Viber Developer Terms of Service

[Last updated: 22 March 2022]

This Developer Terms of Service (or as previously titled "the Viber API Terms of Service") (“**Developer Terms of Service**”) governs the (a) install, download and use of the various Viber application programming interfaces (Each: “**Viber API**” and collectively: the “**Viber APIs**”) and (b) access to the Viber Admin Panel (the “**VAP**” together with the Viber APIs and the Chatbot shall be defined herein as "**Developer Platform**").

For the purpose of these Terms, the terms “**Developer**”, “**you**” or “**your**” shall refer to each administrator (including super admins) of a Chatbot, developers, and business partners implementing or using the Viber APIs on their platform or third-parties' platforms, Merchants using the Chatbots, or the company or business that you are authorized to represent. Capitalized terms not defined however used shall have the meaning ascribed to them in the **Viber Terms of Service**.

BY USING THE DEVELOPER PLATFORM OR ANY PART THEREIN, YOU AGREE TO BE BOUND BY THESE TERMS AND ADDITIONAL POLICIES AND DOCUMENTATIONS AS STATED BELOW.

Viber reserves the right to update, from time to time, these Developer Terms of Service and all documents incorporated herein by reference, by posting a new version which will be reflected on the “Last Updated” heading above. Use of the Developer Platform after such change constitutes your acceptance of such changes. Material changes will be notified to you through the VAP by email correspondence or via the Viber App, so please make sure you keep your contact information up to date.

1. Additional Terms and Policies

These Viber Developer Terms of Service incorporate by reference the following policies and documentation (collectively “**Terms**” or “**Business Terms**”):

- **Acceptable Use Policy** ("**AUP**")
- Ordering Documentation signed by the parties, such as Insertion Orders, addendums or agreements, etc. (“**Ordering Documentation**”) which link and refer to these Developer Terms of Service;
- The **Viber App Terms of Service** governing the use of the Viber App; and
- The Viber API **Documentation**.

2. Services and License Grant

The Viber for Business services include various features enabling Developers to create a business Chatbot, to send outbound messages, integrate the Viber API within your business website or otherwise integrate and engage with your Chatbot users, including subscribers, create, post, store, send, and receive content, etc. ("**Services**" or "**Business Services**"). Subject to your compliance with the provisions of the Business Terms, Viber grants you a non-exclusive, non-transferable, non-sublicensable, license to use the Developer Platform for your commercial and authorized purposes and not for personal use. All rights not expressly granted to you herein are reserved to Viber.

Viber reserves its right to change, suspend, limit or discontinue any aspect of the Developer Platform for any reason and at any time, including the availability of any Developer Platform or any features or services therein, without notice or liability. Viber may set and enforce limits on your use of the Developer Platform, including limiting the Developer's ability to send messages to its Chatbot subscribers, including inactive subscribers (i.e., not initiated a one-on-one message with the Administrator for a certain period of time, subject to Viber's sole discretion), limiting the number of API requests that you may make or the number of users you may serve, or charge you with fees depending on your volume of use (i.e., the number of outbound messages sent) as detailed here, in our sole discretion. You agree that you 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 or charges for that use. Viber reserves the right to limit the use of the Chatbot, including the number of messages sent through the Chatbot, the number of outbound messages, the use of the Viber API, inactivate a chat, or otherwise, at any time.

3. Developer Representations and Warranties

The Developer represents and warrants that: (i) you are above the age of 13. If you are under the age of 18 you may only use the Business Services upon receiving a parental's or other legal guardian's consent; (ii) you will only use and access the Developer Platform in accordance with the Business Terms and any other documentations as may be provided to you by Viber from time to time; (iii) you will comply with all applicable laws and regulations; (iv) you will not embed the Viber API in open source projects; (v) you have not been previously suspended or removed from using the Developer Platform, or engaged in any activity that could result in suspension or removal; (vi) you will not interfere with or disrupt the Developer Platform or the servers or networks providing the Developer Platform; (vii) you will not 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; and (viii) you will notify us immediately if you discover or suspect any security breaches related to our Business

Services or if you discover or suspect any unauthorized access or use of the Developer Platform or the Business Services.

4. Chatbot Specifications

In order to create a Chatbot, you may reach out to one of our verified official partners here, or directly to our team and we will review the application and advise you on the next steps. For the purpose of creating a Chatbot, you will need to provide certain information, such as your name, telephone number and purpose of use. We will use such Information to enable you to create the Chatbot or to contact you, all as detailed in the **Viber Privacy Policy**. You represent and warrant that the associated with you or your business shall be true, accurate and up to date. In the event you provide such information on behalf of a company you hereby represent and warrant that you are an authorized representative of the company which is qualified to represent and make commitments on the company's behalf, and that the business's name must not: (i) be false, misleading, deceptive, or defamatory; (ii) parody a third party or include character symbols, excessive punctuation, or trademark designations; or (iii) infringe any trademark, violate any right of publicity, or otherwise violate anyone's rights. We reserve the right to reclaim names on behalf of any business or individual that holds a legal claim in those names.

The Developer is responsible for all activities occurring under its account. The Developer represents and warrants it will maintain the security of its Chatbot credentials and prevent unauthorized use of or access to its account by keeping its devices and the account information safe and secure;

Viber may allow you to operate your Chatbot by engaging with third-party service providers, which will gain access or control over your account and Viber APIs. The Developer is solely responsible for ensuring that such third parties acknowledge their obligation under the Business Terms and agree to be bound by them. You will remain fully liable to Viber and to your Chatbot users for any third party acts taken under your Chatbot and your account, including without limitation, for any breach of your Chatbot users' privacy and security of information, any breach of the Business Terms or any breach of applicable laws and regulations, even once you have closed such Bot. Therefore, you should only use third parties that you trust and which are obligated to comply with the Terms.

Subject to: (i) payment of a maintenance fee (or as otherwise agreed in writing, depending on the commercial terms agreed by you and Viber), (i) providing Viber with satisfactory assurances, authorizations and certifications, and according to Viber's sole discretion, Viber may enable you to promote, optimize and make your Chatbot searchable. You acknowledge and agree that Viber reserves the right to reject your Chatbot or not to publish it, or cease its publication, at any time, at its sole discretion.

Approval of a Chatbot or promotion of such by Viber shall not imply Viber's indication of its compliance with any of the provisions herein, and shall not infer liability on Viber.

5. Merchant Specifications

As a Merchant using the Developer Platform, you may also be able to offer your goods or services for sale through your owned and operated Chatbot ("**Merchant's Products**"). The Merchant shall ensure that the Merchant's Products comply with the **Acceptable Use Policy** , applicable laws and these Terms. Viber does not exercise control over Merchant's Products, purchases, returns, delivery of goods or services. Viber is not responsible for providing any goods or services and assumes no liability for a Merchant's failure to provide the Merchant's Products or any dissatisfaction with the Merchant's Products.

Payments through the Merchant's Chatbots shall be made through Google Pay or Apple Pay or, if applicable and approved by Viber, through Merchant's payment page, which Merchant shall be solely responsible and liable for. The Merchant acknowledges that all payment transactions are not operated or processed by Viber and Viber is not liable for payments, refunds, chargebacks, the provisioning (or addition) of cards, or other commercial activity relating to payments made using the Merchant's Chatbot.

In the event the payment is processed through Google Pay, the Merchant acknowledges and agrees to be bound by the Google Pay API Terms of Service (available **here**), the Google Pay Policies for Business (available **here**); and any other terms that Google may apply to the Merchant's Service from time-to-time. Merchants shall not make the Google Pay APIs available for use for a transaction or to otherwise transfer money between any Merchant and Chatbot user that does not directly result from that Chatbot user's purchase of a Merchant Product. If any Merchant identifies its primary product type as "non-profit," and such Merchant is in compliance with all applicable requirements (legal or otherwise), then such Merchant may use the Google Payment APIs in connection with donations from Chatbot users. With respect to the sale of digital products and services by a Merchant, the Business Terms and the Google API Terms of Service apply for any transactions completed exclusively through a web browser. A Merchant using Google Pay shall not sell digital products or services through mobile applications.

In the event the payment is processed through Apple Pay, the Merchant acknowledges and agrees to be bound by the Apple Agreements and Guidelines for Apple Developers (available **here**), the Apple Pay Platform Web Merchant Terms and Conditions (available **here** and **here**); and any other terms that Apple may apply to the Merchant's Service from time-to-time.

6. Ownership

The Developer Platform may be protected by copyrights, trademarks, service marks, international treaties, or other proprietary rights and laws. Viber's rights apply to the Developer Platform and all outputs and executables of the Developer Platform, excluding any software components developed by you which do not themselves incorporate any of the Developer Platforms or any output or executables of such software components. You agree to abide by all applicable proprietary rights laws and other laws, including and without limitation, the laws imposed by the country from which you use the Developer Platforms. Except as set forth herein, Viber owns all rights, title, and interest in and to the Developer Platforms.

7. Confidentiality

Our communications with you may contain Viber confidential information. Viber confidential information includes any materials, communications, and information that would usually be considered confidential under the circumstances. If you receive any such information, 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, provided you provide us reasonable prior notice and cooperate with us in order to minimize any harm that might be caused to Viber. If you have entered into a specific Non- Disclosure Agreement with Viber, such Non-Disclosure Agreement shall prevail.

8. Availability and Support

Our Services may be interrupted, including for maintenance, repairs, upgrades, or network or equipment failures. We reserve the right to discontinue some or all of our Services in connection with the Viber Platform, at our sole discretion, including certain features and the support for certain devices and features. Events beyond our control may affect our Services, such as events in nature and other force majeure events. If you require support, please contact Viber Support through our **Contact Us Form**. Depending on your interaction with us, you may be assigned an account manager that can assist in need of technical support. Further, as a developer using the business messaging API and tools, the response time and support level is incorporated as part of the Ordering Documentations.

9. Data Protection

For the purpose of this section and these Business terms, the following definitions shall apply:

- **“Adequate Country**” is a country that received an adequacy decision from the European Commission.

- **"Applicable Data Protection Laws"** means any and all applicable federal, national, state, or other privacy and data protection laws (including, where applicable, EU Data Protection Law) as may be amended or superseded from time to time.

- **“Collected Data”** means the data each party collects on or through their servers or networks, including information that might be provided by Viber to the Developer, if requested by Developer, such as profile photo of the Viber user (if exists), unique identifier of a user for the unique Developer’s product and the user's profile name.

- **"Controller"** means an entity that determines the purposes and means of the processing of Personal Data.

- **"EU Data Protection Law"** means (i) EU General Data Protection Regulation (Regulation 2016/679) (“**GDPR**”); (ii) the EU e-Privacy Directive (Directive 2002/58/EC), as amended (**e-Privacy Law**); (iii) any national data protection laws made under, pursuant to, replacing or succeeding (i) and (ii); (iv) any legislation replacing or updating any of the foregoing (v) any judicial or administrative interpretation of any of the above, including any binding guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority.

- “**Personal Data**” means any information that relates to an identified or identifiable individual (and such term shall include, where required by Applicable Data Protection Law, unique browser or device identifiers).

- **“Standard Contractual Clauses**" means the standard contractual clauses for the transfer of Personal Data to third countries pursuant to the GDPR and adopted by the European Commission **Decision 2021/914** of 4 June 2021, which is attached herein by linked reference: **https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN.**

- **“SCC Annexes”** means Annex I and Annex II attached herein.

- "**UK GDPR**” means the Data Protection Act 2018 and the GDPR as it forms part of the law of England and Wales, Scotland, and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments, etc.) (EU Exit) Regulations 2019 (SI 2019/419).

- “**UK SCC**” means where the UK GDPR applies, the standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR for transferring Personal Data outside the EEA or UK.

The parties acknowledge that some or all of the Collected Data may qualify as or include Personal Data and that Applicable Data Protection Laws may apply to the processing of the Collected Data. Each party shall comply with such Applicable Data Protection Laws with respect to its processing of the Collected Data as an independent Controller of the Personal Data. Each party shall be individually responsible for its compliance with Applicable Data Protection Laws, including for providing any transparency and obtaining any lawful basis for the processing of Collected Data that may be required under Applicable Data Protection Laws.

Each party agrees that it shall process the Collected Data that it collects only for the purposes permitted by this Agreement and Applicable Data Protection Law.

Each party shall implement appropriate technical and organizational measures to protect the Collected Data from (i) accidental or unlawful destruction and (ii) loss, alteration, unauthorized disclosure of, or access to the Collected Data.

Where EU Data Protection Law applies, neither party shall process its Collected Data (nor permit its Collected Data to be processed) in a territory outside of the European Economic Area ("**EEA**") or the UK unless the transfer is to an Adequate Country or it has taken such measures as are necessary to ensure the transfer complies with EU Data Protection Law, including by incorporating the Standard Contractual Clauses and the UK SCC, as applicable. As between Viber and the Developer, Module I of the Standard Contractual Clauses shall apply, including the SCC Annexes.

10. Security

Developers shall implement and follow generally recognized industry standards and best practices for data and information security to protect its data, including implementing technical and security measures as detailed under the SCC Annexes. Developers must promptly delete any information it obtained via the Developer Platform if Viber determines, in its sole discretion, that the Developer breached its obligation to protect and prevent unauthorized use or access to its devices, Developer Platform, or systems, breached the Business Terms, or if the Business Terms are terminated for any reason.

By using the Developer Platform, you hereby acknowledge and agree that Viber may monitor your use of the Developer Platform to ensure quality, improve Viber's products and services, and verify your compliance with the Business Terms, including accessing and using your Chatbot to identify security issues that could affect Viber or its Users. You will not interfere with this monitoring, and Viber may use any technical means to overcome such interference.

11. Termination

We may suspend or terminate the Developer’s access to or use of our Developer Platform and the Business Terms, at any time and for any reason, permissible by applicable law, including if we determine, in our sole discretion, that the Developer violates its obligations or representations under the Business Terms, receives excessive negative feedback, or creates harm, risk, or possible legal exposure for us, our users, or others. To the extent permissible and practicable, subject to Viber's sole discretion, we will endeavor to give you prior notice containing the relevant reasons for termination or suspension. The Developer may cease using the Viber API at any time, without derogating from any outstanding payment obligations below and other obligations applicable under the Ordering Documents.

Upon termination or suspension: (i) all licenses granted to you herein shall terminate immediately; (ii) Developers must promptly discontinue all use of the Developer Platform, uninstall and destroy all copies of software provided by Viber, and delete any information Developer obtained from using the Developer Platform; (iii) upon Viber’s written request, you shall delete or return to us, any Viber confidential information; (iv) pay any outstanding fees to Viber; and (vi) the provisions herein that by their nature are intended to continue indefinitely will continue to apply.

Termination for any reason of these Terms shall not derogate from your rights and obligations accrued prior to the effective date of termination and shall not limit Viber from pursuing other available remedies.

You may contact Viber using our **Viber support** or the **Contact Us Form** to clarify the reasons for our termination or suspension of your interaction or use of the Developer Platform. If we are able to resolve the issue in your favor, resulting in reactivating your use of the Developer Platform, then we will reinstate our Services to you within a reasonable time.

12. 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 THE DEVELOPER PLATFORMS ARE FREE OF INACCURACIES, ERRORS, BUGS, OR INTERRUPTIONS, OR ARE RELIABLE, ACCURATE, COMPLETE, OR OTHERWISE VALID. TO THE EXTENT PERMITTED BY APPLICABLE LAW, THE DEVELOPER PLATFORMS ARE PROVIDED “AS IS” AND "AS AVAILABLE" 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 OR NON-INFRINGEMENT. YOUR USE OF THE DEVELOPER PLATFORMS 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.

13. Limitation of Liability

TO THE EXTENT PERMITTED BY APPLICABLE LAW, VIBER SHALL NOT, UNDER ANY CIRCUMSTANCES, BE LIABLE TO YOU FOR ANY INDIRECT, PUNITIVE, ACTUAL, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH ANY MANNER OF USE, OR INABILITY TO USE, THE DEVELOPER PLATFORMS, 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. 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. In no event shall Viber’s aggregated liability to you for all damages 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.

14. Indemnification

To the maximum extent permitted by applicable law, the Developer agrees 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 or consequential), suits, judgments, litigation costs, and attorneys' fees, every kind and nature. Viber shall use good faith efforts to provide you with written notice of such claim, suit, or action.

PLEASE NOTE THAT ALL OTHER PROVISIONS NOT SPECIFICALLY ADDRESSED HEREIN SHALL BE GOVERNED BY THE VIBER APP TERMS OF SERVICE, INCLUDING BUT NOT LIMITED TO GOVERNING LAW AND JURISDICTION CLAUSE AND MISCELLANEOUS CLAUSE.

Annex to the Standard Contractual Clauses referred in Section 9

Annex I

(Controller to Controller)

A. LIST OF PARTIES

Viber and Developer as defined above.

B. Description of Processing and Transfer

Categories of data subjects whose personal data is processed or transferred:

Viber users (either using the Chatbot or their information is made available to the Developer through Developer tools or the Viber API).

Categories of personal data processed or transferred:

Depending on the Developer’s request, Viber may share the Collected Data with the Developer, which includes one or all of the following: Profile photo of the user (if it exists), unique identifier of the user for the unique Developer’s product, and the user's profile name.

Sensitive data processed or transferred:

NA

The frequency of the processing or transfer (e.g., whether the data is transferred on a one-off or continuous basis):

Continuous basis

Nature of the processing or transfer:

The Developer receives the personal data via the Viber API and processes it for the below purpose.

Purpose(s) of the data transfer and further processing:

Enabling personalization of the Developer’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:

As long as required by applicable laws or to provide the Business Services.

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

NA

C. COMPETENT SUPERVISORY AUTHORITY

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

Annex II

Technical and Organizational Security Measures

This Annex II summarizes the technical, organizational, and physical security measures implemented by the parties:

The Developer shall comply with the following:

Developer 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 unauthorized 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 staffed 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 authorization (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 the 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 login, 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 authorization (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 authorization 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.
- 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 tha appropriate personnel and service providers and monitoring of contract performance, 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 a separate location, mirroring of hard disks, uninterruptible power supply, and auxiliary power unit, remote storage, climate monitoring and control for servers, fireresistant doors, fire, and smoke detection, fire extinguishing system, anti-virus/firewall systems, malware protection, disaster recovery, and emergency plan.

8. *Ensuring that data collected for different purposes or different principles 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.