ANNEX
on the implementation of the requirements of the DORA Regulation
(hereinafter: "DORA Annex")
concluded on [·]/[date of last electronic signature] between:

VERCOM S.A. with its registered office in Poznań, Poland ul. Wierzbięcice 1B, 61-569 Poznań, entered in the Register of Entrepreneurs of the National Court Register, kept by the District Court 400Poznań – Nowe Miasto and Wilda in Poznań, VIII Commercial Division of the National Court Register, under the number 0000535618, NIP 7811765125, REGON 300061423, LEI: 259400P9VT804CUH6G16, EUID: PLKRS.0000535618, with a share capital of PLN 444,475.70 paid in full,

hereinafter referred to as the "**Service Provider**", represented by [·] – [·]

and

[NAME] [·] – a [·] law company [·] with its registered office in [·], at: [·], entered in the commercial register kept by [·], under the number [·], with a tax identification number: [·],

hereinafter referred to as the "**Client**" represented by [·] – [·].

The Service Provider and the Client shall be hereinafter collectively referred to as the "**Parties**" or individually as a "**Party**".

Whereas:

1. *The Client is an entity obliged to fulfil the duties imposed upon it by Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 ("DORA");*
2. *The Client has entrusted the Service Provider with the provision of specific services, and the Service Provider has undertaken to provide such services, under the terms and conditions specified in the agreement dated* [·] *on [·] (the "**Main Agreement**");*
3. *The Service Provider's services provided under the Main Agreement constitute ICT Services within the meaning of DORA,*
4. *Therefore, the need has arisen to adapt the Main Agreement to the requirements of DORA, including in particular the requirements described in Articles 28-30 of DORA,*

The Parties hereby enter into an Annex to the Main Agreement with the following content:

§ 1
Definitions. Collision rules

1. Unless expressly stated otherwise, all definitions used in Annex DORA shall have the following meaning:

Business Day	Every day from Monday to Friday, except statutory holidays in Poland
DORA	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, together with implementing acts
ICT-related Incident	A single event or a series of linked events unplanned by the Service Provider that compromises the security of the network and information systems and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the Service Provider
Competent authority/ KNF	The Polish Financial Supervision Authority (Komisja Nadzoru Finansowego – KNF)
Employee	An employee within the meaning of the Labour Code or a natural person cooperating with the Service Provider on the basis of a civil law contract
Subcontractor	An entity other than an Employee to whom the Service Provider has entrusted the provision of the ICT Service or a substantial part thereof. Individuals conducting sole proprietorships who perform activities for the Service Provider under a civil law agreement (B2B contract) that provides mainly for the personal provision of services by such individuals, supporting the ICT Services provided by the Service Provider to the Client, shall not be considered Subcontractors.
ICT Services	Services provided by the Service Provider to the Client under the Main Agreement which are digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services;
ICT-related Risk	Any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems, of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects in the digital or physical environment;
Resolution authorities	The Bank Guarantee Fund or other institutions whose purpose is to conduct the restructuring and orderly winding-up procedures of a financial entity.

2. Words and expressions defined in the Main Agreement shall have the same meaning in the DORA Annex, unless otherwise stated in the DORA Annex or unless the context provides otherwise.

3. Terms not defined in the DORA Annex but having their definitions in the DORA shall have the meaning given to them in the DORA.
4. In the event of a conflict between the provisions set out in the Main Agreement and the provisions contained in the DORA Annex, the provisions set out in the DORA Annex shall apply accordingly, unless the DORA Annex expressly provides otherwise.

§ 2

ICT Services [*requirement under Article 30(2)(a) of DORA]*

1. A clear and complete description of the ICT Services provided by the Service Provider to the Client is provided in the Main Agreement.
2. The ICT Services provided by the Service Provider to the Client do not constitute ICT Services supporting a critical or important function within the meaning of Article 3 point 22) of DORA.

§ 3

Subcontracting [*requirement under Article 30(2)(a) of DORA]*

1. The Service Provider has the right to provide ICT Services using Subcontractors.
2. The Service Provider represents that it has implemented and applies Subcontractor assessment processes, enabling the due evaluation of the activities of Subcontractors.
3. The Service Provider undertakes to inform the Client of:
   a) an intention to enter into cooperation with a Subcontractor whose place of supply of services is outside the European Economic Area (EEA) zone;
   b) a change in the place of service provision by an existing Subcontractor to a location outside the EEA;

   no later than within 5 (five) Business Days prior to the date of initiating cooperation with such Subcontractor or, respectively, no later than 5 (five) Business Days from the date of obtaining information about the change in the place of service provision by the existing Subcontractor.
4. The Service Provider shall be liable for the provision of services by Subcontractors.
5. The list of Subcontractors used by the Service Provider for the provision of ICT Services as of the date of the DORA Annex is set out in § 4 Sec. 1 below. The Service Provider undertakes to inform the Client of a planned entity change in the list of Subcontractors no later than 5 (five) Business Days preceding the date of establishing cooperation with such Subcontractor.

§ 4

Locations of ICT Services [requirement *under Article 30(2)(b) of DORA]*

1. The Parties shall specify the locations, i.e. the regions or countries, where the ICT Services covered by the Main Agreement or the subcontract will be provided and where the data is to be processed, including the storage location:

Name **Address** **LEI/EUID number**	**ICT Services Location (Country/Region)**	**Place of processing including data storage (country/region)**
Service Provider:		
Vercom S.A ul. Wierzbięcice 1B, 61-569 Poznań LEI: 259400P9VT804CUH6G16	EEA, Poland	EEA, Poland

EUID: PLKRS.0000535618		
Subcontractor:		
Beyond Solutions sp. z o. o. ul. Kręglewskiego 11, 61-248 Poznań EUID: PLKRS.0001099085	EEA, Poland	EEA, Poland
NTT Global Data Centers EMEA GmbH Voltastraße 15, 65795 Hattersheim, Germany EUID: DEM1201.HRB77478	EEA, Germany	EEA, Germany
cyber_Folks S.A. ul. Wierzbięcice 1B, 61-569 Poznań LEI 259400I7J8I4F638KS93 EUID: PLKRS.0000685595	EEA, Poland	EEA, Poland
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, LU-1855 Luxembourg EUID: LURCSL.B186284	EEA, Germany	EEA, Luxembourg
Cloudflare, Inc. 101 Townsend St, San Francisco, CA 94107, USA LEI: 5493007DY18BGNLDWU14	EEA	EEA

2. The Service Provider undertakes to inform the Client of a change in the location of the ICT Services or the place of processing, including data storage, outside the EEA no later than 5 (five) Business Days prior to the planned date of the change.

§ 5
Data security. ICT-related Incident management
[requirement under Articles 28(5) and 30(2)(c) and (f) of DORA]

1. The Service Provider undertakes to implement appropriate information security standards, including the application of principles based on internationally recognised standards set out in ISO/IEC 27001, ISO/IEC 27018 and ISO 22301, which ensure availability, authenticity, integrity and confidentiality in relation with the protection of data, including personal data.
2. The Service Provider is obliged to remedy vulnerabilities, in particular critical and significant ones in accordance with the risk analysis performed and procedures in place, in its systems, tools and processes and to respond to cyber threats that may adversely affect the ICT Service.
3. The Parties undertake to report ICT-related Incidents to each other.
4. In particular, the following events shall be reported as an ICT-related Incident:
   a) breach of one or more of the attributes of confidentiality, integrity, authenticity, accountability or availability of protected information, e.g. unauthorised access to such information (leakage outside the IT infrastructure or unauthorised access to documentation stored outside the IT infrastructure);
   b) impersonation of the Service Provider or the Client using IT techniques (e.g. phishing, pharming) or social engineering, insofar as this affects the provision of the ICT Services provided by the Service Provider under the Main Agreement;
   c) misuse of the Service Provider's or the Client's personnel threatening the security of the Client's or the Service Provider's legally protected information or the performance of the ICT Services provided by the Service Provider under the Main Agreement.

5. In the event of an ICT-related Incident, the Parties are obliged to immediately, but not later than within 1 (one) Business Day from confirming the occurrence of the ICT-related Incident, and in each case no later than within 72 hours from becoming aware of the occurrence of the ICT-related Incident, inform each other of such event and provide materials and information necessary for the effective handling of such ICT-related Incident, including its remediation.
6. ICT-related Incidents identified by:
   a) Service Provider – the Service Provider is obliged to immediately report to the Client, by e-mail to the following address: [email address of the administrator of the account in the service [...]];
   b) Client – the Client is obliged to immediately report to the Service Provider by e-mail to the following address: soc@vercom.pl.
7. Each Party, when reporting an ICT-related Incident, shall update the report periodically as more data is acquired until the ICT-related Incident is closed.
8. Cooperation in the management of an ICT-related Incident in excess of the necessary, specified above, shall be performed by the Service Provider for remuneration in the amount constituting the product of the rate of EUR 100.00 (in words: one hundred euros) net plus the applicable value added tax and the number of hours necessary for the Service Provider to perform the aforementioned activities.
9. The payment of the remuneration to the Service Provider, referred to in § 5 Sec. 8 above, will be made on a monthly basis, on the basis of a VAT invoice duly issued and delivered to the Client. The provisions of the Main Agreement relating to remuneration (within the scope relating to, inter alia, the payment term, the method of submitting the invoice) shall apply accordingly.

§ 6

Access to data [*requirement under Article 30(2)(d) of DORA]*

The Service Provider will make the data processed under the ICT Service available to the Client in an easily accessible format under the terms of the Main Agreement, while respecting the rules on data storage and archiving, including the possibility of making backups, as well as the rules under 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 and repealing Directive 95/46/EC (GDPR).

§ 7

SLA [*requirement under Article 30 (2)(e) of DORA*]

1. Unless the Parties have agreed on other guaranteed service levels in the Main Agreement, the Service Provider undertakes to ensure the availability of ICT Services on the terms described in this paragraph.
2. The Service Provider shall endeavour to ensure that the availability of the system, i.e. - the time during the billing period in which all ICT Services are fully functional and allow for the execution of ordered messages, including the possibility of logging into the Client panel, sending messages, receiving and transmitting reports, the availability of the API and all other elements necessary for the execution of messages, is 99% during the billing period.
3. The Service Provider shall endeavour to ensure that maintenance work or updates to the system are carried out in accordance with the aforementioned system availability.
4. The provisions of Sec. 3 above shall not apply if, for technical reasons, beyond the Service Provider's control or for security reasons, it is necessary to carry out maintenance or update works at a frequency exceeding the declared SLA.

§ 8

Cooperation with authorities [*requirement under Article 30(2)(g) of the DORA]*

1. The Service Provider will cooperate with KNF or other Resolution authorities or a person designated by the Competent authority or Resolution authorities on matters where required to do so, including in connection with the performance of an obligation or right under law or an investigation by the Competent authority or Resolution authorities. The form of cooperation may consist in making available or providing access to documentation, information, data, systems, premises and telecommunications networks that are in the possession, custody or control of the Service Provider.
2. The Client is obliged – in the following order – to:
   1) immediately submit to the Service Provider the relevant administrative decision, ruling or other summons issued by the Competent authority or Resolution authorities ordering the Service Provider to take a specific action by or against the Service Provider;
   2) take all measures to satisfy the request of the Competent authority or Resolution authorities independently (i.e. without the participation of the Service Provider) and to inform the Service Provider of the measures taken, together with an indication of the scope, subject matter and timing of the measures so taken.
3. In the event of ineffectiveness of the measures taken by the Client on the terms set out in Sec. 2 point 2 above, the Service Provider undertakes to cooperate with the Competent authority or Resolution authorities (including their designees) to the extent required by law and the content of the request, with the Client, whenever requested by the Service Provider, being obliged in good faith to provide full support, free of charge, to the Service Provider without delay, including giving any instructions in connection with such supervisory request. For the avoidance of doubt, the support provided, including instructions, shall in no way contradict the law, the content of the request or raise doubts in the Service Provider's mind as to the satisfaction of the supervisory, restructuring or liquidation purpose presented.
4. In the event that a request made to the Service Provider by the Competent authority or the Resolution authorities (including individuals appointed by them) results from the Client's failure to comply with a prior request from the Competent authority or the Resolution authorities, the Service Provider shall be entitled to recover from the Client any costs and expenses incurred in connection with such cooperation with the Competent authority or the Resolution authorities (including individuals appointed by them) or the financial entity, including any incurred and documented administrative and operational costs.

§ 9

Termination of the Main Agreement [*requirement under Article 28(7) and Article 30(2)(h) of the DORA]*

The Client may terminate the Main Agreement, notwithstanding any contrary provisions of the Main Agreement, if:

1) the Competent authority or the Resolution authorities issue an appropriate recommendation or decision – with effect on the last day of the term resulting from such decision or recommendation, or, in the absence of a specified term for termination in such decision or recommendation, with a 30-day notice period, effective at the end of the month. Prior to terminating the Main Agreement for this reason, the Client shall be obliged to immediately notify the Service Provider thereof (no later than 5 days from the date of delivery of such decision or recommendation);

2) the Service Provider commits a material breach of statutory or executive regulations, or provisions of the Main Agreement directly related to the provision of ICT Services – with immediate effect. Before terminating the Main Agreement for this reason, the Client must give the Service Provider a notice to cease the breach or present a statement, within a period no shorter than 5 Business Days. Termination of the Main Agreement due to the circumstances set forth in this point is possible after the expiration of this period without effect;

3) during risk monitoring by the Client, the following are identified:
   a) circumstances that are deemed to significantly affect the execution of the ICT Services provided under the Main Agreement,
   b) significant changes impacting the Main Agreement or the Service Provider's situation

   – with immediate effect. Prior to terminating the Main Agreement for this reason, the Client will inform the Service Provider of the scope of the circumstances and significant changes referred to in points a-b above, and set a minimum 30-day period for implementing appropriate corrective actions. Termination of the Main Agreement due to the circumstances described in this point is possible after the expiration of this period without effect;
4) weaknesses in the Service Provider's overall ICT-related Risk management are identified, particularly concerning the manner in which the Service Provider ensures the availability, authenticity, integrity, and confidentiality of data, whether personal or otherwise sensitive, or non-personal data – with immediate effect. Prior to terminating the Main Agreement for this reason, the Client will inform the Service Provider of the scope of the weaknesses and set a minimum 30-day period for implementing appropriate corrective actions. Termination of the Main Agreement due to the circumstances described in this point is possible after the expiration of this period without effect;
5) due to the conditions or circumstances related to the Main Agreement, the Competent authority can no longer effectively supervise the Client – with immediate effect.

§ 10

Training programmes [requirement *under Article 30(2)(i) of DORA]*

1. At the Client's request, the Service Provider's employees or, with the Service Provider's consent, other representatives of the Service Provider may be subject to the Client's obligation to participate in ICT security awareness programs and training related to digital operational resilience. The Client ensures that the nature, scope, and level of complexity of such training and programs will be proportionate to the functions held by the individuals subject to such obligations on the Service Provider's side. Subject to the provisions of Sec. 2 below, the timing and terms of participation in such programs and training will be jointly agreed upon by the Parties.
2. The costs related to the organization and participation of persons on the part of the Service Provider in the programs or trainings referred to in Sec. 1 above shall be borne by the Client.

§ 11

Final provisions

1. All notices under the DORA Annex shall be made in documentary form (via e-mail correspondence), unless explicitly stated otherwise in the DORA Annex.
2. This DORA Annex shall be governed by and construed in accordance with the laws of Poland. Parties agrees that the courts of Poland shall have exclusive jurisdiction to settle any dispute or

claim arising out of or in connection with his DORA Annex and the venue for such disputes and claims will be in the place of registered office of the Service Provider.

3. The DORA Annex has been executed in electronic form within the meaning of Article 78^1 of the Polish Civil Code.
4. The DORA Annex is valid only for the duration of the provision of ICT Services and is not subject to separate termination other than the Main Agreement.

Service Provider	**Client**
Service Provider	