Viber Developer Distribution Agreement

or Viber API Terms of Service

Last updated: September 2021

Thank you for using the Viber application programming interfaces (the “Viber APIs”). As used herein, the terms “you” and “your” refer to each administrator, developer and user of the Viber APIs. You may also be referred to as Developer. By using the Viber APIs, you agree to these Terms of Service (the “Terms of Service”) and the Viber Terms of Use (the “TOU”). If you use the Viber APIs as an interface to, or in conjunction with other Viber products or services, then the terms of those products or services will also apply. If you disagree with any of the terms below or the TOU, Viber does not grant you a license to use the Viber APIs. In the event of any inconsistency between these Terms of Service and the TOU, these Terms of Service control. Viber Media S.à r.l., its subsidiaries and affiliated companies (collectively, “Viber,” “we,” “our,” or “us”) reserve the right to update and change, from time to time, these Terms of Service and all documents incorporated by reference, and Viber may change these Terms of Service by posting a new version without notice to you. Use of the Viber APIs after such change constitutes acceptance of such change.

1. **License** Subject to the restrictions set forth in these Terms of Service, Viber grants you a non-exclusive, worldwide, personal, non-transferable, non-assignable, non-sublicensable, royalty-free license to use the Viber APIs. All rights not expressly granted to you are reserved by Viber.

2. **Use of the Viber APIs.**

- You will comply with all applicable law, regulation, and third party rights (including without limitation laws regarding the import or export of data or software, privacy, and local laws). You will not use the Viber APIs to encourage or promote illegal activity or violation of third party rights. You will not violate any other terms of use or agreements with Viber.

- You will only access (or attempt to access) the Viber APIs by the means described in the documentation of that API. If Viber assigns you developer credentials (e.g. client IDs), you must use them with the applicable Viber APIs. You will not misrepresent or mask either your identity or your API Client's identity when using the Viber APIs or developer accounts.
- Viber may set and enforce limits on your use of the Viber APIs (e.g. limiting the number of API requests that you may make or the number of users you may serve) in our sole discretion. You agree to and will not attempt to circumvent such limitations. If you would like to use any Viber API beyond the applicable limits, you must obtain our express consent (and we may decline such request or condition acceptance on your agreement to additional terms and/or charges for that use).

3. **API Clients and Monitoring.** The Viber APIs are designed to help you enhance your websites and applications ("API Client(s)"). Viber is not required to promote or recommend your API Client. YOU AGREE THAT VIBER MAY MONITOR USE OF THE APIS TO ENSURE QUALITY, IMPROVE VIBER PRODUCTS AND SERVICES, AND VERIFY YOUR COMPLIANCE WITH THE TERMS OF SERVICE. This monitoring may include Viber accessing and using your API Client, for example, to identify security issues that could affect Viber or its users. You will not interfere with this monitoring. Viber may use any technical means to overcome such interference. Viber may suspend access to the Viber APIs by you or your API Client without notice if we reasonably believe that you are in violation f the Terms of Service or the TOU.
4. **Security.** You will use best commercial efforts to protect user information collected by your API Client, including personally identifiable information ("PII"), from unauthorized access or use and will promptly report to your users and any other party as required by applicable law any unauthorized access or use of such information to the extent required by applicable law.
5. **User Privacy and API Clients.** You will comply with all applicable privacy laws and regulations including those applying to PII. You will provide and adhere to a privacy policy for your API Client that clearly and accurately describes to users of your API Client what user information you collect and how you use and share such information (including for advertising) with Viber and third parties. You agree that you are the controller of any EU Personal Data (as defined in Exhibit A hereto) of end users collected by you, and Viber is a controller of any EU Personal Data of end users collected by it, and, you agree that you will be regarded as business with respect to any U.S. Personal Information (as defined in Exhibit A hereto) of end users collected by you, and Viber will be regarded as business with respect to any U.S. Personal Information of end users collected by it., and you further agree to the terms of the Data Processing Addendum attached as Exhibit A hereto in connection with any EU Personal Data and/or U.S. Personal Information transferred between the Parties in connection with your use of the Viber API. You

represent that you will not request the Viber API Personal Data (as defined in Exhibit A hereto) of users which you do not have a legal basis to process.

6. **Viber API Prohibitions.** When using the Viber APIs, you may not (or allow those acting on your behalf to):

- Perform an action with the intent of introducing to Viber products and services any viruses, worms, defects, Trojan horses, malware, or any items of a destructive nature.
- Defame, abuse, harass, stalk, or threaten others.
- Interfere with or disrupt the Viber APIs or the servers or networks providing the Viber APIs.
- Promote or facilitate unlawful online gambling or disruptive commercial messages or advertisements.
- Reverse engineer or attempt to extract the source code from any Viber API or any related software, except to the extent that this restriction is expressly prohibited by applicable law.
- Use the Viber APIs for any activities where the use or failure of the Viber APIs could lead to death, personal injury, or environmental damage (such as the operation of nuclear facilities, air traffic control, or life support systems).
- Use the Viber APIs to process or store any data that is subject to the International Traffic in Arms Regulations maintained by the U.S. Department of State.
- Remove, obscure, or alter any Viber Terms of Service or any links to or notices of those terms.

Viber reserves the right to charge fees for future use of or access to the Viber APIs in Viber’s sole discretion. If Viber decides to charge for use of the Viber APIs, such charges will be disclosed to you prior to their effect. Viber also reserves the right to include advertising in or associated with any information provided to you through the Viber APIs.

7. **Confidential Information.**

- Developer credentials (such as passwords, keys, and client IDs) are intended to be used by you and to identify your API Client. You will keep your credentials confidential and make reasonable efforts to prevent and discourage other API Clients from using your credentials. Developer credentials may not be embedded in open source projects.
- Our communications to you and the Viber APIs may contain Viber confidential information. Viber confidential information includes any materials, communications, and information that are marked confidential or that would normally be considered confidential under the circumstances. If you receive any such information, then you will not disclose it to any third party without Viber’s prior written consent. Viber confidential information does not include information that you independently developed, that was rightfully given to you by a third party without confidentiality obligation, or that becomes public through no fault of your own. You may disclose Viber confidential information

when compelled to do so by law if you provide us reasonable prior notice. If you have entered a specific Non Disclosure Agreement with Viber, such Non Disclosure Agreement shall prevail over the confidentiality obligations set forth in this Section 7(b).

8. **Ownership.** The Viber APIs may be protected by copyrights, trademarks, service marks, international treaties, and/or other proprietary rights and laws of the U.S. and other countries. Viber's rights apply to the Viber APIs and all output and executables of the Viber APIs, excluding any software components developed by you which do not themselves incorporate the Viber APIs or any output or executables of such software components. You agree to abide by all applicable proprietary rights laws and other laws including without limitation the laws of the United States of America and all other countries where you use the Viber APIs, as well as any additional copyright notices or restrictions contained in these Terms of Service. Viber owns all rights, title, and interest in and to the Viber APIs. These Terms of Service grant you no right, title, or interest in any intellectual property owned or licensed by Viber, including (but not limited to) the Viber APIs.
9. **Termination.** You may stop using the Viber APIs at any time with or without notice. Further, if you want to terminate the Terms of Service, you must provide Viber with prior written notice and upon termination, cease your use of the Viber APIs. Viber reserves the right to terminate the Terms of Service with you without notice, liability, or other obligation to you.
10. **Support.** Viber may elect to provide you with support or modifications for the Viber APIs (collectively, "Support"), in its sole discretion, and may terminate such Support at any time without notice to you. Viber may change, suspend, or discontinue any aspect of the Viber APIs for any reason at any time, including the availability of any Viber APIs. Viber may also impose limits on certain features and services or restrict your access to parts or all of the Viber APIs without notice or liability.
11. **Your Obligations Post-Termination.** Upon any termination of the Terms of Service or discontinuation of your access to the Viber APIs, you will immediately stop using the Viber APIs, and upon Viber's written request, delete and/or return to us, any Viber confidential information. Viber may independently communicate with any account owner whose account(s) are associated with your API Client and developer credentials to provide notice of the termination of your right to use the Viber APIs.
12. **Survival clause.** When the Terms of Service terminate, those terms that by their nature are intended to continue indefinitely will continue to apply.
13. **Disclaimer of Warranty.** SOME OF THE VIBER APIS ARE EXPERIMENTAL AND HAVE NOT BEEN TESTED IN ANY MANNER. VIBER DOES NOT REPRESENT OR WARRANT THAT VIBER APIS ARE FREE OF INACCURACIES, ERRORS, BUGS, OR INTERRUPTIONS, OR ARE RELIABLE, ACCURATE, COMPLETE, OR OTHERWISE VALID. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THE VIBER APIS ARE PROVIDED "AS IS" WITH NO WARRANTY, EXPRESS OR IMPLIED, OF ANY KIND AND VIBER EXPRESSLY DISCLAIMS ANY AND ALL WARRANTIES AND CONDITIONS, INCLUDING, BUT NOT LIMITED TO,

ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AVAILABILITY, SECURITY, TITLE AND/OR NON-INFRINGEMENT. YOUR USE OF THE VIBER APIS IS AT YOUR OWN DISCRETION AND RISK, AND YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE THAT RESULTS FROM THE USE OF THE VIBER APIS INCLUDING, BUT NOT LIMITED TO, ANY DAMAGE TO YOUR COMPUTER SYSTEM OR LOSS OF DATA.

14. **Limitation of Liability**. TO THE EXTENT PERMITTED BY APPLICABLE LAW, VIBER SHALL NOT, UNDER ANY CIRCUMSTANCES, BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, PUNITIVE, ACTUAL, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH ANY USE, OR INABILITY TO USE, THE VIBER APIS, WHETHER BASED ON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, OR ANY OTHER PECUNIARY LOSS, REGARDLESS OF THE BASIS UPON WHICH LIABILITY IS CLAIMED AND WHETHER OR NOT VIBER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES. UNDER NO CIRCUMSTANCES SHALL VIBER BE LIABLE TO YOU FOR ANY AMOUNT. WITHOUT LIMITATION, YOU (AND NOT VIBER) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVING, REPAIR, OR CORRECTION IN THE EVENT OF ANY SUCH LOSS OR DAMAGE ARISING THEREIN. IF APPLICABLE LAW DOES NOT ALLOW ALL OR ANY PART OF THE ABOVE LIMITATION OF LIABILITY TO APPLY TO YOU, THE LIMITATIONS WILL APPLY TO YOU ONLY TO THE EXTENT PERMITTED BY APPLICABLE LAW. In no event shall Viber’s total liability to you for all damages (other than as may be required by applicable law in cases involving personal injury) exceed the amount of fifty U.S. dollars ($50.00). The foregoing limitations will apply even if the above stated remedy fails of its essential purpose.
15. **Indemnification.** To the maximum extent permitted by applicable law, you agree to hold harmless and indemnify Viber and its subsidiaries, affiliates, officers, agents, licensors, co-branders or other partners, and employees from and against any third party claims arising from or in any way related to your use of the Viber APIs, including any liability or expense arising from all claims, losses, damages (actual and/or consequential), suits, judgments, litigation costs and attorneys’ fees, of every kind and nature. Viber shall use good faith efforts to provide you with written notice of such claim, suit or action.
16. **Relationship of the Parties**. Notwithstanding any provision hereof, for all purposes of the Terms of Service, you and Viber shall be and act independently and not as partner, joint venturer, agent, employee or employer of the other. You shall not have any authority to assume or create any obligation for or on behalf of Viber, express or implied, and you shall not attempt to bind Viber to any contract.
17. **Invalidity of Specific Terms**. If any provision of these Terms of Service is adjudged, by written decision, to be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions.

18. **Choice of Law**. To the extent permitted by law, the Terms of Service and any provisions therein shall be governed by, construed and enforced in accordance with the laws of the State of New York, as they are applied to agreements entered into and to be performed entirely within New York.
19. **No Waiver of Rights by Viber**. Viber's failure to exercise or enforce any right or provision of the Terms of Service shall not constitute a waiver of such right or provision.
20. **Miscellaneous**. The section headings and subheadings contained in this agreement are included for convenience only, and shall not limit or otherwise affect the terms of the Terms of Service. Any construction or interpretation to be made of the Terms of Service shall not be construed against the drafter. The Terms of Service, the Viber Terms of Use and any other applicable Viber product or service terms, constitute the entire agreement between Viber and you with respect to the subject matter hereof.

Exhibit A

General Data Protection Addendum to the Viber API Terms of Service

This Addendum to the Viber API Terms of Service (the "Agreement") is by and between Viber Media S.a.r.l, a Luxembourg limited liability company ("Viber"), and Developer having selected to use the Viber API under the Agreement. Viber and Developer are each a "Party" and collectively the "Parties." This Addendum is an integral part of the Agreement. Any words or terms not otherwise defined in this Addendum have the same meaning as in the Agreement. In the event of a conflict between definitions in the Agreement and this Addendum, the definitions within this Addendum control.

1. **Definitions**.

(a) "**Personal Data,**" "**Process/Processing,** " **Controller**", " **Processor,**" "**Data Subject**" and " **Supervisory Authority** shall have the same meanings given to them in the Regulation
(or where the same or similar terms are used under another applicable Data Protection Law, the meanings given to such terms under such Data Protection Law).

(b) "**EU Personal Data**" means personal data of natural persons subject to the Regulation.

(c) "**U.S. Personal Information**" means any information that relates to, is capable of being associated with, or could be linked, directly or indirectly, with a particular United States resident or household.

(d) "**Data Protection Law(s)**" means privacy or data protection laws that apply to data transferred by each of the Parties to the other, including, but not limited to, the Regulation, any successor thereto, and the California Consumer Privacy Act.

(e) “**Directive**” means the Directive 95/46/EC of the European Parliament and of the Council (Personal Data Directive).

(f) “**Regulation**” means Regulation (EU) 2016/679 of the European Parliament and the Council (General Data Protection Regulation).

2. **Role of the Parties**. In order to provide the Services under the Agreement, Viber discloses data, including EU Personal Data and/or U.S. Personal Information to Developer solely for the purposes described in the Agreement (the “Permitted Purposes”) and Viber is a Controller of the EU Personal Data, and business with respect to any U.S. Personal Information, it discloses to Developer. Pursuant to the Agreement, Developer uses the data as a separate and independent Controller or Business for the Permitted Purposes. In no event will the Parties process the data as joint Controllers.

3. **Obligations**.

   a. Each Party shall use the Personal Data in accordance with the Regulation and other applicable Data Protection Laws, will not cause the other Party to breach its obligations under Data Protection Laws and will individually and separately fulfill all obligations that apply to it as a Controller under the Regulation or Business under the California Consumer Privacy Act.

   The Developer shall use the Personal Data it receives from the Viber only for the Permitted Purposes in line with the Agreement and this Addendum, unless otherwise required by applicable laws.

   b. In order to disclose Personal Data to for the Permitted Purposes and in compliance with the Regulation and other applicable Data Protection Laws, each Party’s obligations include without limitation: (i) identifying and establishing its independent legal basis for processing and disclosing Personal Data; and (ii) fulfilling transparency requirements regarding its use of and disclosure of Personal Data.

   c. The Developer will assure it obtains the necessary right(s) from Data Subjects to request Personal Data from Viber pursuant to the Agreement for the Permitted Purposes.

4. **International Data Transfers.**

   a. The Parties acknowledge that in the course of their cooperation under the Agreement, E.U. Personal Data may be transferred internationally. In all cases where Personal Data is transferred internationally to a country not providing adequate Personal Data protection in accordance with applicable Data Protection Laws, the Parties will ensure that appropriate safeguards that ensure a level of data protection of Personal Data essentially similar to that provided under applicable Data Protection Laws and this Addendum are put in place.

b. The obligations herein shall apply inter alia to any onward transfer to another third country; or to another entity within the same country it has been exported to.

c. Further restrictions on data exports from the European Economic Area (“**EEA**”):

i. For any Personal Data originating in the EEA, Developer agrees to comply with the C-to-C Transfer Clauses set forth by the European Commission in the form attached as Schedule 1 hereto.
ii. In the event that the C-to-C Transfer Clauses are amended, replaced or repealed by the European Commission or under applicable Data Protection Laws, the Parties shall enter into an updated version of the C-to-C Transfer Clauses.

5. This Addendum shall survive termination or expiration of the Agreement. Upon termination or expiration of the Agreement, the Developer may only continue to process Personal Data received from Viber provided if such use complies the requirements of this Addendum and under the Regulation.

Schedule 1 to the Addendum

C-to-C Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 in accordance with Commission Implementing Decision (EU) 2021/914 of 4 June 2021

MODULE ONE: Transfer controller to controller

These C-to-C Standard Contractual Clauses for the transfer of personal from the European Economic Area community to third countries data transfer agreement between Viber Media S.a.r.l (“Viber”) and the Developer which is making use of the Viber API according to the Viber API Terms of Service. For the purposes of these C-to-C Standard Contractual Clauses, Viber is the data exporter and Developer is the data importer. Developer and Viber are each a “Party” and collectively the “Parties”.

SECTION I

Clause 1 – Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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 (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties have agreed to these standard contractual clauses (hereinafter: '**Clauses'**).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 – Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 – Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Clause 8.5 (e) and Clause 8.9(b);

(iii) Clause 12 – Clause 12(a) and (d);

(iv) Clause 13;

(v) Clause 15.1(c), (d) and (e);

(vi) Clause 16(e);

(vii) Clause 18 – Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 – Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 – Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 – Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 – Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter '**personal data breach**'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter '**sensitive data**'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter '**onward transfer**') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9 – Use of sub-processors

[Not applicable]

Clause 10 – Data subject rights

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter '**automated decision**'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

Clause 11 – Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 – Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13 – Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 – Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 – Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 – Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 – Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Luxembourg.

Clause 18 – Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Luxembourg.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

Annex I

A. LIST OF THE PARTIES:

The Parties mentioned in the Preamble of the Clauses.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

End users of Viber who elect to communicate with data importer’s product.

Categories of personal data transferred:

The personal data transferred concern the following categories of data: Profile photo of user (if exists), unique identifier of user for the unique data importer’s product, profile name of user.

Sensitive data transferred (if applicable):

The personal data transferred concern the following categories of sensitive data:

N/A

The frequency of the transfer:

On continuous basis.

Nature of the processing:

Data importer receives the personal data via the Viber API and processes it for the below purpose.

Purpose(s) of the data transfer and further processing

The personal data will be transferred to the data importer to enable personalization of data importer’s product.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The period for which the personal data will be retained will be determined by the Data importer accordance with its data privacy and data retention policies.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

N/A

C. COMPETENT SUPERVISORY AUTHORITY

The National Commission for Data Protection of the Grand-Duchy of Luxembourg (“CNPD”).

Annex II

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

In addition to any data security requirements set forth in the Agreement, the data importer shall comply with the following:
Data importer undertakes to implement, maintain, and continuously control and update, appropriate technical and organizational security measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected. This includes:

1. *Preventing unauthorised persons from gaining access to data processing systems with which personal data are processed or used (physical access control); in particular, by taking the following measures:*
    - Controlled access for critical or sensitive areas
    - Video monitoring in critical areas
    - Incident logs
    - Implementation of single entry access control systems,
    - Automated systems of access control,
    - Permanent door and windows locking mechanisms,
    - Key management
    - Permanently manned reception
    - Code locks on doors
    - Monitoring facilities (e.g. alarm device, video surveillance)
    - Logging of visitors
    - Compulsory wearing of ID cards
    - Security awareness training
2. *Preventing data processing systems from being used without authorisation (logical access control); in particular, by taking the following measures:*
    - Network devices such as intrusion detection systems, routers and firewalls
    - Secure log-in with unique user-ID, password and a second factor for authentication (OTP, MFA, 2FA).
    - Policy mandates locking of unattended workstations. Screensaver password is implemented such that if user forgets to lock the workstation, automatic locking is ensured.
    - Logging and analysis of system usage
    - Role-based access for critical systems containing personal data
    - Process for routine system updates for known vulnerabilities
    - Encryption of laptop hard drives
    - Monitoring for security vulnerabilities on critical systems
    - Deployment and updating of antivirus software

- individual allocation of user rights, authentication by password and username, use of smartcards for log in, minimum requirements for passwords, password management, password request after inactivity, password protection for BIOS, blocking of external ports (such as USB ports), encryption of data, virus protection and use of firewalls, intrusion detection systems.

3. *Ensuring that persons entitled to use a data processing system can gain access only to the data to which they have a right of access, and that, in the course of processing or use and after storage, personal data cannot be read, copied, modified or deleted without authorisation (access control to data); in particular, by taking the following measures:*
    - Network devices such as intrusion detection systems, routers and firewalls
    - Secure log-in with unique user-ID, password and a second factor for authentication (OTP, MFA, 2FA).
    - Logging and analysis of system usage
    - Role based access for critical systems containing personal data
    - Encryption of laptop hard drives
    - Deployment and updating of antivirus software
    - Compliance with Payment Card Industry Data Security Standard
    - Definition and management of role based authorization concept, access to personal data only on a need-to-know basis, general access rights only for a limited number of admins, access logging and controls, encryption of data, intrusion detection systems, secured storage of data carriers, secure data lines, distribution boxes and sockets.
4. *Ensuring that personal data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage and that it is possible to verify and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (data transfer control); in particular, by taking the following measures:*
    - Encryption of communication, tunneling (VPN = Virtual Private Network), firewall, secure transport containers in case of physical transport, encryption of laptops
5. *Ensuring that it is possible retrospectively to examine and establish whether and by whom personal data have been inserted into data processing systems, modified or removed (entry control); in particular, by taking the following measures:*
    - Logging and analysis of system usage
    - Role based access for critical systems containing personal data
    - Logging and reporting systems, individual allocation of user rights to enter, modify or remove based on role based authorization concept.

6. *Ensuring that personal data processed on the basis of a commissioned processing of personal data are processed solely in accordance with the directions of the data exporter (job control); in particular, by taking the following measures:*
    - Mandatory security and privacy awareness training for all employees
    - Employee hiring procedures which require the completion of a detailed application form for key employees with access to significant personal data and, where allowed by local law
    - Periodic audits are conducted
    - Implementation of processes that ensure that personal data is only processed as instructed by the data exporter, covering any sub-processors, including diligently selecting appropriate personnel and service providers and monitoring of contract peformance, entering into appropriate data processing agreements with sub-processors, which include appropriate technical and organizational security measures.
7. *Ensuring that personal data are protected against accidental destruction or loss (availability control); in particular, by taking the following measures:*
    - Backup procedures and recovery systems, redundant servers in separate location, mirroring of hard disks, uninterruptible power supply and auxiliary power unit, remote storage, climate monitoring and control for servers, fire resistant doors, fire and smoke detection, fire extinguising system, anti-virus/firewall systems, malware protection, disaster recovery and emergency plan.
8. *Ensuring that data collected for different purposes or different principals can be processed separately (separation control); in particular, by taking the following measures:*
    - Internal client concept and technical logical client data segregation, development of a role based authorization concept, separation of test data and live data.

- Viber Out
- Business
- Support

COMPANY

- About Viber
- Brand Center
- Careers
- Terms & Policies
- Terms of Use
- Privacy Policy
- Ads Policy
- CCPA Do Not Sell My Data

DOWNLOAD

- Android
- IPhone & IPad
- Windows PC
- Mac
- Linux

English

Rakuten Viki Rakuten Kobo Rakuten Global Market Rakuten Travel Rakuten Marketing Rakuten Insight Rakuten TV