HiveMQ SaaS Terms

1. Introduction

For Customers with a billing address in the EMEA region HiveMQ GmbH, Postplatz 397, 84028 Landshut, Germany and for Customers with a billing address outside the EMEA region HiveMQ Inc., 600 N Broad Street, Suite 5, 553 Middletown DE 19709, USA (each of which referred to as “**Company**” or “**HiveMQ**”) and Customer as specified in the given Quote (“**Customer**”) agree upon the provision of the Services by executing a Quote, each Party's rights and obligations regarding the provision of the Service are exclusively governed by the following HiveMQ Subscription Terms (“General Terms”) and the accompanying Annexes listed below (“**Services Terms**”). The General Terms and the Service Terms only enter into effect once a corresponding Quote has been executed by both Parties. The Quote, the General Terms and the Service Terms shall together be referred to as the "Agreement". In the event of any conflict or inconsistency between the provisions of the General Terms and the provisions of any Quote or Service Terms, the provisions positioned higher in the following list shall take precedence only to the extent of any such conflict or inconsistency:

1. These General Terms
2. Services Terms
   - **Annex C – Support Policy**
   - **Data Processing Agreement**
3. Quote

1. Definitions

Unless otherwise defined herein, the following terms shall have the meaning set out below:

- **“Authorized Affiliate”** has the meaning given to that term in Section “**Use by Authorized Affiliates**”

- "**Company Marks**" means the trademarks, trade names, service marks, logos, and/or service names of the Company.

- "**Confidential Information**" has the meaning given to that term in Section "**Confidential Information**".

- "**Contract Year**" means every 12-month period during the Term of a Quote or the Agreement, calculated from its Effective Date.

- "**Contractual Use**" means the use of the HiveMQ Platform for the permitted use cases or any further license volume description detailed in the given Quote. By way of example (but not limited to), a Quote may set forth the permitted maximum number of CPU cores and/or clusters, on which HiveMQ Platform may be deployed and/or the maximum number of concurrent connections managed by HiveMQ Platform and/or the physical locations at which the HiveMQ Platform may be used.

- "**Customer Data**" means any data uploaded into or run through the HiveMQ Platform (whether manually, or automatically via APIs) by or on behalf of Customer or an Authorized Affiliate, or generated through Customer's, or an Authorized Affiliate's, use of the HiveMQ Platform in accordance with this Agreement, including any modifications to such data. For clarity, Service Generated Data is not Customer Data.

- "**Customer Marks**" means the trademarks, trade names, service marks, logos, and/or service names of the Customer.

- **"Deliverables"** means any software work product, which is and / or will be developed on behalf of Customer as a separate technical functionality to any

HiveMQ Platform and which has originally, prior to such development, neither been a part or functionality of the HiveMQ Platform, nor has been scheduled for development under any product roadmap by HiveMQ's own initiative. A Deliverable is and stays legally and technically separated from the HiveMQ Platform and can be delivered to Customer as a separate software piece, independent of HiveMQ Platform.

- "**Documentation**" means the documentation for the HiveMQ Platform generally supplied by the Company to assist Customer in the use of the HiveMQ Platform and which includes user and functional reference manuals and other written materials, including application notes.

- "**Effective Date**" means the date on which either this Agreement or a Quote enters into force. In both cases, this is the date of the last signature on or acceptance of the respective contractual document.

- "**Extensions**" means applications which provide additional functionalities to a Specific Version of HiveMQ Platform and, if any, are subject to a Subscription according to a Quote. Extensions are provided by HiveMQ only in connection with the Subscription of a Specific Version of HiveMQ Platform. Any references made in this Agreement to HiveMQ Platform shall also apply to Extensions.

- "**Foreseeable Damages**" has the meaning given to that term in Section "**Foreseeable Damages**".

- "**GDPR**" means General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016.

- **"HiveMQ Platform"** means collectively the functionalities of HiveMQ's software-as-a-service platform which transmits and exchanges data between various devices, which Customer subscribed to under the applicable Quote, as further described in the applicable Quote, and as updated from time to time, including Updates of HiveMQ's software-as-a-service platform.

- "**Intellectual Property Rights**" or "IP" means intellectual property or proprietary rights, including but not limited to copyright rights (including rights in audiovisual works), moral rights, patent rights (including patent applications and disclosures), know-how, rights of priority, trademark rights, and trade secret rights recognized in any country or jurisdiction in the world.

- **"Term"** means the period in time during which the Agreement or a Quote is in effect, subject to the provisions under Section "**Term and Termination**".

- **"SaaS"** means provision of (i) the access to and use of the functionalities of the HiveMQ Platform remotely via an interface and (ii) support to Customer's use of the HiveMQ Platform as further described in Annex C.

- **"Personal Data"** means personal data that (a) has the meaning given to it in the GDPR and (b) would cause HiveMQ to be subject to GDPR as a data processor for Customer.

- **"Person Day"** means the efforts of one of Company's employees conducted within 8 (eight) hours.

- "**Professional Services**" means consulting and professional services designed to help Customer use of the HiveMQ Platform and Extensions as agreed upon under a Quote.

- **"Quote"** means an order form issued by HiveMQ and executed by Customer and HiveMQ via an online click-through process or in written form specifying the

HiveMQ Platform and Services HiveMQ will provide to Customer under this Agreement.

- **“Quote Term”** has the meaning given to that term in Section “**Quote Term**”.

- **“Service Generated Data”** means data or information about the operation, delivery, usage or performance of the SaaS, including, for clarity, activity logs or other data or information about Customer’s usage of the SaaS. Such data or information may be generated or derived automatically by the SaaS or tools associated with it, or manually by or on behalf of HiveMQ.

- “**Subscription**” means the Customer subscribing to the SaaS and/or Extensions as well as accompanying Support Services under a Quote.

- “**Subscription Fees**” means the remuneration for the Subscription as specified in the given Quote.

- “**Subscription Period**” means the contractual term detailed in each given Quote for which Customer is granted the rights in accordance with Section “**Right to Use and Access**” starting from the Effective Date of each given Quote.

- “**Support**” or “**Support Services**” means the provision of support services and provision of Updates for HiveMQ Platform as further described in Section “**Support Services**” and Annex C.

- “**Updates**” means new versions of the HiveMQ Platform released by HiveMQ after the respective Subscription of HiveMQ Platform, as further specified in Annex C.

2. Proprietary Rights

2.1. Retention of Rights.

Save as expressly set out in this Agreement, neither Party shall receive any right, title or interest in or to any Intellectual Property Rights owned by the other Party (including any modifications or enhancements made thereto). All rights not expressly granted in this Agreement are reserved by the Parties or their respective licensors. For the avoidance of doubt, HiveMQ (or its suppliers, where applicable) owns any Intellectual Property Rights in the HiveMQ Platform and the Documentation and all modifications, enhancements, improvements, derivative works, upgrades, new releases and other alterations of either of the foregoing (even if paid for, or requested or directed, by Customer), and Customer (or the relevant Authorized Affiliate) owns any right, title or interest, including any Intellectual Property Rights in Customer Data.

2.2. Feedback License

Customer grants, and ensures that every Authorized Affiliate grants, to HiveMQ a worldwide, royalty-free, transferable, sublicensable, irrevocable, perpetual license to use and incorporate into the HiveMQ Platform and the Documentation, and otherwise to freely exploit without restriction, any recommendations, enhancements, requests, corrections, suggestions or other feedback provided by or on behalf of Customer or an Authorized Affiliate relating to the functionality or operation of the HiveMQ Platform and the Documentation.

2.3. Use of Customer's Name

Customer agrees that the Company may use Customer's name and may disclose that Customer is a customer of the Company in advertising, press, promotion and similar public disclosures upon the prior written consent of Customer (such consent not to be unreasonably withheld or delayed). Customer also hereby grants the Company a non-exclusive license during the Term of this Agreement and Company shall list Customer's name and display Customer Marks on its home page and in the "partner," “customer” or similar sections of the Company’s website. The Company may also publicly issue and distribute a “case study” relating to this Agreement and the Company’s services performed on behalf of Customer, provided that it first obtains Customer’s prior written consent, such consent not to be unreasonably withheld or delayed. Customer agrees to act as a “reference account” with respect to the Company’s marketing and promotional initiatives.

2.4. Trademarks

Company may use the then current Customer Marks, provided that Company shall: (i) only use Customer Marks in the form and manner, and in accordance with the quality standards, that Customer prescribes (and which it may change from time to time) and (ii) upon termination of this Agreement for any reason, immediately cease all use of the Customer Marks. All goodwill associated with Customer Marks and Company’s use of such Customer Marks shall inure to the Customer. Company will not use, register or attempt to register, or take other action with respect to any name, logo, trademark, service mark, or other identifier used anywhere in the world by Customer (or a mark confusingly similar thereto), except to the extent authorized in writing by Customer in advance. For the avoidance of doubt, nothing in this Agreement grants Company any Intellectual Property Rights belonging to Customer.

3. Right to Access and Use

3.1. Customer’s Usage Right

Subject to Customer’s material compliance with its obligations under this Agreement, HiveMQ grants Customer, on a limited, non-exclusive and (subject to the Sections “**Use by Affiliates and Third Parties**” and “**Use by Authorized Affiliates**”) non-transferable basis, the right to access and use the SaaS, the Documentation and any output of the Related Services solely for the Purpose.

3.2. Use by Affiliates and Third Parties

Customer may allow its third party suppliers or service providers, and its Affiliates, to access and use the SaaS on Customer’s behalf, provided that: (i) such access or use must be solely for the benefit of Customer and not for the benefit of that supplier, service provider or Affiliate, (ii) the supplier’s, service provider’s or Affiliate’s access or use must be limited solely to what is required to provide its services to Customer in support of the Purpose and otherwise in accordance with the Agreement, and (iii) any such use must not be intended, in whole or in part, to circumvent any of the license restrictions in this Agreement or the applicable Order Form.

3.3. Use by Authorized Affiliates.

If an Authorized Affiliate is designated in a given Quote, Customer may allow such Authorized Affiliate to access and use the SaaS, provided that: (i) such right is limited to the Contractual Use specified in the Quote in which the Authorized Affiliate is mentioned, (ii) such use is limited to use by that Authorized Affiliate for that Authorized Affiliate’s own Contractual Use and (iii) the Authorized Affiliate will abide by all use restrictions and obligations applicable to Customer. Section “**Use by Affiliates and Third Parties**” does not apply to Authorized Affiliates.

3.4. Responsibility

Customer shall ensure Customer's Affiliates, third party suppliers or service providers and Authorized Affiliates are bound by written agreements incorporating terms and conditions that are at least as protective and restrictive as those in this Agreement. Customer shall be responsible and liable for the acts, defaults, omissions and negligence of any such parties as fully as if they were Customer's own acts, defaults, omissions or negligence.

3.5. Restrictions

Neither Customer nor any Authorized Affiliate nor any person acting on their behalf may use, directly or indirectly, the SaaS, the Documentation, materials or intellectual property provided or accessed under this Agreement in any manner or for any purpose other than as permitted by this Agreement. Without limiting the foregoing, the following are prohibited (including any attempt to do any of the following): (i) testing or reverse engineering, disassembling, or decompiling the SaaS, or parts thereof or any underlying code, methodology or intellectual property, or applying any other process or procedure to derive the code of any software included in the SaaS, (ii) accessing or using the SaaS in a way intended to avoid incurring any applicable fees or charges or purchasing additional licenses or access rights, (iii) reselling of the SaaS (iv) any misappropriation or unauthorized use or disclosure of the SaaS, Documentation or other HiveMQ intellectual property, (v) interfere with the use of the SaaS – or the equipment used to provide the Service, (vi) monitor data or traffic on any network or system without HiveMQ's authorization, (vii) use the SaaS where failure or fault of the SaaS could lead to death or injury of any person or to physical or environmental damages, (viii) use of the SaaS by persons, organizations, companies or any such legal entities, including affiliates, which are involved or suspected of involvement in activities or causes relating to illegal gambling; terrorism; narcotics trafficking; arms trafficking or proliferation, -development, design, manufacture, production, stockpiling, or use of nuclear, chemical or biological weapons, as well as weapons of mass destruction or missiles; this applies to any affiliation or part taking in such activities whatsoever, (ix) create an unusual level of load on the SaaS via non-intentional use, included in the SaaS or by using scripts or applications to access the APIs of the SaaS or (x) intentionally overflow and misuse of the SaaS by storing unusual amounts of persisted sessions and/or offline messages.

3.6. Use of HiveMQ Platform Non-Production Versions

If HiveMQ provides testing or non-production access to the HiveMQ Platform (including sandboxes) under a given Quote or subsequently, its use is limited solely to evaluation purposes within Customer’s own business environment and must not be used on production systems. HiveMQ shall not be liable for any damages arising out of or in connection with a use in productive systems.

3.7. Use of Extensions

To clarify, Extensions have no stand-alone capability and must only be used within the Contractual Use of the HiveMQ Platform as detailed in the applicable Quote. Unless otherwise provided for in a Quote, access rights to the Extension are granted for the Subscription Period applicable to the HiveMQ Platform which they functionally extend.

4. Modification and Deprecation of Services

4.1. Discontinuance Right

Subject to Section “**Deprecation Announcement**”, HiveMQ may discontinue any of the HiveMQ Platform features or functionality for any reason at any time without liability to Customer.

4.2. Deprecation Announcement

In the event that HiveMQ intends to discontinue or make backwards incompatible changes to the HiveMQ Platform, HiveMQ will notify Customer of such intention in advance. HiveMQ will then use commercially reasonable efforts to continue to operate those affected versions, features or functionalities without the noted changes for at least three months after that announcement, unless (as HiveMQ determines in its reasonable good faith judgment) (i) required by law or third-party relationship (including if there is a change in applicable law or relationship), or (ii) such continued operation could create a security risk or substantial economic or material technical burden.

4.3. Modification of the Service

In order to maintain a progressive and modern product experience and/or in order to keep up with good industry standards regarding security, reliability or regulatory compliance, HiveMQ reserves the right to make reasonable updates to the HiveMQ Platform from time to time. Such updates may relate to any features or functionality and/or the limitations of the HiveMQ Platform. If HiveMQ makes a material change to the HiveMQ Platform, HiveMQ will inform Customer reasonably in advance, but no later than 30 days before such change becomes effective. This does not apply in cases where such changes are required in order to solve security issues or to address regulatory changes or changes of the law.

5. Customer's Obligations

5.1. Prevention of Unauthorized Access

Customer shall implement and maintain processes and procedures to prevent unauthorized access to and use of the SaaS and shall notify HiveMQ as soon as practicable after Customer becomes aware of any such unauthorized access and use. Customer shall at all times use industry standard and up-to-date firewall and virus protection programs designed to ensure that no malicious code, such as viruses, worms, time bombs, Trojan horses, are uploaded to the SaaS.

5.2. Access Credentials

Customer or, as the case may be, an Authorized Affiliate, will create a username and a password for the initial access to the SaaS, which thereafter will be required for any further use of the SaaS. Customer, any Authorized Affiliate, third party suppliers or service providers shall keep the username and the password confidential and prevent any unauthorized access thereto. Any log-in credentials and private keys generated by the SaaS are for Customer's and any Authorized Affiliate's internal use only and

Customer and any Authorized Affiliate may not sell or transfer them to any other entity or person, except that Customer and any Authorized Affiliate may disclose its private key to any individual or entity that requires to use the SaaS in accordance with the permissions granted in this Agreement. Except to the extent caused by HiveMQ's breach of this Agreement, Customer is responsible for all activities that occur under its or an Authorized Affiliate's log-in credentials or private keys, regardless of whether the activities are authorized or undertaken by Customer or the Authorized Affiliate, or by their respective employees, contractors, agents or end clients.

6. Customer Data

6.1. General

As between the parties, Customer or, as the case may be, an Authorized Affiliate owns all right, title and interest in and to all Customer Data and shall have sole responsibility for the legality, accuracy and maintenance of Customer Data. Without limiting the foregoing, Customer shall obtain and maintain all necessary licenses, consents and other permissions (including those required under applicable laws), to authorize the processing of Customer Data (including any content protected by Intellectual Property Rights) by HiveMQ and HiveMQ's sub-processors in accordance with the terms of this Agreement. Customer hereby authorizes HiveMQ and HiveMQ's sub-processors to use, copy and process Customer Data for the purpose of providing the SaaS, Professional Services and performing its obligations under this Agreement.

6.2. Service Generated Data

Notwithstanding anything to the contrary, HiveMQ may aggregate, collect and analyze Service Generated Data and will be free (during and after the term of the Agreement) to: (i) use the Service Generated Data to develop and improve the HiveMQ Platform, Professional Services and any other HiveMQ offerings, and for other internal business purposes from time to time, and (ii) disclose the Service Generated Data solely in an anonymized format that does not identify Customer or any individual.

6.3. Backups

Customer acknowledges that the SaaS does not produce regular backups of Customer Data. Thus, Customer is solely responsible for regular and sufficient backups of all Customer Data on an environment other than the SaaS.

7. Suspension Right

HiveMQ has the right to immediately suspend Customer's and/or Customer's Affiliate's and/or Authorized Affiliate's use of the SaaS and/or Support Services (partially or in full) if HiveMQ assumes a: (i) violation of Section "**Prevention of Unauthorized Access**"; (ii) violation with applicable law; or (iii) Customer's breach of Section "**Restrictions**" or (iv) of its material payment obligations. HiveMQ will notify Customer of the reason for the suspension without undue delay. This notification obligation shall not apply where such notification would/may violate any applicable laws or regulations. HiveMQ will terminate any such suspension as soon as HiveMQ determines that the risk underlying the suspension has been mitigated to HiveMQ's satisfaction.

8. Pricing

8.1. Subscription Fees

a. Customer shall pay the Subscription Fees in accordance with the relevant Quote and this Agreement.

b. Customer is not entitled to withhold or delay payment of any invoice on the grounds that HiveMQ has failed to comply with a requirement not stated in the applicable Quote.

8.2. Tax

All Subscription Fees exclude taxes, including VAT, GST or IVA, and any withholding tax, except for HiveMQ's income taxes. If any withholding or deduction is required under applicable laws, Customer shall, when making payment of the Subscription Fees to which the withholding or deduction relates, pay to HiveMQ such additional amount as will ensure that HiveMQ receives the same total amount of the Subscription Fees that it would have received if no such withholding or deduction had been required.

8.3. Late Payment

If Customer fails to pay an invoice in a timely manner, HiveMQ will give Customer written notice. If such notice has been provided and payment has not been made within 5 (five) days of the receipt of the notice by Customer, then HiveMQ may charge Customer interest at the rate of 12% per year (or the highest rate permitted by law, whichever is lower). If HiveMQ initiates efforts to collect any payment due to it under any Quote, Customer shall be responsible for and pay all costs and expenses incurred by HiveMQ, including reasonable attorneys' fees.

8.4. Price Revisions

HiveMQ may modify the prices of Subscriptions at any time up to an amount of eight (8) percent of the annual aggregate pricing of the preceding Contract Year, unless otherwise expressly agreed in a Quote explicitly mentioning this Section. HiveMQ will notify Customer at least 30 days in advance of any such price increases. If HiveMQ notifies Customer of any price increase for a Subscription or Professional Services that Customer has used prior to receipt of such notification, Customer may terminate the respective Quote on 30 days' prior written notice to HiveMQ on condition that Customer provides such notice within 30 days of being informed of the respective price increases by HiveMQ. Customer's outstanding payment commitments (if any) that have accrued before the effective date of such termination are not affected.

8.5. Travel and Expenses.

Any Subscription Fees exclude travel and accommodation expenses for any business travel agreed by the Parties. Customer shall reimburse HiveMQ for reasonable and evidenced travel and accommodation cost upon Customer's prior approval.

8.6. Non-Payment

HiveMQ may suspend the provision of the SaaS or the Professional Services, or both, or terminate the Agreement for Customer's breach (either immediately or after a period of suspension), if Customer has failed to pay any Fees and the following conditions are met: (i) HiveMQ has served upon Customer two notices, each of which specifies the undisputed invoiced amount that is then unpaid and states HiveMQ's intention to suspend the SaaS or the Related Services, or both, or to terminate the Agreement for non-payment, and gives Customer 30 days to pay, with the second notice served no earlier than 30 days after the date of the first, (ii) 30 days have elapsed since the date of the second notice and Customer has failed to pay in full the undisputed invoiced amount specified in that notice. After suspension, access to the SaaS and the Related Services will be re-established promptly upon receipt of the sums referred to in the notices. HiveMQ and Customer shall discuss the overdue payment as soon as possible after HiveMQ has served the first notice.

9. Information Requests and Audits

9.1. Information Requests

No more than once per 6-month period, HiveMQ may request the Customer to provide information in written form about (i) the scope of use of HiveMQ Platform including the necessary details to assess the Contractual Use and (ii) any HiveMQ Platform sub-licenses granted by Customer pursuant to Sections "**Sublicenses to Affiliates/Third-Parties**" or "**Use by Authorized Affiliates**". Customer shall provide HiveMQ with the information within fifteen (15) days of written notice.

9.2. Audit Right

Should the Customer delay or fail to comply with the information obligation pursuant to Section "**Information Requests**", HiveMQ or an independent certified public accountant selected by HiveMQ may, at HiveMQ's sole expense, and no later than upon a five (5) days' advance written notice to Customer and during Customer's normal business hours, inspect the records of Customer related to its activities set forth in Section "**Information Requests**". If, upon performing such audit, it is determined that Customer has underpaid the Company by an amount greater than five (5) percent of the payments due the HiveMQ in the period being audited, Customer will bear all reasonable expenses and costs of such audit in addition to its obligation to make full payment under the given Quote. Company shall use commercially reasonable efforts to minimize any interference with Customer’s business while such audit is conducted.

10. Support and Professional Services

10.1. Support Services

HiveMQ shall provide Support Services during the Subscription Period of each given Quote in accordance with Annex C and covered by the Subscription Fees.

10.2. Additional Professional Services

Customer may purchase additional services or order deliverables from HiveMQ by executing a separate Quote referencing this Agreement and Annex B. Such services are subject to further terms and conditions set forth in each Quote. The fees per Person Day shall be determined in each applicable Quote.

11. Data Protection

The Parties shall comply with applicable data protection laws during the Term of the Agreement and each given Quote. If required by law, the Parties shall enter into a data protection agreement governing the data processing operations.

12. Confidentiality

12.1. Confidential Information

"Confidential Information" means: (i) the non-public code portions of the HiveMQ Platform and any accompanying Documentation; and (ii) any business, financial or technical information of either Party communicated to the other in connection with this Agreement, including but not limited to any information relating to such Party’s product plans, designs, costs, product prices and names, finances, marketing plans, business opportunities, personnel, research, development or know-how.

12.2. Exceptions

Confidential Information shall not include information that: (i) is in or enters the public domain without breach of this Agreement through no fault of the receiving party; (ii) the receiving party was demonstrably in possession of prior to first receiving it from the disclosing party; (iii) the receiving party can demonstrate by objective evidence was developed by the receiving party independently and without use of or reference to the disclosing party's Confidential Information; or (iv) the receiving party receives from a third party without restriction on disclosure and without breach of a nondisclosure obligation.

12.3. Obligations

Each Party will maintain the Confidential Information of the other Party in strict confidence and will exercise due care with respect to the handling and protection of such Confidential Information, consistent with its own policies concerning protection of its own Confidential Information of like importance (but in no event less than reasonable care). Each Party will use and disclose the Confidential Information of the other Party only as expressly permitted herein, and will disclose such Confidential Information only to its employees and consultants as is reasonably required in connection with the exercise of its rights and obligations under this Agreement. However, each Party may disclose Confidential Information of the other party pursuant to the order or requirement of a court, administrative agency, or other governmental body, provided that the receiving party gives reasonable notice to the other party to afford such Party an opportunity to intervene and contest such order or requirement. Any such disclosure by the receiving party of the Confidential Information of the disclosing party, will, in no way, be deemed to change, affect or diminish the confidential and proprietary status of such Confidential Information. The obligations of the Parties set forth in the Section "**Confidentiality**" shall survive the termination or expiration of this Agreement.

12.4. Destruction or Deletion

Within five (5) days of a termination or expiration of this Agreement, each Party will destroy all Confidential Information (and all copies and extracts thereof) of the other in its control or possession. Customer will certify to the Company that all copies of Confidential Information of the Company have been returned to the Company or destroyed, and the Company will certify to Customer that all copies of any Confidential Information of Customer have been returned to Customer or destroyed. Notwithstanding the foregoing, the receiving party may retain copies of Confidential Information stored on backup disks or in backup storage facilities automatically produced in the ordinary course of business which are not, in the ordinary course of business, accessible from employee workstations. Any such Confidential Information so retained will be held subject to the confidentiality and use limitations of this Agreement and will not be accessed by any person except information technology systems administrators (if technically required) nor used for any purpose except necessary data storage systems maintenance.

12.5. Injunctive Relief

Each Party acknowledges that the unauthorized use or disclosure of the Confidential Information of the other Party would cause substantial harm to such other Party that could not be remedied by the payment of damages alone. Accordingly, the non-breaching Party will be entitled to seek preliminary and permanent injunctive relief and other equitable relief for any breach of the Section “**Confidentiality**”.

13. Infringements

13.1. Indemnification by HiveMQ

Subject to the provisions of the Section “**Infringements**”, if a third party makes a claim against Customer alleging that HiveMQ Platform when used in accordance with its Documentation and this Agreement infringes the Intellectual Property Rights of any third party arising under U.S. or E.U. law, HiveMQ shall defend Customer against the claim and shall pay all damages awarded by a court of competent jurisdiction or agreed to in settlement of the claim.

13.2. Indemnification by Customer

Subject to the provisions of the Section “**Infringements**”, if a third-party makes a claim against HiveMQ alleging that Customer Data infringes or misappropriates that third party’s patent, copyright, trademark or trade secret, Customer shall defend HiveMQ against the claim and shall pay all damages awarded by a court of competent jurisdiction or agreed to in settlement of the claim.

13.3. Exclusions and Procedure

a. In the event that HiveMQ Platform is likely to, in HiveMQ’s sole opinion, become the subject of a claim described in Section “**Indemnification by HiveMQ**”, HiveMQ shall, in its sole discretion, either (i) modify or replace HiveMQ Platform without loss of significant functionality, or (ii) procure a license for Customer to continue using HiveMQ Platform as licensed herein. If HiveMQ determines that neither of the foregoing is commercially practicable, HiveMQ may terminate this Agreement and all licenses granted hereunder by written notice to the Customer, and Customer will cease all use of HiveMQ Platform. HiveMQ will have no liability to Customer as a result of such termination.

b. HiveMQ shall have no liability for any claim or demand arising from (i) an allegation that does not state with specificity that HiveMQ Platform is the basis of the claim; (ii) the use or combination of HiveMQ Platform or any part thereof with software, hardware, or other materials not developed by HiveMQ where HiveMQ Platform or use thereof would not constitute infringement but for said combination; (iii) modification of HiveMQ Platform by a party other than HiveMQ, where the use of unmodified HiveMQ Platform would not constitute infringement; (iv) an allegation that the HiveMQ Platform consists of a function, system or method that utilizes functionality that is in general use in the industry; or (v) an allegation made against Customer prior to the execution of this Agreement or any allegation based upon actions taken by Customer prior to the execution of this Agreement, or relating to any patent that Customer was aware of prior to the execution of this Agreement. Customer shall bring to HiveMQ's attention any such prior or existing or known patent or other intellectual property claims, demands or allegations made on it that are material to the Section "**Infringements**", in writing, prior to the execution of this Agreement.

c. The obligations under the Section "**Infringements**" and any other indemnification obligations set forth in this Agreement shall be subject to the following conditions: (i) Customer shall notify HiveMQ in writing within ten (10) days of learning of any claim for which indemnification is sought, provided however, that any failure to provide such notice shall relieve HiveMQ of its indemnification obligations hereunder only to the extent of any demonstrable prejudice suffered by HiveMQ as a result of such failure; (ii) HiveMQ shall have sole control of the defense or settlement of such claim, provided that Customer shall have the right to participate in such defense or settlement with counsel of its selection and at its sole expense and provided further that HiveMQ shall not enter into any settlement of any claim without Customer's prior, written approval, which approval shall not be unreasonably withheld, conditioned or delayed; and (iii) Customer shall reasonably cooperate with Company in the defense and settlement of the claim, at HiveMQ's expense.

d. Subject to Section "**Limitation of Liability**", the Section "**Infringements**" states the sole remedy of Customer and the entire liability of HiveMQ with respect to any infringement of Intellectual Property Rights.

14. Warranty Disclaimer

HIVEMQ PLATFORM AND ALL SERVICES ARE PROVIDED BY COMPANY AS IS AND, TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, COMPANY DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, ORAL OR WRITTEN, INCLUDING, BUT

NOT LIMITED TO, THE IMPLIED WARRANTIES AND CONDITIONS OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTIES ARISING FROM COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY COMPANY, ITS EMPLOYEES OR AGENTS SHALL CREATE ANY WARRANTIES.

Further, HiveMQ does not represent or warrant that: (i) HiveMQ Platform will meet Customer's business requirements; (ii) HiveMQ Platform will be error-free or uninterrupted or that the results obtained from its use will be accurate or reliable; or (iii) all deficiencies in HiveMQ Platform can be found or corrected.

15. Limitation of Liability

15.1. Limited Liability

EXCEPT FOR AMOUNTS DUE HEREUNDER, LIABILITY ARISING FROM A PARTY'S BREACH OF ITS CONFIDENTIALITY OBLIGATIONS SET FORTH IN SECTION "CONFIDENTIALITY", USE BY CUSTOMER OF HIVEMQ PLATFORM, IN WHOLE OR IN PART, OUTSIDE OF THE SCOPE OF THE LICENSES GRANTED HEREIN, OR A PARTY'S GROSS NEGLIGENCE OR WILFUL MISCONDUCT, IN NO EVENT SHALL EITHER PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, EXCEED THE AMOUNTS ACTUALLY PAID BY AND DUE FROM CUSTOMER UNDER THIS AGREEMENT DURING THE TWELVE (12) MONTHS PRIOR TO THE DATE ON WHICH SUCH CLAIM OR CAUSE OF ACTION AROSE.

15.2. Exclusion of Consequential and Related Damages

EXCEPT FOR AMOUNTS DUE HEREUNDER, LIABILITY ARISING FROM A PARTY'S BREACH OF ITS CONFIDENTIALITY OBLIGATIONS SET FORTH IN SECTION

“CONFIDENTIALITY”, USE BY CUSTOMER OF HIVEMQ PLATFORM, IN WHOLE OR IN PART, OUTSIDE OF THE SCOPE OF THE LICENSES GRANTED HEREIN, OR A PARTY’S GROSS NEGLIGENCE OR WILFUL MISCONDUCT, IN NO EVENT SHALL EITHER PARTY OR ITS EMPLOYEES OR AGENTS BE LIABLE TO THE OTHER PARTY OR ANY OTHER PARTY FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING WITHOUT LIMITATION DAMAGES DUE TO LOSS OF DATA, LOSS OF PROFITS, LOSS OF REVENUE, LOSS OF USE COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR COMPUTER FAILURE ARISING FROM THIS AGREEMENT OR THE USE OF THE HIVEMQ PLATFORM, HOWEVER CAUSED AND, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY REMEDY. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON DURATION OR THE EXCLUSION OF AN IMPLIED WARRANTY, SO THE ABOVE LIMITATION MAY NOT APPLY.

15.3. Limitation of Action

Except for actions for non-payment or breach of either Party's intellectual property rights, no action (regardless of form) arising out of this Agreement may be commenced by either Party more than one (1) year after the cause of action has accrued.

16. Term and Termination

16.1. Agreement Term

This Agreement commences on the Effective Date and continues in force and effect until all Quotes have been terminated or have expired, subject to the termination rights under the Agreement.

16.2. Quote Term

Subject to earlier termination as provided herein, each Quote shall be in force for an unlimited period of time. The Parties are entitled to terminate the Quote at any time for any reason by giving at least fourteen (14) days written notice.

16.3. Termination

Either Party may terminate this Agreement or a Quote for cause immediately by written notice upon the occurrence of any of the following events:

I. if the other Party ceases to do business, or otherwise terminates its business operations;

II. if the other Party is adjudicated as bankrupt, or if a petition in bankruptcy is filed against the other party and such petition is not discharged within sixty (60) days of such filing; or

III. if Customer breaches (i) Section "**Prevention of Unauthorized Access**" or (ii) Section "**Restrictions**"; or

IV. if the other Party breaches any material provision of this Agreement and fails to fully cure such breach within thirty (30) days of written notice describing

16.4. Effect of Termination

Termination shall not relieve Customer of the obligation to pay any Subscription Fees accrued or payable to Company prior to the effective date of termination. Upon termination or expiration of this Agreement and/or a Quote, the rights and licenses granted to Customer hereunder shall automatically terminate.

16.5. Separation Damages

Upon expiration of this Agreement or termination in accordance with the Section "**Term and Termination**", Customer shall not be entitled to any separation compensation or damages of any kind, including indemnification, compensation, reimbursement, or damages for loss of prospective compensation, goodwill or loss thereof, or expenditures, investments, leases, or any type of commitment made in connection with the business of such party or in reliance on the existence of this Agreement including, but not limited to advertising and promotion costs, costs of supplies, termination of employees, employee salaries, and other such costs and expenses.

16.6. Survival

Termination or expiration of this Agreement shall not relieve either party of any payment or other obligation under this Agreement which was to have been performed by such party prior to the termination. All provisions of this Agreement which by their nature are intended to survive the termination or expiration of this Agreement including, without limitation, the provisions of an applicable Quote and Sections "**Information Requests and Audits**", "**Confidentiality**", "**Proprietary Rights**", "**Limitation of Liability**", "**Effect of Termination**", "**Separation Damages**", "**Survival**" and "**General**" will survive the termination of this Agreement.

17. General

17.1. Modification Right

a. HiveMQ may make changes to this Agreement from time to time subject to the following conditions:
   i. Unless noted otherwise, material changes to the Agreement will become effective 30 days after they are communicated to Customer.
   ii. If the changes will apply to new features or functionalities or the changes are required by a court order or applicable law, they will be effective immediately.

b. HiveMQ shall have the following objection right in connection to changes to the Agreement as set forth in Section "**Modification Rights**":
   i. If a change to the Agreement (other than as described in Section "**Modification Rights**", point 2) has a material adverse impact on Customer, then Customer may object to the change by notifying HiveMQ within 30 days after HiveMQ provides notice.
   ii. If Customer so notifies HiveMQ, then Customer, in case a Subscription Period was agreed between the Parties, will remain governed by the

Agreement in effect immediately before the change until the earlier of: (a) the end of the then-current Subscription Period; or (b) 12 months after the notice was given.

17.2. Compliance with the Law

Customer is responsible for compliance with legal obligations, especially any regulatory and security requirements. Customer acknowledges and agrees that the HiveMQ Platform and other technical data provided hereunder may be subject to restrictions and controls imposed by the United States Export Administration Act of 1979, as amended and the regulations promulgated thereunder. Customer represents that Customer, any of its Affiliates or other third parties receiving a sublicense in accordance with Section "**Sublicenses to Affiliates/Third-Parties**" or "**Use by Authorized Affiliates**" are not subject to sanctions or otherwise designated on any list of prohibited or restricted parties, including but not limited to the lists maintained by the United Nations Security Council, the U.S. Government (e.g., the U.S. Department of Treasury's Specially Designated Nationals list and Foreign Sanctions Evaders list, and the U.S. Department of Commerce's Entity List), the European Union or its member states, or other applicable government authority. A breach of this Section is a material breach of the Agreement. Customer further agrees to comply with all laws and regulations of all jurisdictions in Customer's use of the HiveMQ Platform.

17.3. Choice of Law

This Agreement will be governed by and construed in accordance with the laws of the State of New York without regard to conflicts of laws principles and specifically excluding the provisions of the United Nations Convention on the International Sale of Goods or the UCITA. Any legal action or proceeding with respect to this Agreement will be brought in the United States District Court for the Southern District of New York or any state court located in such Southern District. By execution and delivery of this Agreement, each of the Parties hereto accepts for itself and in respect of its property, generally and unconditionally, the exclusive jurisdiction of the aforesaid courts.

17.4. Assignment

Customer may not assign this Agreement, in whole or in part, without the Company's prior written consent. Any attempt to assign this Agreement without such consent will be null and void. Company may freely assign this Agreement without Customer’s consent. Subject to the foregoing, this Agreement shall bind and insure to the benefit of the Parties, their respective successors and permitted assigns.

17.5. Notices

All notices in connection with this Agreement shall be in writing in English and shall be delivered by email to the contact specified by the Parties.

17.6. Severability

If any provision of this Agreement is found by any court, tribunal or administrative body or authority of competent jurisdiction to be illegal, invalid or unenforceable then that provision will, to the extent required, be severed from this Agreement and will be ineffective without, as far as is possible, modifying any other section or part of this Agreement, and the legality and enforceability of the other provisions of this Agreement will not be affected.

17.7. Waiver

No failure of either Party to exercise or enforce any of its rights under this Agreement will act as a waiver of such rights.

17.8. Independent Contractors

The Parties to this Agreement are independent contractors. There is no relationship of partnership, joint venture, employment, franchise, or agency between the Parties. Neither party will have the power to bind the other or incur obligations on the other’s behalf without the other’s prior written consent.

17.9. Force Majeure

Neither Party will be responsible for any failure to perform due to causes beyond its reasonable control, including, but not limited to, acts of God, war, riot, embargoes, acts of civil or military authorities, denial of or delays in processing of export license applications, fire, floods, earthquakes, accidents, strikes, or fuel crises, pandemics provided that such party gives prompt written notice thereof to the other Party.

Annex C
HiveMQ Cloud Support Policy

This Annex C – HiveMQ Support Policy, governs the provision of Support Services for the HiveMQ Platform offered under the applicable HiveMQ SaaS Terms (hereinafter "**Agreement**"). All capitalized terms used but not otherwise defined herein have the meanings given to them in the Agreement.

1. Definitions

- **"Basic Support"** means HiveMQ's standard support offerings as specified in this Support Policy.
- **"Support Services"** means the support services contracted by Customer from HiveMQ in accordance with the Agreement and the applicable Quote.
- **"Designated Contact(s)"** means the individual(s) within Customer's organization assigned in accordance with Section 2.2 of this Annex C.
- **"Incident(s)"** means those issues relating to the Software that are covered under this Support Policy, as specifically set forth herein below.
- **"Response Time(s)"** means the amount of time within which HiveMQ's Customer support team commits to respond to Service Requests (as set forth in Section 2.7 of this Annex C).
- **"Service Request"** means a Customer request as set forth in Section 2.4 of this Annex C for assistance from HiveMQ with respect to an Incident.
- "**Support Hours**" means the applicable Support Hours (Basic Support Hours or Extended Support Hours) as defined in this Support Policy.
- "**Basic Support Hours**": Mon-Fri 9:00am CET - 6:00pm EST, excluding applicable international holidays.

2. Contracted Support Coverage

2.1 **Duration**. HiveMQ shall provide Support Services for the Subscription Period specified in the respective Quote.

2.2 **Appointment of Designated Contacts**. To receive Support Services, Customer shall (i) appoint at least one Designated Contact and (ii) notify HiveMQ in written form (email sufficient) of the names and contact details of the Designated Contact(s).

2.3 **Scope of Support Service**. The Support Services cover HiveMQ Platform and Certified Customer Plugins as follows:

(a) Submission of Service Requests by Designated Contacts via email;

(b) Customer may demand up to two (2) Designated Contacts;

(c) Email support during Support Hours with Basic Support;

(d) Unlimited number of Incidents; and

(e) Response Times for Incidents as defined in the Response Times table below.

2.4 Submission of Service Requests

(a) Customer shall submit all Service Requests via email to HiveMQ.

(b) Customer shall ensure that the software involved in the incident is covered by Support Services under Basic.

(c) Customer shall use reasonable efforts to fix any error, bug, malfunction or network connectivity defect before submitting a Service Request to HiveMQ.

(d) Customer shall suggest a Priority level according to Section 2.7 upon submission of Service Requests. HiveMQ reserves the right to check and in its sole discretion change Customer's Priority suggestion if HiveMQ believes that Customer's suggestion is incorrect and will inform Customer of any such change in its response to the Service Request. Customer may appeal any such reclassification to HiveMQ's support management for review through any available support channel. To successfully challenge a classification by HiveMQ, Customer needs to provide proof in accordance with the Priority level definition that HiveMQ's Priority designation was incorrect.

(e) Customer shall provide all requested diagnostic and technical information and assist HiveMQ as may be reasonably required to resolve a Service Request.

(f) HiveMQ may respond to a Service Request by acknowledging receipt of the request. Customer acknowledges and understands that HiveMQ may be unable to provide answers to, or resolve all Service Requests.

(g) If HiveMQ deems a Service Request to be a "New Feature" Service Request, HiveMQ will log such requests for consideration to add to a future update or release of the Software and will consider the matter closed. HiveMQ is under no obligation to respond to or resolve any feature request or to include any such feature request in any future version.

(h) HiveMQ does not demand or require personal data/personally identifiable information ("PII") for resolving Service Requests, other than the email address of the individual who submitted the Service Request for communication purposes. When uploading evidence or information related to an issue in the form of e.g., log files or screenshots/screen captures, Customer shall ensure that (1) all PII has been anonymized or masked before being uploaded into the support ticket; and (2) if masking or anonymizing the PII is technically impossible, the respective data subject has consented to the processing of the related PII or you have other valid legal grounds for it.

2.5 **Delivery of new Versions.**

The Support Services include the delivery of the following Updates for HiveMQ Platform:

(a) “**Major Version**” means a version of HiveMQ Platform resulting in major enhancements to the HiveMQ Platform and is identified by the first number of the Software’s version numbering (e.g. HiveMQ 3.x.x).

(b) “**Feature Versions**” means a version includes minor enhancements and/or error corrections to HiveMQ Platform and is identified by the second number of the HiveMQ Platform’s version numbering (e.g. HiveMQ x.2.x).

(c) **“Long Time Support (LTS) Versions”** means a special Feature Versions that focus on performance and stability improvements. LTS Versions offer longer support than regular Feature Versions of HiveMQ.

(d) “**Maintenance Versions**” means a new version of HiveMQ Platform with a fix of certain issues and is identified by the third number of the HiveMQ Platform’s version numbering (e.g. HiveMQ x.x.1).

(e) **“Hotfix Versions”** means a version of HiveMQ Platform with a temporary fix of certain issues developed in HiveMQ’s sole discretion upon a specific Customer request and delivered before a formal version with correct and final fixes are provided.

2.6 **Priority Definitions**

(a) **“Priority 1 – High Severity”** means an Incident preventing Customer from continuing use of Software, or critically impacting a core function of the Software or Customer’s environment causing the Software to experience downtime. No workaround is known to Customer.

(b) **“Priority 2 – Medium Severity”** means an Incident preventing Customer from continuing use of a non-core function of the Software, but does not affect the performance or functionality of Customer’s environment in its entirety. The Incident impacts Customer’s ability to use the Software, the severity of which is significant and may be repetitive in nature. Priority 2 is the highest possible level for all non-production systems.

(c) **“Priority 3 – Low Severity”** means minor errors, which do not inhibit any of the core functionality of the Software. Error negligibly impacts Customer’s ability to use the Software, and the Software remains mainly functional. This Priority level may include any Software issue with a viable workaround.

(d) **“Priority 4 – Request for Information”** includes minor, cosmetic, or documentation-related issues, and enhancement requests that are not time-sensitive. There is no impact on the Software existing features, functionality, performance or stability. This Priority Level includes any development support related incidents.

2.7 Response Times

HiveMQ shall use commercially reasonable efforts to answer to Customer’s Service Requests. The Priority Level shall be indicated by Customer with each Service Request. HiveMQ may reclassify the Priority Level at its sole discretion.

Response Times for Cloud Starter Plan during Support Hours are defined as follows:

	Basic Support
Priority 1 Response Time*	8 hours
Priority 2 Response Time* (within Support Hours)	8 business hours
Priority 3 Response Time* (within Support Hours)	16 business hours
Priority 4 Response Time* (within Support Hours)	24 business hours

*Response Times begin when Customer has submitted a Service Request in accordance with Section 2.4.

2.8 Support Services Exclusions.

The following cases are not covered by the Support Services:

(a) Support Requests in a period in which Customer has not fully paid all fees due to HiveMQ;

(b) Maintenance and support of the system environment, including, but not limited to, mobile hardware and third-party applications used by Customer in connection with the Software;

(c) Training and setup of HiveMQ Platform;

(d) Identification of errors caused by force majeure, environmental conditions, defective mobile hardware or errors caused by Customer, its affiliates or third parties, in particular due to incorrect or incomplete system or data entries or interventions in the program code by employees or contractors of Customer and/or its affiliates;

(e) Data conversion services;

(f) IT architectural guidance and consulting on how to integrate HiveMQ into Customer’s specific use case; and

3. Service Level Agreement (SLA)

During the term of HiveMQ Subscriptions, the SaaS Services booked by the Customer will be made available by HiveMQ with a Monthly Uptime Percentage as defined below (the “**Service Level**”).

3.1 Definitions

- “Downtime” is the total accumulated minutes in a calendar month during which the entire HiveMQ Cluster Package booked by the Customer within a certain HiveMQ Subscription is unavailable. Downtime does not include (i) Events beyond HiveMQ’s Control as defined in the following; (ii) Downtimes during Maintenance Windows as defined in the following and ○ Downtimes of less than 1 (one) minute per hour. The point of delivery relevant for the calculation of Downtimes is the interface between the servers on which the HiveMQ Cluster(s) is/are hosted and the Internet.
- “Events beyond HiveMQ’s Control” are the events as further described in Section 3.5 below.
- “Maintenance Windows” are periods of time during which HiveMQ performs maintenance works that cause unavailability of SaaS Services, provided that HiveMQ has notified the Customer of these periods at least 5 days in advance in textual form. The total duration of the Maintenance Windows per calendar month for each HiveMQ Subscription is 4h (four hours). If calendar months are not completely within the term of a HiveMQ Subscription, the total duration of the Maintenance Windows in the relevant month is reduced pro rata temporis.
- “Monthly Uptime Percentage” means the total number of minutes in a calendar month, minus the number of minutes of Downtime in such month, the result of which being divided by the total number of minutes in such month, multiplied by 100.
- “Service Credit” means an amount of money, equaling the percentage of monthly Subscription fees for a certain HiveMQ Subscription, calculated as described below, credited to Customer in accordance with the process described in this SLA.

3.2 Service Level

HiveMQ warrants a Monthly Uptime Percentage of 99.95% for C*loud Starter Plan* and 99.5% for the *Pay As You Go Plan* booked with HiveMQ Subscriptions. The Service Level will be calculated separately for each HiveMQ Subscription.

3.3 Calculation of Service Credits

In the event that the Service Level is not met in a calendar month with respect to one or more active Subscription Agreement(s), the Customer will be granted certain Service Credits according the following provisions of this SLA.

Service Credits are calculated in accordance with the schedule below as a percentage of the total monthly net Subscription fees payable by the Customer for the unavailable HiveMQ Cluster

Package for the calendar month in which the Service Level is not met. In case of non-monthly payments (such as one-time payments, upfront payments etc.) the calculation is based on the calculated monthly amount from the total amount taking into account the contractually agreed duration of the affected Subscription Agreement.

HiveMQ Cloud Pan	**Monthly Uptime Percentage**	**Service Credit**
HiveMQ Cloud Starter Plan	Less than 99.9% but equal to or greater than 99.0%	5% of the calculated monthly net subscription fee
	Less than 99.0% but equal or greater than 90.0%	10% of the calculated monthly net subscription fee
	Less than 90.0%	25% of the calculated monthly net subscription fee

3.4 Service Credit Request and Payment

In the event that HiveMQ fails to meet the above-mentioned Service Level, HiveMQ shall offer Service Credits as compensation to the Customer in accordance with the following provisions.

To receive a Service Credit, Customer must submit a textual request (the “Credit Request”), either by logging a support ticket or by sending an email to cloud@hivemq.com. To be eligible, the Credit Request must be received by HiveMQ within ten (10) calendar days after the last day of the month in which the SaaS have not met the Service Level, and must include all information reasonably necessary for HiveMQ to verify the request, including:

a. the words “SLA Credit Request” in the subject line;
b. a description of the Customer’s applicable MQTT client(s), the version of each such client, and the configurations for each such client; and
c. a description of the time and duration of the Downtime and Customer and system logs that document the failed connect and publish attempts.

If HiveMQ’s monitoring systems accessing the same endpoints as well as its system logs, monitoring reports, configuration records, and other available information determine that the Monthly Uptime Percentage applicable to the calendar month to which the Credit Request referred did not meet the Service Level, then HiveMQ will confirm the Credit Request and will issue the Service Credit to Customer within one billing cycle following the month in which Credit Request is confirmed. Customer’s failure to provide the request as required above will disqualify Customer from receiving a Service Credit.

Service Credits are exclusive of any applicable taxes charged to Customer or collected by HiveMQ.

Service Credits will be offset against the Subscription fees payable by the Customer which are subject to invoicing following HiveMQ's confirmation of the Credit Request. In case there is no further invoicing (e.g. due to termination or prepayment) within 6 (six) months after HiveMQ's confirmation of the Credit Request, the Service Credits will be refunded to the Customer upon Customer's request. In no event does HiveMQ's confirmation as stated above or the crediting or payment of Service Credits constitute or imply an admission or acknowledgement of the existence of any other or additional obligations on the part of HiveMQ towards the Customer or third parties, including obligations to pay damages.

The provisions regarding the granting of Service Credits shall not exclude the Customer from exercising his existing mandatory rights for compensation in accordance with the provisions of the SaaS Framework-Agreement - if any - in case the Service Level is not reached, provided however that the Customer bears the burden of proof for any damages and confirmed Service Credits must be offset against any claims for damages.

3.5 Events beyond HiveMQ's Control

The following events are beyond the reasonable control of HiveMQ and are not taken into account for determining the Service Level. They are therefore not included as Downtimes in the calculation of the Monthly Uptime Percentage.

a. Events in public cable networks, computer networks or the Internet that occur outside the sphere of influence of HiveMQ and temporarily or permanently impair or even exclude the use of the SaaS Services and for which HiveMQ is not responsible;
b. Events beyond the control of HiveMQ in which the availability of the servers of HiveMQ or its subcontractors is impaired or even excluded due to technical or other problems (including but not limited to force majeure, fault of third parties including DDoS attacks, network intrusions, denial of service attacks etc.) for which HiveMQ is not responsible, taking into account customary market standards;
c. Suspension of access to or provision of SaaS Services in exercise of HiveMQ's rights in accordance with the HiveMQ SaaS-Terms in the event of a breach of Customerobligations;
d. Events resulting from the use of services, hardware, or software provided by a third party and not within the control of HiveMQ, including issues resulting from inadequate bandwidth;
e. Events resulting from Customer's failure to use MQTT clients with acceptable implementation and configuration values as recommended by HiveMQ under https://www.hivemq.com/mqtt-client-library-encyclopedia/.
f. Events resulting from Customer's unlawful or contract-violating action or lack of action when required, including those of Customer's users or by means of Customer's passwords;
g. Unavailability due in whole or in part to any of the following: Failure by Customer to take any remedial action in relation to the SaaS Services as contractually agreed or reasonably required by HiveMQ, or otherwise preventing HiveMQ from doing so or Customer's failure to provide information reasonably and lawfully required by HiveMQ in order to provide SaaS Services.

Data Processing Agreement (DPA)

between

For Controllers with a billing address in the EMEA region HiveMQ GmbH, Postplatz 397, 84028 Landshut, Germany and for Controllers with a billing address outside the EMEA region HiveMQ Inc., 600 N Broad Street, Suite 5, 553 Middletown DE 19709, USA

– hereinafter referred to as the "**Processor**" or the "**Supplier**" -

and

Customer specified in the Quote

– hereinafter referred to as the "**Controller**" -

– the Controller and the Processor will be together referred to as the "**Parties**" -

Preamble

1. HiveMQ provides a SaaS solution in the field of data transmission and exchange between various devices over existing connections as set forth in the SaaS Terms.

2. Customer subscribes to the SaaS by submitting to the SaaS Terms with the applicable Quote.

3. HiveMQ will provide the SaaS and accompanying Support Services in accordance with the applicable SaaS Terms and Quote between the Parties within the course of which HiveMQ may process personal data on behalf of Customer as the data controller. The Parties intend to enter into this Data Processing Agreement (hereinafter referred to as "**DPA**").

4. HiveMQ shall be referred to as the "**Processor**" or "**Supplier**" and Customer as the "**Controller**".

Definitions

Within the scope of this DPA the following terms shall have the meaning as defined in this section:

- "GDPR" means the General Data Protection Regulation (Regulation (EU) 2016/679) of the European Parliament and of the Council of 27 April 2016, in force since 25 May 2018;
- "Controller", "Processor", "Personal Data", "Data Subject", "Processing", "Personal Data Breach" and "Supervisory Authority" shall have the same meaning as defined in Art. 4 GDPR;
- "Cloud Service" means an IT-infrastructure which is not in the possession of the Supplier, but is a third-party-service which the Supplier uses to store and/or process Personal Data of the Controller and for which the Supplier is in a contractual relationship with the Cloud Service provider;
- "EU" means the European Union;
- "EEA" means the European Economic Area.

I. Subject Matter and Duration

1. Subject Matter

The subject matter of the DPA results from the SaaS Terms entered between the Controller and the Processor as well as the applicable Quote (hereinafter referred to as "**Service Agreement**").

2. Duration

The duration of this DPA corresponds to the duration of the Quote and the SaaS Terms.

II. Specification of the DPA

1. Nature and Purpose of the intended Processing of Personal Data

The nature and purpose of Processing of Personal Data by the Supplier for the Controller are defined in the SaaS Terms and Quote between the Parties.

The undertaking of the contractually agreed Processing of Personal Data shall be carried out exclusively within a member state of the EU or within a member state of the EEA, unless Customer chooses a data location outside the EEA. In the latter case and for each and every transfer of Personal Data to a state which is not a member state of either the EU or the EEA the conditions of Article 44 et seq. GDPR must be met.

Each transfer of Personal Data to a third country requires Controller's prior written approval, as may be given in the respective Annex 1, and is only permissible if the requirements of Chapter V of the GDPR are complied with. In case Personal Data is to be processed in a third country (including remote access from a third country), Processor will adequately support Controller in particular, but not limited to the identification and implementation of adequate safety measures as well as providing relevant information including but not limited to all statements provided by Processor in course of Controller's questionnaire regarding international data transfers. In case Processor implements technical and/or organizational measures in order to comply with the requirements of Chapter V of the GDPR, Processor assures their effectiveness.

If Supplier is located in a third country, Supplier and Customer enter, with the conclusion of this DPA, also into the EU Standard Contractual Clauses, Module 2 (2021/914/EU) attached as **Appendix 2 – EU Standard Contractual Clauses** including Appendices I to III. Customer enters into the EU Standard Contractual Clauses as Data Exporter, Supplier as Data Importer.

With respect to the Appendices I to III the EU Standard Contractual Clauses the following shall apply:

- With respect to the information required according to the EU Standard Contractual Clauses, Appendix I A of the EU Standard Contractual Clauses including the information about the Parties, the information laid down in the Quote shall apply,
- With respect to the information required according to the EU Standard Contractual Clauses, Appendix I B of the EU Standard Contractual Clauses, the information laid down in the Quote shall apply,
- Competent supervisory authority within the meaning of the EU Standard Contractual Clauses, Appendix I C of the EU Standard Contractual Clauses shall be the competent supervisory authority in the country in which Customer has its headquarter,
- Appendix 1 shall apply as the EU Standard Contractual Clauses, Appendix II of the EU Standard Contractual Clauses,
- Approved subprocessors according to the Appendix III of the EU Standard Contractual Clauses are laid down in this DPA.

In the event of a conflict between the EU Standard Contractual Clauses according to Appendix 2 and this DPA, the EU Standard Contractual Clauses shall prevail.

2. Type of Personal Data

The Subject Matter of the Processing of Personal Data comprises the following data types/categories:

- Contact Data (email address and name of Controller's employee)
- Communication Data (Personal Data pushed through the SaaS by Controller)
- Traffic Data (means information necessarily incurred while initiation, maintenance or transaction of a communication process such as IP-address, device identifier, log-files)
- Other: IP addresses, Personal Data included by Controller into a support ticket, if any

Should the Supplier receive encrypted or pseudonymised Personal Data he ensures that Supplier's employees do not make any efforts to identify any individuals by using these encrypted or pseudonymised Personal Data.

3. Categories of Data Subjects

The categories of Data Subjects comprise: Controller's employees interacting with Processor's Support Services team any Data Subjects whose Personal Data is being included into messages send via the SaaS.

III. Technical and Organisational Measures (see Appendix 1)

1. Documentation

Before the commencement of Processing, the Supplier shall document the execution of the necessary Technical and Organisational Measures, set out in the Annex of this Contract (hereinafter referred to as "**Technical and Organisational Measures**"), specifically with regard to the detailed execution of the Contract, and shall present these documented measures to the Controller for inspection. Upon acceptance by the Controller, the documented measures become the foundation of the contract and will be specified in the Annex to this Agreement. Insofar as the inspection/audit by the Controller shows the need for amendments, such amendments shall be implemented by mutual agreement.

2. Data Security Measures

The Supplier shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1 and

Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems. The state of the art, implementation costs, the nature, scope and purposes of Processing as well as the probability of occurrence and the severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account (details in the Annex).

3. State of the Art

The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

IV. Rectification, restriction and erasure of data

1. Prohibition of unauthorized actions

The Supplier may not on its own authority rectify, erase or restrict the Processing of Personal Data that is being processed on behalf of the Controller, but only on documented instructions from the Controller.
Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of Processing, the Supplier will immediately forward the Data Subject's request to the Controller.

2. Data Subject's Rights

Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by the Supplier in accordance with documented instructions from the Controller without undue delay.

V. Quality assurance and other duties of the Supplier

In addition to complying with the rules set out in this Order or Contract, the Supplier shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, the Supplier ensures, in particular, compliance with the following requirements:

1. Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR. The Controller shall be informed of his/her contact details for the purpose of direct contact. The Controller shall be informed immediately of any change of Data Protection Officer.

2. Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the Processing of Personal Data outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to Personal Data, shall not process that data unless on instructions from the Controller, which includes the powers granted in this contract, unless required to do so by law.

3. Implementation of and compliance with all Technical and Organisational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR.

4. The Controller and the Supplier shall cooperate, on request, with the Supervisory Authority in performance of its tasks.

5. The Controller shall be informed immediately of any inspections and measures conducted by the Supervisory Authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the Processing of Personal Data in connection with the Processing of this Order or Contract.

6. Insofar as the Controller is subject to an inspection by the Supervisory Authority, an administrative or summary offence or criminal procedure, a liability claim by a Data Subject or by a third party or any other claim in connection with the Order or Contract Processing by the Supplier, the Supplier shall make every effort to support the Controller.

7. The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that Processing within his area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the Data Subject.

8. Verifiability of the Technical and Organisational Measures conducted by the Processor as part of the Controller’s supervisory powers referred to in Clause VII of this Contract.

VI. Subcontracting

1. Customer hereby generally consents to Supplier’s use of subcontractors. With the execution of this DPA, Supplier will use the following subcontractors:

Subcontractor	**Address**	**Service**
Amazon Web Services	410 Terry Avenue North, Seattle, WA	Hosting of the HiveMQ Platform.
Atlassian Pty Ltd	Level 6 341 George St, Sydney, NSW 2000, Australia	Provision of Jira Service Management
Microsoft Deutschland GmbH	Walter-Gropius-Straße 5, 80807 München	Hosting of the HiveMQ Platform.
Auth0	10800 NE 8th St #600, Bellevue, WA	Credential management for customer sign up.
Mixpanel	One Front Street, 28th floor, San Francisco, CA 94111	Tracking user interactions on our customer portal.
Refiner	Paris, Ile-de-France, France	Feedback collection for users.
HiveMQ, Inc. (where HiveMQ GmbH acts as Customer’s contracting party)	600 N Broad Street, Suite 5 # 553 Middletown DE 19709, USA	Support and IT services

HiveMQ GmbH (where HiveMQ, Inc. acts as Customer’s contracting party)	Postplatz 397, Postplatz 397, 84028 Landshut, Germany	Support and IT services

2. Supplier shall, prior to the replacement or change of subcontractors, inform Customer thereof in documented form. In the event that a replacement or change is needed due to urgent emergency or security reasons, Supplier may notify Customer after the change or replacement has been made. In any case, Customer shall be entitled to reasonably oppose to any change or replacement of subcontractors within fourteen (14) business days and for materially important reasons. Where Customer fails to oppose to such change within such period of time, Customer shall be deemed to have expressed its consent to such change or replacement. Where a materially important reason for such opposition exists and failing a bona fide resolution of this matter by the Parties, either Party shall be entitled to terminate the Agreement with immediate effect.

3. Where Supplier commissions subcontractors for the purpose of Contract Processing, Company shall contractually ensure that Company’s obligations on data protection resulting from this DPA are valid and binding upon subcontractor.

4. If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

VII. Supervisory powers of the Controller

1. Audits and Inspections

The Controller has the right, after consultation with the Supplier, to carry out audits and inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this agreement by the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.

2. Providing Evidence

At the choice of the Processor, customer’s right to conduct audits may also be complied with by submitting the evidence referred to in Section 3 instead of on-site inspections.

3. Proof of Compliance

The Supplier shall ensure that the Controller is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR**.** The Supplier undertakes to provide the Controller with the necessary information on a yearly basis (at the date of execution of this Order), in particular, to demonstrate the execution of the Technical and Organizational Measures.

3. Measures of Proof

Evidence of such measures, which concern not only the specific Order or Contract, may be provided by

a) Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;

b) Certification according to an approved certification procedure in accordance with Article 42 GDPR;

c) Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, Data Protection Officer, IT security department, data privacy auditor, quality auditor)

d) A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT Baseline Protection certification developed by the German Federal Office for Security in Information Technology (BSI)) or ISO/IEC 27001).

4. Remuneration

Supplier may claim remuneration for enabling Controller inspections.

VIII. Communication in the case of infringements by the Supplier

1. Duty to Assistance

The Supplier shall assist the Controller in complying with the obligations concerning the security of Personal Data, reporting requirements for Personal Data Breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:

a) Ensuring an appropriate level of protection through technical and organizational measures that take into account the circumstances and purposes of the Processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events.

b) The obligation to report a Personal Data Breach immediately to the Controller.

c) The duty to assist the Controller with regard to the Controller's obligation to provide information to the Data Subject concerned and to immediately provide the Controller with all relevant information in this regard.

d) Supporting the Controller with its data protection impact assessment.

e) Supporting the Controller with regard to prior consultation of the Supervisory Authority.

2. Compensation

The Supplier may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of the Supplier.

IX. Authority of the Controller to issue instructions

1. Form

The Controller will provide any instructions in documented form.

2. Notification

The Supplier shall inform the Controller immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Controller confirms or changes them.

X. Deletion and return of Personal Data

1. Copies and Duplicates

Copies or duplicates of the data shall never be created without the knowledge of the Controller, with the exception of back-up copies as far as they are necessary to ensure orderly Processing of Personal Data, as well as data required to meet regulatory requirements to retain data.

2. Destruction of Data

The Supplier has to immediately destroy all documents, Processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner once (i) the data is not needed anymore to fulfill the Supplier's obligations towards the Controller and/or (ii) the contract between the Controller and its customer ceases to exist and the Controller informs the Supplier respectively.

Any Personal Data, particularly when related to the customers of the Controller, has to be destroyed at the latest upon termination of the Service Agreement. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided.

3. Exception for Documentation Purposes

Documentation which is used to demonstrate orderly Processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention periods. It may hand such documentation over to the Controller at the end of the contract duration to relieve the Supplier of this contractual obligation.

XI. Liability

1. In the event that a breach of any obligation set forth in this DPA or under applicable law causes a third-party claim or leads to statutory fines or any other claims towards either Customer or Supplier, both are jointly liable following the principal of Art. 82 of the GDPR.

2. Supplier is solely liable towards Customer subject to the applicable liability provisions and limitations of the SaaS Terms, for damages caused within his sphere of responsibility and only in the event that he culpably

    a. did not comply with the specific statutory processing obligations set forth in the provisions of the GDPR applicable to data processors;

    b. processed Customer's Data or otherwise acted irrespective of and not in compliance with the legitimate instructions provided by Customer in regard to the Data;

    c. actively infringed Customer´s legitimate instructions; or

    d. is in breach of this DPA.

3. In the event that Customer is liable towards the Data Subject, Customer may recover any damages paid to such data subject only under the provision of Section XI.2.

XII. Governing law and jurisdiction

The governing law and jurisdiction shall follow from the SaaS Terms.

Appendix 1 - Technical and Organisational Measures

Global Technical and Organisational Measures (TOMs) and other applicable Information Security Measures, appendix to Data Processing Agreement (DPA)

Supplier ensures the implementation and adherence to the required technical and organizational measures in accordance with § 32 GDPR. This includes security measures to ensure the ongoing confidentiality, integrity, authenticity, availability and resilience of processing systems and services. It also includes the pseudonymization and encryption of personal data where such measures are necessary.

Supplier must have policies, procedures and documentation for periodic review, assessment and evaluation of the effectiveness of technical and organizational measures in place to ensure the security of processing.

1. **Information Security Management Systems**
    - Supplier must operate an information security management system (ISMS) that is based on recognized, marketable standards (e.g., ISO27001, BSI Grundschutz)
    - Supplier must prepare at least one comprehensive information security risk report per year and make it available to Controller.
    - This must contain at least the following information on security-relevant topics with regard to the provision of services:
        - The basic compliance with the contractually agreed security measures.
        - Identified information security risks (to be replaced, if necessary, by separate risk reporting)
        - Status and development of information security incidents
        - General overview of vulnerability scans carried out and their results
        - General overview of penetration tests carried out and their results
        - Results of security audits performed by the ISMS organization
        - Security awareness measures carried out
        - Relevant results of the internal audit and third-party auditors (e.g., auditors) with reference to the Supplier ISMS as well as security-relevant findings in connection with the performance of services under the contract.

- Supplier grants Controller the right to verify compliance with the contractually agreed information security specifications.

2. Risk Management

Supplier has to ensure that the following processes are in place related to risk management:

- An annual Information Security risk assessment must be performed covering Vendors facilities and information assets.
- The risk assessment must be conducted using an industry standard methodology to aid in identifying, measuring, and treating known risks.
- Risk assessment results and risk mitigation suggestions must be shared with the executive management team.
- The risk assessment results will specify proposed changes to systems, processes, policies, or tools, in order to reduce security vulnerabilities and threats, if any.

3. Protection requirement of information

Supplier has to ensure that the following processes are in place related to protection requirements of information:

- Procedures have to be in place on which information get classified in the context of the business processes in which it is used, processed or stored, as well as the applicable legal requirements with regard to its need for protection in terms of confidentiality, integrity and availability,
- A concept for the classification of documents must be defined. This concept must define risk-oriented specifications with regard to the unambiguous marking depending on the need for protection.
- Documented processes must be established which provide complete and up-to-date overviews of the company's protection objects in context with the information and processes as well as their links and interfaces (information domain) and the set of protection measure based on the protection requirements,
- In addition to its designation and description, each protection object must be assigned to a responsible person (e.g. process owner, operations manager) who is responsible for the maintenance of the protection object. The

maintenance of the protected object includes at least the implementation responsibility for the following tasks:

    - Inventory of the object
    - Classification of the protection need for the object
    - for applications and IT systems - if applicable - the recertification of authorisations; and
    - protection of the object in accordance with the security measure.

Supplier shall where appropriate or specifically instructed, use measures such as pseudonymisation and encryption, for the protection of personal data.

Pseudonymisation is considered effective where:

- personally identifiable information fields within a data record are replaced by artificial identifiers or separated from the rest of the data record, such that a third party cannot attribute the data record to a specific data subject, or the information of data subjects are extracted in groups and as part of a summary, such a third party cannot individualise (or ascribe specific identity to) any member of that group;
- the additional information that can lead to re-identification of a data subject, or the algorithm or repository that enables re-identification, is held exclusively by the Supplier;
- disclosure or unauthorised use of that additional information is prevented by appropriate technical and organisational safeguard; and
- the Supplier has established by means of a thorough analysis of the data in question taking into account any information that the public authorities of the recipient country may possess, that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information.

Encryption is considered effective where:

- the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis, active or passive attacks performed by third parties (including the public authorities) taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to the said third parties;

- the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved;
- the encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification; and
- the encryption keys are reliably managed and retained solely under the control of either the Controller or the entity to whom the Controller is transmitting data.

4. Security Policies and Procedures

Supplier has to ensure that the following processes are in place related to security policies and procedure:

- Policies, including those related to data privacy, security and acceptable use, are assessed and approved by Controller senior management. Policies are documented and published among all relevant personnel.
- Employees and contracted third parties are required to comply with Supplier policies relevant to their scope of work.
- New employees attend new hire training, which includes training modules on confidentiality obligations, information security, compliance, and data protection.
- Employees attend annual Information Security training, which covers Supplier Information Security policies and expectations.
- Where required, policies are supported by associated procedures, standards, and guidelines.
- Information Security policies are updated, as needed, to reflect changes to business objectives or risk.
- Senior management performs an annual review of all Information Security policies.
- Information Security policies are stored, maintained, updated, and published in a centralized location accessible to employees and third parties.
- Supplier employee handbook contains sections on password requirements, Internet usage, computer security, confidentiality, social media, customer data protection, and company data protection.
- Adoption of adequate internal policies with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for

cases of covert or official requests from public authorities to access the data. Especially in case of transfers among groups of enterprises, these policies may include, among others, the appointment of a specific team, which should be based within the European Economic Area (EEA), composed by experts on IT, data protection and privacy laws, to deal with requests that involve personal data transferred from the EEA; the notification to HIVEMQ upon receipt of such requests; the procedural steps to challenge disproportionate or unlawful requests and the provision of transparent information to data subjects.

5. Asset Management

- Supplier assigns ownership for all information assets.
- A process has to be in place which collects and documents all information assets as well as the links or interaction between the assets. The ongoing actualization of the assets and their attributes has to be established.
- Desktops and laptops utilize encrypted storage partitions whenever an employee is in a role involving access to Customer Content or Contentful intellectual property.
- For the systems and applications used, including web access, IT architecture and infrastructure as well as network infrastructure, at least the following documentation must be available:
    - Technical system and operational documentation
    - Technical user manual
    - Documentation of safety measures; and
    - User access rights concept

6. Physical access control (*Zutrittskontrolle*)

Supplier has to ensure that the following security measures have been implemented to prevent unauthorized persons from accessing data processing locations within which personal data is processed or used:

- Access to locations that house servers or end user terminals must only be granted to authorized personnel and that access must be documented,

- Personnel who are no longer authorized, must have their access revoked immediately,
- Authorization must be granted on a need-to basis, which must only be required for maintenance of equipment and emergency response purposes,
- Access to locations that house servers must require at least two-factor authentication,
- Access to locations with end user terminals must be protected with appropriate locked doors or access controls,
- An audit trail of access to locations that house servers must be kept and inspected at least quarterly for suspicious actions,
- Procedures for decommissioning hardware and data must be implemented, and
- Server locations must be protected using access control systems, intrusion detection systems, security alarms, and 24/7 monitoring with cameras and/or security personnel.

7. Media control (*Datenträgerkontrolle*)

Supplier has to ensure that the following measures have been implemented to prevent unauthorized reading, copying, modifying or deleting of data media:

- Media must be encrypted, and
- Media must be kept in locations with adequate physical access controls.

8. Storage control (*Speichercontroller*)

Supplier has to ensure that the following measures have been implemented to prevent unauthorized entry of personal data as well as the unauthorized reading, modification and deletion of stored personal data:

- All access to the customers services or data must be protected using Identity Management Systems (IMS) that complies with an access management policy which defines the access granting, revocation, modification and the revision and recertification process,
- The IMS must enforce the requirement from access management policy
- All services with remote access capabilities that grant access to customer data and company business data or are otherwise critical must be protected and a two-factor authentication method must be used, and

- All IT access rights and authorisations for users of the IT-systems and networks must be reviewed and re-certified at least annually; for privileged access rights, a recertification process must be performed at least biannually.

9. User control (*Benutzerkontrolle*)

Supplier has to ensure that the following measures have been implemented for the prevention of the use of automated processing systems by means of data communication equipment by unauthorized users:

- All privileged access to services, such as administrator access, with remote access capabilities require two-factor authentication. Administrative work on any system component must be done securely and must be auditable,
- Unsuccessful access attempts must be evaluated regularly,
- All servers must have proper security configurations and must be tested continuously for vulnerabilities and all found vulnerabilities must be dealt with promptly and accordingly alongside with a documented procedure,
- The network, workstations and the live infrastructure must be protected with an endpoint protection/antivirus solution and from unauthorized changes,
- All IT services must require a username and password that complies with a Password Policy,
- A Password Policy must be in place with the following requirements:
    - Passwords must not be shared with anyone. All passwords are to be treated as sensitive and confidential information,
    - Default passwords must be changed immediately for all IT systems and hardware components,
    - All user-level passwords must be changed at least every six months. For critical access, the password must be changed at least every quarter,
    - Passwords must contain upper and lowercase letters, special characters and numbers. The minimum length is 12 characters,
    - The number of permitted unsuccessful login attempts must be configured as per best practice (e.g. 6 attempts),
    - User sessions must be configured to be terminated or locked, or users must need to be re-authenticated, after 15 minutes of inactivity (if the operating system does not enforce this), and

    - It is forbidden to work under domain administrator credentials during daily operations (reading emails, browsing the Internet, etc.).
- A Workplace and Clean Desk Policy must be in place with the following requirements:
    - Workplace Access security controls in order to minimize the risk of unauthorized access to physical and logical systems,
    - Security of IT equipment, and
    - Clean desk policy that covers protection of non-digital information.

10. Data access control (*Zugriffskontrolle*)

Supplier has to ensure that the persons entitled to use a data processing system from customer can only access exclusively for the data covered by their access authorization:

- User access permissions to systems and data must be requested, modified or revoked on a predefined workflow, including the formal approval/sign-off or (a formal/digital approval) by the superior and granting of access rights,
- The process for user access administration must be documented, and the administration process itself must have an audit trail,
- Each user account must be given exclusively to a specific user, group accounts are not permitted,
- The use of depersonalized administrative accounts must be forbidden; in case of exceptions (i.e. admin accounts for emergency situations), passwords for such accounts must consist of two parts and must be created and entered by two different employees. Neither of them must know the full password.
- Each permission within an IT system must be tied to groups or roles, not to individual users,
- All users must be assigned to specific groups,
- Access to customers resources must only be granted if the individual requiring or requesting access is authorized to have access to that resource,
- In general, access to resources must follow this process:
    - is requested by the requester,
    - is approved by the IT manager,
    - is granted by the service owner,
    - is granted only in accordance with the IT Permissions Concept,
    - is granted only once the identity of the user has been confirmed by authoritative bodies,
    - is only granted on a need-to-know basis,

    - is always tied to a unique user account, and
    - must be revoked when the user is no longer authorized to access a resource.
- A process must be implemented in which the granted access rights get reviewed on a regular basis (recertification). Critical access rights have to be evaluated at least every six month.
- When granting access rights separation of duties must be taken into account in accordance with legal and regulatory as well as internal requirements.
- For each application, a user access rights concept must be available and has to be reviewed on a regular basis.
- User access should be based on a strict need-to-know principle, monitored with regular audits and enforced through disciplinary measures. Data minimisation should be practiced in order to limit the exposure of personal data to unauthorised access. In cases where it might not be necessary to grant access to an entire database, restricted access must be granted instead of full access.
- Supplier must document and record the requests for access received from public authorities and the response provided, alongside the legal reasoning and the actors involved. These records should be made available to the HIVEMQ, who can in turn provide them to the data subjects concerned.

11. Data transfer control (*Weitergabekontrolle*)

Supplier has to ensure that personal data can be checked and ascertained where a transmission of personal data is intended and to which involved parties personal data was provided or transmitted:

- All personnel is responsible to ensure that data is only communicated when:
    - it is done using pre-defined communication technologies,
    - there is a clear lawful or business purpose,
    - the employee signed a Non Disclosure Agreement (NDA) accepting responsibility for the Data Protection and is compliant with existing Non-Disclosure-Agreements (NDA),
    - the recipient is authorized to receive the data, and
    - it does not violate the security principles explained in a security training.
- IT personnel is allowed to communicate with servers or application directly when:

    - the connection is secured using strong encryption protocols, and
    - the authenticity of the server or application is verified.
- In case data will be transferred to a recipient in a third country, the Supplier must ensure that the data is afforded an appropriate level of protection in that country, and also ensure that the transferred data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred to and processed in that third country.
- Data transfer for the purpose of backup, or other purpose that does not require access to data in the clear, shall be secured using encryption.
- All encryption should have keys kept beyond the reach of unauthorised parties (including public authorities). The encryption protocols employed shall be state-of-the-art and provide effective protection against active and passive attacks that may happen at the countries of origin, transit and destination.
- All employees must sign NDAs or any other terms and conditions that cover acknowledging that customer will monitor communication done through company hardware or software,
- Communication of data to non-customers employees or companies is only allowed if that party can guarantee the security of the sent data,
- IT infrastructure must be protected against unauthorized electronic transmission by using firewalls, host-based firewalls, IP white lists, and the like must be employed where practical as an additional layer of defense.
- IT infrastructure must be protected by deactivating not required ports and transport protocols.
- To ensure appropriate and secure operations and a standard security level in the network environments, the following requirements must be fulfilled:
    - Roles and responsibilities for the operating network- and network security management are to be defined,
    - Monitoring and control of network management must be implemented, taking account of the security requirements in respect to separation of function,
    - On the basis of best practices and manufacturer recommendations, internal requirements (technical standards) for establishing network infrastructures and network services have to be specified. On this basis, the network infrastructures and network services are configured, documented and operated,
    - There must be appropriate monitoring of availability, transmission times and the level of resource utilisation, and
    - It is necessary to document an operating concept.

- The network traffic has to get logged on a risk-oriented basis. Traffic between protected networks and public networks must be logged centrally. The logs have to get reviewed on a regular basis. Events have to be managed based on a defined procedure.

12. Data entry control (*Eingabekontrolle*)

Supplier has to ensure that the following measures have been implemented to ensure that it can be subsequently verified and ascertained whether and by whom personal data has been entered, changed or removed in data processing systems:

- Data processing systems can only be used after strong identification and authorisation controls for the user,
- A backup and retention policy and procedure exists defining the steps and the process or data backup and secure storage over the retention time,
- All access to data must be logged:
    - For every login/logout attempt as well as the start and termination of each session, the following must be logged: a timestamp of the event, which userID or username was used, sessionID (if applicable), from which IP the attempt was made, and the result of the action,
    - When data is viewed, the following must be logged: a timestamp of the event, a sessionID, username or userID, and the type of data that is viewed, and
    - When data is changed, the following must be logged: a timestamp of the event, the type/field of data that was changed, the old and new value, sessionID (if applicable), username or userID.
- All logged data must be stored on secure servers, access to these servers must be protected by an Identity Management System (IMS), and
- Access logs must be reviewed regularly, at least every quarter, suspictions actions must be addressed immediately.

13. Transport control (*Transportkontrolle*)

Supplier has to ensure that during the transmission of personal data and during transport of storage media, the confidentiality and integrity of data is protected:

- Policies and procedures must be in place to ensure that:

    - data sent over public networks is encrypted using strong encryption protocols, valid and correct certificates and be tested at least quarterly,
    - all authentication data is encrypted, and
    - all personnel and partners are made aware of their responsibilities.
- Communicating data in physical form (including USB sticks, printouts, CDs, etc.) must be only used when there is no digital transport way and only be done using signed mail, personal handover or secure transport methods, if USB sticks are used then they must be encrypted and a proper handover process must be inplace.

14. Recoverability (*Wiederherstellbarkeit*)

Supplier has to ensure that the systems used can be recovered in case of failure:

- Regular creation of backup copies,
- A backup and retention policy and procedure exists defining the process for data backup and secure storage over the retention time,
- Procedures to store the backups in a secure location outside the original data processing location, and
- Requirement to test data backups at least annually.

15. Reliability (*Zuverlässigkeit*)

Supplier has to ensure that all functionalities of the system are operational and that incidents in the functions are reported:

- Procedures for Incident and Problem Management,
- Procedures include an evaluation of the Incident or Problem as well as escalation procedures and a call tree,
- Procedures for Security Incident Event Management (SIEM), in case of security breaches, information loss or unauthorized disclosure, and other disasters do occur,
- Standardised Change and Patch Management and testing procedures in order to ensure uninterrupted service delivery. The procedure has to make sure that changes get classified based on their risk and criticality and specific approvals are in place,

- Release and Deployments have to follow a defined workflow. This has to make sure that all relevant approval from the software development and/or change management are provided before deployment, and
- Procedures for the development of systems and applications (software) must be defined and documented in a risk-oriented manner. Responsibilities must be clearly defined in terms of requirements, development, testing, acceptance and release, and communication. This includes the approval of the requirements by the department responsible as well as the user acceptance tests.

16. **Integrity (*Datenintegrität*)**

Supplier has to ensure that stored personal data must not be corrupted due to system malfunctions by:

- Redundant infrastructure of the data center with a fail-over data center, or
- Using database management techniques that allow the recovery of data in case of system malfunctions.

17. **Control of processing instructions (*Auftragskontrolle*)**

Supplier has to ensure that the following measures have been implemented to ensure that personal data can only be processed according to the instructions of the customer:

- Regulation of all assignments for processing personal data in written contracts,
- Regulation of the basic requirements for liability, assigning of competences, safety requirements and measures, as well as control rights,
- Contracting authorities are assisted in the exercise of the control rights by the data protection officer of the customer in which the latter acts to ensure compliance with the data protection regulations for the order data processing and data protection of the applications, and
- Verification of compliance with the contractual obligations.

18. **Availability control (*Verfügbarkeitskontrolle*)**

Supplier has to ensure that the following measures have been implemented to ensure that personal data are protected against accidental destruction or loss:

- Rules for the business continuity and disaster recovery based on a Business Impact Analysis (BIA)
- The BIA must include at a minimum the following:
    - Definition of a scope and identification of the assets that are within scope,
    - Identification of the processes, IT assets, data and control flows and their status, as either existing or planned,
    - Identification of the threats, the type of threats represented and their sources,
    - Assessment of the impact that losses of confidentiality, integrity, authenticity and availability may produce, and
    - derived protection measures for these impacts.
- Data processing center must have appropriate environmental controls, including:
    - Automatic fire detection mechanisms,
    - Protection measures against water damage,
    - Uninterruptible Power Supply (UPS) units or an alternative power supply, and
    - Climate, temperature, humidity and vibration control mechanisms.

19. **Separation control (*Trennungskontrolle*)**

Supplier has to ensure that the following measures have been implemented to ensure that data collected for different purposes can be processed separately:

- Segregated IT processing environments (logically or physically) for multi-client service CUSTOMERs,
- Access to data processing systems only after strong identification and authorisation of the personal of Supplier,
- Standardised testing procedures with separated IT environments for development, test and production,
- Standardised testing procedures for performing functional and nonfunctional tests, and
- Standardised sign-off and error management procedures.

20. **Deletion and return of customer data**

Supplier has to ensure that the following measures have been implemented to ensure that data is deleted or returned in a data-protection compliant manner:

- Copies or duplicates of the data must never be created without the knowledge of HIVEMQ, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data, and
- After conclusion of the contracted work, or earlier upon HIVEMQ request, at the latest upon termination of the Service Agreement, the Supplier must hand over to HIVEMQ or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected tests, waste, redundant and discarded material. The log or certification of the destruction or deletion must be provided on request.

21. Information Security Incident Management

- Supplier must maintain an incident response process that includes direct participation and cooperation between support, security, and operations teams.
- The Supplier incident response process includes notification, escalation, and reporting
- Supplier Must notify and report to HIVEMQ security incidents that are related to the scope of the contract.
- Internally, Supplier must maintain an incident response plan that is tested on a yearly basis. The plan addresses specific incident response procedures, roles and responsibilities, customer communication, contact strategies, and legal and shareholder information flow. The Supplier must escalate, notify and report the incidents to security@HiveMQ.com
- The Supplier must test the incident response plan on a regular basis, at least annually and the results must be shared with HIVEMQ.
- Supplier maintains relationships with law enforcement to assist during incidents with criminal intent.
- Customer must assist with providing evidence, audit trails, and support, for the requests in investigation by authorities.
- Supplier has relationships with third-party vendors to assist with forensics and investigations, as necessary.

- Supplier must monitor the logs of the activities related to the service as per the scope of the contract through SIEM (Security information and event management) and alert HIVEMQ of anomalies.

22. **Personal security**
   - Employees and service providers must be obliged to comply with the written guidelines and regulations,
   - Employees must be informed that disciplinary or criminal proceedings may be initiated in the event of intentional or (gross) negligent acts. This information must be documented,
   - Employees and service providers who are given access to non-public information must sign a confidentiality agreement, taking into account the requirements of confidentiality or non-disclosure agreements, before they are given access to information processing facilities.
   - Employees and service providers are to be trained according to the respective needs in order to:
     - know and observe the information security requirements,
     - identify information security problems and incidents; and
     - be able to react in accordance with the requirements of their field of activity.

Applicable if the Work from Home option is used

WFH Workplace Security Requirements and Guidelines

- Work location must be limited to the home lived in and cannot be another location.
- Any change must be pre-approved by vendors Management and/or Human Resources
- Workspace must be an isolated area (private room) with all doors closed to ensure physical, visual, and audible segregation from any other areas in the building.
- All device screens used for work must be pointed away from windows.
- Non-employee access to the workspace during work hours must not be permitted. This includes any outside entities, family members, or others who live in the household.
- Access to the HIVEMQ virtualization environment will be exclusively established via a secure system set up by the HIVEMQ (e.g. VPN etc.). Any

other access is only permitted with the express permission of HIVEMQ in writing (letter), by fax or by e-mail.

- Any of the customer's Personal Identifiable Information (PII) (for example: - email, name, credit card, account numbers etc.) cannot be written or electronic storage in users' working devices.
- No unattended company, customer or HIVEMQ confidential material can be left on the workstation (this includes visible on-screen) or in the workspace area.
- Workstation must be logged out of or locked any time the employee is away from the system and not performing any work-related activity.
- Portable Media devices (CD, audio-visual devices, DVD, tapes, drives, external storage, memory sticks, USB etc.) should not be connected to the workstation or assets.
- Printing of any corporate or HIVEMQ materials is strictly prohibited.
- Use of unapproved or unlicensed software while performing the daily operations is strictly prohibited.
- Forwarding business mails containing sensitive data to private mail addresses is strictly prohibited.
- Employees must not write down their user id and password under any circumstance.
- Employees must not delete, alter or make any physical or logical alteration to either Supplier-owned or HIVEMQ systems.
- Supplier-owned or HIVEMQ systems are for authorized company purposes only.
- No photo activity is allowed in the workplace during working hours by any employee or non-employee (visitor, family member, etc.).

In order to allow an employee to work from home, the Supplier must secure the following "Requirements for the Home Office workplace" are agreed and signed by every single employee before starting home office:

- Measures to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control)
    - The Supplier will obligate its employees via organizational work instructions ("work instructions") in order to ensure that only persons authorised to carry out the processing are present on the premises of the processing operation during the processing operation. The

premises shall be secured by appropriate measures such as closed doors in such a way that unauthorised access to the data is prevented.

- Measures to prevent data processing systems from being used without authorization (access control)
    - Access to the HIVEMQ virtualization environment ("target data processing systems") will be exclusively established via a secure system set up by the HIVEMQ (e.g. VPN etc.). Any other access is only permitted with the express permission of the HIVEMQ in writing (letter), by fax or by e-mail.
    - The registration to the target data processing systems at the beginning of the data processing is carried out according to the instructions of the HIVEMQ with a username and password and, if applicable, a second factor for the authentication (e.g. hardware token etc.).
    - After data processing, an adequate logout from the target data processing systems is carried out.
    - User IDs and passwords for access to the target data processing systems are stored carefully and separately from each other. Passwords are kept secret. If there is reason to believe that unauthorized third parties have obtained knowledge of a password, the password must be changed immediately or a change must be initiated immediately.
    - The following minimum requirements are observed when assigning passwords: It is a personal password with system-specific specifications. The password will not be passed on to third parties.
    - Pursuant to a work instruction, the employee's Personal Computer ("workstation") will be secured by the employee with a password protected screensaver in case of absence.

- Measures to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control)
    - Only persons authorized to process data are granted access to the HIVEMQ data.
    - Pursuant to a work instruction, the employee is prohibited from using the internet and/or e-mail for private reasons during the data processing.

- Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control)
    - The Supplier employees will be obligated via a work instruction not to process the HIVEMQ data outside of the target data processing systems. Deviations from this regulation require the express permission of the HIVEMQ in writing (letter), by fax or by e-mail

- Measures to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control)
    - Since the target data processing systems will be made available by the HIVEMQ, ensuring the verifiability of data processing operations (e.g. access authorization, rules regarding creation and deletion of protocol data, etc.) is the HIVEMQ responsibility.

- Measures to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control)
    - The Supplier ensures with adequate work instructions that data security regulations are complied with and that violations or a suspicion of a violation are reported and treated accordingly without undue delay.
    - Obligation of the Supplier employees to confidentiality.

Appendix 2 – EU Standard Contractual Clauses

Disclaimer: This document was generated based on the text available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc12-L_2021199EN.01003701-E0012 and is provided for convenience purposes. It should not be considered an authoritative text or legal guidance.

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

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) ([1]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) 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 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 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, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the 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. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. 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 return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 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 data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties 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 subjects. 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. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) 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 breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 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 and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([2]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer 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 Regulation of (EU) 2016/679 with respect to the processing in question;

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

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a). GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 14 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([3]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

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.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([4]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(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) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) 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 and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(e) 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.

(f) The Parties agree that if one Party is held liable under paragraph (e), 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.

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

Clause 13
Supervision

(a) [Where the data exporter is established in an EU Member State:] 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.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, 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 ([5]);

(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 the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of the Federal Republic of Germany.

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 the Federal Republic of Germany.

(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

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: ____

Address: ____

Contact person's name, position and contact details: _________________________

____

Activities relevant to the data transferred under these Clauses:

____

____

Signature and date: ____

Role (controller/processor):

2. …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: ____

Address: ____

Contact person's name, position and contact details: _________________________

____

Activities relevant to the data transferred under these Clauses:

____

____

Signature and date: ___________________________________

Role (controller/processor):

2. …

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

…

Categories of personal data transferred

…

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

…

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

…

Nature of the processing

…

Purpose(s) of the data transfer and further processing

…

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

…

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

…

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

…

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

…

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: …

   Address: …

   Contact person's name, position and contact details: …

   Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): …

2. …

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has

been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[4] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.