30) days after notification of a new subcontracting arrangement.

The Supplier shall enter into a Data Processing Agreement with all engaged subcontractors.

The Supplier shall ensure that all engaged subcontractors comply with the Supplier´s Supplier Code of Conduct.

To the extent that the Supplier engages subcontractors, the Supplier is fully liable for the subcontractor. The Supplier is hence responsible for any subcontractor’s acts or omissions as for its own part pursuant to the Agreement. The Supplier is responsible to maintain the adequate level of oversight and control of any subcontractor to fulfil its duties pursuant to the Agreement.

2 DORA Art 30.2(a)

between TellusTalk, LEI.no 89450035BKH9VKE92U17 and Financial entity under Article 2 of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, as amended from time to time.

2.b Location of data processing[3]

The Supplier agrees to inform the Customer about where the Supplier´s data is to be processed, including the storage location.

Upon notifying the Customer pursuant to 2.a, the Supplier agrees to inform the Customer about where the subcontractor's data is to be processed, including the storage location. This clause shall not apply if the subcontractor is not to process or store any data pertaining to the Customer.

The Supplier shall inform the Customer whether any approved subcontractor envisages changing of such location.

2.c Information security[4]

The Supplier shall manage relevant ICT risks and comply with appropriate information security standards regarding availability, authenticity, integrity, and confidentiality concerning the protection of data, including personal data, relevant for the Service delivery.

Appropriate information security standards are those that are widely accepted within the industry, including but not limited to ISO/IEC 27001, NIST Cybersecurity Framework, and ISF Standard of Good Practice. Under all circumstances, appropriate information security standards shall at least address the control objectives below.

Governance arrangements for data and services are initiated by top management and documented (governance arrangements), including but not limited to: documented policies, standards and procedures covering necessary topics; a risk-based approach; regular review and approval of policies, standards and procedures by appropriate level of management; and regular control procedures to ensure compliance with policies and standards.

Changes to data and services are authorized, tested, approved, implemented and documented (change control), including but not limited to: segregation of development and production environments; and concern for separation of duties between responsibilities.

Logical access to data and services is restricted to authorized individuals only (access control), including but not limited to: lifecycle management of identities; procedures to update access rights for individuals joining, moving and leaving; procedures to regularly review access rights; appropriate use of passwords and

3 DORA Art 30.2(b)

4 DORA Art 28.5 and 30.2(c)

strong authentication technologies; and control of individuals' use of privileged access rights.

Operations ensure accurate processing of data and availability of services (IT operations), including but not limited to: backup procedures; redundant processing where appropriate; logging and monitoring capabilities; incident and problem management procedures; and disaster recovery procedures.

2.d Exit management[5]

The Supplier shall ensure that the Customer can get access to and return to the Customer all personal and non-personal data including recovery of all such data in case of insolvency, resolution or discontinuation of the Supplier's business operations.

The Parties acknowledge the importance of establishing effective exit strategies to mitigate risks and ensure the continuity of the Services. Hence, in the event the Agreement is terminated, the Supplier undertakes to assist the Customer to facilitate an orderly and efficient transfer of the Services affected by such expiry or termination to an alternate service provider or to the Customer such that the Services can be performed with a minimum amount of interruption and inconvenience to the Customer and its customer.

If the Supplier processes and/or stores data pertaining to the Customer, the Supplier agrees to cooperate to enable the access, recovery and return of the Customer's data in the case of termination of the Agreement and it is expressly noted that this provision also applies in a case of insolvency, resolution or discontinuation of the Supplier's business operations.

Upon the Customer's request, and unless the Supplier is required to retain the Customer's data pursuant to law or regulation, the Supplier shall provide written confirmation that the Customer owned information assets have been securely deleted from all Supplier-controlled IT assets, including storage devices, such as hard drives and backup tapes that are not handed over to the Customer at the termination of contract.

2.e Service level agreement[6]

The Supplier shall perform the Service in a professional manner with the allocation of adequate and appropriate resources and always use trusted Representatives who are suitable, qualified and skilled for the relevant tasks.

Delivery and monitoring

5 DORA Art 30.2(d)

6 DORA Art 30.2(e)

between TellusTalk, LEI.no 89450035BKH9VKE92U17 and Financial entity under Article 2 of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, as amended from time to time.

The Supplier has on average successful delivery status on 99,99% of correctly addressed messages. The Supplier can not guarantee delivery if the receiving carrier or government filters incoming messages. The Supplier provides a web portal where all transactions can be monitored by the Customer in real time. Incoming messages can also be downloaded from the web portal when needed. The Supplier provides delivery reports on sent messages. Delivery reports are sent when delivery is complete or when re-sending has ceased, this means that a report on failed delivery could be delivered up to a couple of days after the initial message was sent. Automatic and manual monitoring takes place continuously around the clock to ensure continuous operation. Alarms are triggered in the event of operational disturbances that are extensive. Due to the nature of the service, it is not always possible to determine whether a non-delivery is due to a malfunction or whether the number or receiving device is faulty. Therefore, it is important that the Customer takes measures in the event of missing delivery reports or delivered reports of failed delivery. These can be provided in different ways depending on the Customer's needs and wishes.

Stored data
The Supplier maintains information about the message, who sent the message and to what number and address the message was sent, as well as the time of dispatch and delivery. It is possible to set automatic log deletion times.

Support
Support is available around the clock by phone (+46(0)8 509 126 00 - press 3), or during office hours (weekdays 08:00-17:00 CET) by email (support@tellustalk.com). During office hours emails are normally handled within the hour. Status reports are communicated by phone or email.

Case management system
A case management system is part of the documentation routine and incoming cases are registered there. This takes place via telephone, e-mail or via a form on the website.

Escalation process
1.Registration, prioritization, overall troubleshooting and first report back within an hour. Applies to office hours for cases received via e-mail and 24 hours a day, every day, for cases received via telephone.
2.Problem resolution by support staff or 1st escalation to technician.
3.Resolution or status update from technician, otherwise 2nd escalation to manager technician.
4.Solution and report back.

Error classification
Classification of the case is done in consultation with the Customer.

Prio 1 - Function in the system does not work, or is not available. No reasonable alternative exists for users to solve their work task. The error causes degraded use of the system which means serious problems for many users.

Prio 2 - More important functions in the system are incorrect. Alternative ways exist for the user to solve their work task. The error causes significant problems for many users.

Prio 3 - Minor functional error of minor importance. Alternative ways exist for the user to solve their work task. The error may cause slight or negligible inconvenience to one or more users.

Response times

Prio	Time to 1st escalation	2nd escalation	Solution
1	2 tim	3 tim	6 tim
2	4 tim	6 tim	12 tim
3	1 working day	3 working days	7 working days

2.f Assistance upon ICT incident[7]

The Supplier is obliged to provide reasonable assistance to the Customer, at no additional cost, when an incident related to the Services occurs.

2.g Cooperation with authorities[8]

In relation to the Service delivery, the Supplier agrees to fully cooperate with all relevant Competent Authorities, the Lead Overseer if relevant, and Resolution Authorities or third parties appointed by them.

2.h Termination rights[9]

Without prejudice to any other rights or remedies conferred on the Customer under the Agreement, the Customer may terminate the Agreement (or any part of it), with immediate effect, without paying any penalty or termination fee, by giving written notice to the Supplier upon the occurrence of any of the following circumstances:

- If the Supplier defaults in the performance of any of its material obligations under the Agreement, and such default or breach continues and is not remedied within a period of thirty (30) days after the Customer has given

7 DORA Art 30.2(f)

8 DORA Art 30.2(g)

9 DORA Art 30.2(h)

written notice to the Supplier specifying such default or breach and requesting it to be remedied,[10]

- If the Supplier is, in a material manner, in breach of applicable law, regulations, guidelines or other relevant legislation or case law relevant to the performance of the Services under the Agreement and has not rectified the breach in accordance with the procedure stated above,[11]
- If the Customer has found and can demonstrate that there has been deterioration in the Service that may adversely affect the Supplier's performance of the Service or circumstances have been identified during the monitoring of the Supplier that are deemed to be capable of altering the performance of the Services, including material changes affecting the Agreement or situation of the Supplier,[12]
- If the Supplier has demonstrated weaknesses in its overall ICT risk management as further specified in section 2.c, and in particular the way in which it ensures the availability, authenticity, integrity, and confidentiality of data, whether personal data or other types of confidential information.[13]
- If a Competent Authority or Resolution Authority has given instructions that it is no longer able to effectively supervise the Customer because of the conditions of, or circumstances related to, the Agreement,[14]
- If the Customer receives a notification in accordance with section 2.a above from the Supplier and the Customer before the end of the time limit stated therein notifies the Supplier that it objects to the proposed subcontracting arrangement and the Parties do not reach an agreement within thirty (30) days.
- If the Supplier implements a new subcontracting arrangement, or a material change to a pre-existing subcontracting arrangement, without notifying the Customer in accordance with 2.a.

In the event of termination by the Customer pursuant to section 2.h, the Supplier is obliged to cooperate with the Customer as further specified in section 2.d.

The Parties acknowledge that the Customer, as an entity within the scope of Directive 2014/59/EU (also known as the Bank Recovery and Resolution Directive), should ensure that the Agreement is robust and fully enforceable in the event of resolution of the Customer. The Supplier therefore agrees that the Agreement cannot be terminated, suspended, or modified solely on grounds of restructuring or resolution if the Customer complies with the Agreement, including the payment obligations.[15]

10 DORA Art 28.7(a)

11 DORA Art 28.7(a)

12 DORA Art 28.7(b)

13 DORA Art 28.7(c)

14 DORA Art 28.7(d)

15 DORA recital 74 and Art 30.2(h)

2.i Security awareness training[16]

The Supplier shall develop ICT security awareness programmes and digital operational resilience training as compulsory modules in its staff training schemes. Security awareness programmes and training shall be applicable to all employees and to senior management staff, whereas digital operational resilience training shall be provided to relevant security personnel and shall have a level of complexity in proportion to their functions. The Supplier shall upon request provide evidence of its programmes and its applicability to the delivery of the Service to the Customer. The Supplier shall, if relevant to the delivery of the Service, offer reasonable participation in the Customers security awareness training, subject to the Parties agreeing in a subsequent separate agreement, on the place, time, agenda and further details for such ICT security awareness program or digital operation resilience training.

The Supplier will also comply with the following terms according to DORA Article 30.3

30.3

3.a Extended Service level agreement[17]

Not covered by these Supplemental Terms. Available under separate agreement if required.

3.b Reporting timelines[18]

The supplier shall notify the Customer of ICT incidents, that are classified as critical by the Supplier, related to the Service without unnecessary delay.

3.c Disaster recovery and business continuity[19]

The Supplier confirms that it has and will at all times during the term of the Agreement maintain a business continuity plan, appropriate for a professional provider of the Services, to secure continued services in case of unforeseen events. The business continuity plan shall include strategies for response to and recovery from potential disasters that could disrupt the operations and lay out the actions that need to be taken if normal business activities cannot be continued due to a disabling event, including but not limited to sudden staff shortage, IT-related break downs, natural disasters, fire and flood.

The Supplier undertakes to update its business continuity plan regularly and perform regular testing of such plan once per year or more often if required, as well

16 DORA Art 30.2(i)

17 DORA Art 30.3(a)

18 DORA Art 30.3(b)

19 DORA Art 30.3(c)

as, at the Customer's request, to provide a redacted copy of the most recent business continuity plan.

3.d Penetration testing[20]

The Customer or its appointed third party, shall be entitled to conduct ICT testing, including threat-led penetration testing of the Service as required. Both Parties shall mutually agree on the scope, time schedule and methodology of such testing, which shall be performed in accordance with industry standards and best practices.

3.e Audits and cooperation[21]

i. The Customer (itself or through a third party) and its auditors or, if applicable, relevant Financial Supervisory Authorities, shall be entitled to carry out audit(s) of the Supplier's business, in order to control that the Supplier meets its obligations according to the Agreement and to ensure compliance with all applicable Regulatory Requirements.

ii. Not covered by these Supplemental Terms. Available under separate agreement if required.

iii. The Supplier shall fully cooperate and participate in the preparations and performance of the audits and shall provide the Customer or the auditors of the Customer or the Financial Supervisory Authority (including persons appointed by the Financial Supervisory Authority), as applicable, access to the relevant premises and equipment, reply to questions that they may have and also provide them with all relevant information, documentation and material requested by them. If the Financial Supervisory Authority directly queries the Supplier, the Supplier must promptly respond to the Financial Supervisory Authority's inquiries.

The Customer will bear, and indemnify the Supplier against, all reasonable costs and expenses arising from the exercise of an audit described in this appendix regardless of whether it was exercised by the Customer or the Financial Supervisory Authority, except if significant non-compliance by the Supplier is identified during such audit. For the avoidance of doubt, reports or other information to which the Customer is expressly entitled to under the Agreement, shall be provided free of charge when reasonably requested.

Audit by Customer

The Parties agree that the Customer's audit rights shall be exercised in the following order:

-The Customer shall primarily use standard features of the Service and the information and documents provided by the Supplier to the Customer.

20 DORA Art 30.3(d)

21 DORA Art 30.3(e) i and iii

-If the information obtained via these means is not enough, the Supplier shall, upon Customer's request, provide the Customer with internal audit reports.
-If the information included in the audit reports is not enough, the Supplier shall provide the Customer, the Customer's auditor and/or an independent auditor engaged by the Customer rights of inspection and auditing. This includes providing access to relevant information and business premises (e.g. head offices and operation centers) used for providing the Service.
-The Customer shall observe the Supplier's reasonable confidentiality and security instructions when performing the audit. Such instructions shall not be more far-reaching or include other obligations than similar instructions applicable to the Supplier's Representatives.

Audit by Financial Supervisory Authority
In the event the Financial Supervisory Authority requests information relating to the Customer's use of the Service, the Customer will use its best endeavours to resolve that request directly with the Financial Supervisory Authority by using the standard features of the Services and the information and documents provided by the Supplier to the Customer.
If the Financial Supervisory Authority determines that the Customer's effort to resolve the request is insufficient, the Supplier will provide the Financial Supervisory Authority with rights of inspection and auditing. This includes providing access to relevant information and business premises (e.g. head offices and operation centers) used for providing the Service.
The Customer authorizes and expressly consents to giving the Financial Supervisory Authority access to Customer Data directly from the Supplier when, upon written request by the Financial Supervisory Authority, such access is required to enable the Financial Supervisory Authority's supervisory activities and the Financial Supervisory Authority cannot obtain such information directly from the Customer. The Supplier shall immediately notify the Customer upon receipt of such written request from the Financial Supervisory Authority.

iv. Audit(s) shall be carried out during business hours after giving reasonable notice to the Supplier.

Nothing in this section should be construed as a limitation of the right to information or audit that the Parties may have already agreed upon and which is therefore evident from the Agreement.

3.f Exit strategies[22]

22 DORA 30.3(f)

i. If it is necessary for the transition of the Service as mentioned in Section 11, the Customer may elect to extend the Service for as long as is necessary to secure the transition of the Service. During such period, the Supplier will continue to provide, and the Customer will continue to receive and pay for, the Service pursuant to the Supplier's standard terms and conditions and standard pricing.

ii. The Parties acknowledge the importance of establishing effective exit strategies to mitigate risks and ensure the continuity of the Services. Hence, in the event the Agreement is terminated, the Supplier undertakes to assist the Customer to facilitate an orderly and efficient transfer of the Services affected by such expiry or termination to an alternate service provider or to the Customer such that the Services can be performed with a minimum amount of interruption and inconvenience to the Customer and its customer.

These Supplemental Terms have been adapted by TellusTalk as a standard amendment to the Service agreement, where applicable.