HOSTPOINT

General Terms and Conditions
Managed Flex Server

These General Terms and Conditions (GTC) shall apply to all services offered by Hostpoint AG (hereafter "Hostpoint"). By using our services you accept the following terms and conditions completely without any alteration.

1. Scope of application and conclusion of contract

1.1 These GTC cover the use of services and products which Hostpoint provides or offers to its Customers (hereafter "Customer").

1.2 Consent to these GTC is given by using the corresponding services and products. The Customer may when requesting individual services be requested to reiterate his consent to the GTC by activating a corresponding check box. When delivering a contract or a customized quote relating to Hostpoint services and products, Hostpoint shall provide these GTC to the Customer together with the contractual documents in writing by mail or by e-mail. The Customer shall in this case confirm his consent to the GTC by signing and returning the quote or the contract, or by using the service or paying the invoice. The GTC shall form an integral part of the contract with the Customer.

2. Services and rights of Hostpoint

2.1 General

Hostpoint provides both free and chargeable services. The Customer shall select the services to be provided by Hostpoint from the range of services available at the time of use. The conditions published on the websites of Hostpoint or in the Hostpoint Control Panel, or the conditions of the customized quote as the case may be, shall apply to all services. Hostpoint may at any time change the range of services and limit individual services and/ or cease providing them.

2.2 Hosting services

2.2.1 As part of hosting services, Hostpoint shall provide the Customer to the extent selected by the latter with storage space and server services on an infrastructure connected to the internet.

2.2.2 The calculation of services is based on average usage of Hostpoint resources. The resources provided for Flex Server Hosting (particularly storage, traffic, vCPU/RAM use) must only be used for the purposes of the Customer's normal operations. Storage space for e-mail or other data files will be provided to the Customer for the intended use. Subletting storage space is not permitted unless otherwise agreed in writing with the Customer. This service offer is designed for use by individuals and small or medium-sized companies. Hostpoint may at any time set thresholds or other usage restrictions – in particular with respect to the monthly volume of uploaded data, the permitted size and type of uploaded files or the permitted number of stored e-mail boxes (Fair Use Policy). Individual offers may be made on request for institutions (e.g. schools or universities) and larger companies requiring storage for a quantity of e-mail boxes that exceeds the normal requirements of individuals and small or medium-sized companies.

2.2.3 With respect to resource-intensive use of the Customer website by the Customer or by users of the Customer website (e.g. up/ download of sound that goes beyond ordinary operations, video, streaming, games, high resolution images and graphics, high number of simultaneous accesses to the website, excessive storage of data files, in particular, caching files, on the server, excessive hard drive access (read and/or write), etc.), Hostpoint is also permitted to set thresholds for individual Customers or Customer groups at any time and in its absolute discretion for the resource consumption or other usage restrictions (Fair Use Policy) and to limit the provision of the service for the Customer accordingly.

2.2.4 Hostpoint also reserves the right to block the user account of the Customer if the latter's user behavior or the user behavior of the users of the Customer website (e.g. a high number of simultaneous access attempts through DDoS attacks) in any way adversely affects the way the service or the Customer website operates. Hostpoint shall inform the Customer (if possible within the scope of its operating resources and with respect to the concrete circumstances) in advance or immediately after the blocking.

2.2.5 Hostpoint shall endeavor within the limits of its operational resources to offer the services continuously round the clock without any interruptions. Maintenance work, rectification of problems, expansion of services, measures to protect Hostpoint's infrastructure, etc. may make temporary operating interruptions necessary. The Customer shall be informed early on of such operating interruptions if this is possible in the circumstances.

2.3 Domain name services

Hostpoint offers Customers services for the management, registration and/or transfer of domain names. By utilizing the domain name services the Customer accepts the General Terms and Conditions for Domain Names in addition to these GTC.

2.4 Applications and additional services of Hostpoint and third-party providers

2.4.1 Hostpoint offers the Customer via the Hostpoint Control Panel applications (such as TYPO3, Joomla!, WordPress) and other additional services (e.g. SSL certificates) of Hostpoint or third-party providers. By using the application or the additional service, the Customer additionally accepts the licensing terms, terms of business, terms and conditions of use and/or the conditions of Hostpoint or the respective third-party provider, as described on the respective offer page or in the Hostpoint Control Panel, that apply to the corresponding applications or additional services.

2.4.2 Hostpoint may at any time and without prior notice limit the use of applications or other additional services and/or remove individual applications or additional services from the range that is offered. The Customer also acknowledges that with regard to the applications there is no entitlement of any kind to receive support services from Hostpoint and that he bears sole responsibility for backing up his data in connection with the use of the applications (see Cl. 4.1).

3. Rights and obligations of the Customer

3.1 General

3.1.1 The Customer is authorized to make the intended legal use of the services and products and undertakes to comply with these GTC and any instructions of Hostpoint, in particular with regard to maintenance, updating or deletion of software.

3.1.2 When ordering and registering and in the context of using the services, the Customer is obligated to provide truthful and verifiable information. Hostpoint may at any time and without providing reasons request that the Customer subsequently provides documents or information which enable Hostpoint to verify the accuracy of the information provided by the Customer. Hostpoint is entitled to defer the acceptance of an order or registration, to suspend services or to terminate the contract with the Customer with immediate effect in the event that the Customer fails to provide the requested documents or information within the deadline set by Hostpoint.

3.1.3 The Customer undertakes to select passwords appropriately, keep them carefully and protect them from access by third parties. The Customer bears full and sole responsibility for the use of the passwords. If the Customer finds that his account is being misused, he must inform Hostpoint immediately in writing (by e-mail with subsequent acknowledgement of receipt by Hostpoint).

3.1.4 The Customer is not authorized to provide a service (for free or chargeable) purchased by him to third parties. If Hostpoint finds that the services purchased by the Customer are not being used by the latter but by a third-party, Hostpoint shall be authorized to suspend provision of the relevant service until this defect is remedied. The Customer shall in such a case remain obligated to make payment in full of the fee due for this service.

3.1.5 The Customer undertakes to keep the applications and software used by him (both in respect of the server and the client) up to the latest technical standard, maintain them regularly and conduct regular updates. The Customer also undertakes to delete applications and software which he no longer needs and uses from the server.

3.1.6 The Customer is obligated to notify Hostpoint immediately of any disruptions and interruptions in the services requested by him and where possible assist Hostpoint in remedying the disruption. The Customer shall bear the costs of Hostpoint isolating and remedying disruptions if the Customer has called for the investigation and the cause of the disruption is attributable to the behavior of the Customer or the equipment used by him or to the behavior of the users of the Customer website.

3.2 The Customer's responsibility for content

3.2.1 The Customer is responsible for the content of the information (language, images, sounds, computer programs, databases, audio/video files etc.) which he himself and third parties communicating with him through Hostpoint arrange to be transmitted or processed, disseminate or keep available for retrieval. The Customer is also responsible for references (in particular, links) to such information. Hostpoint is not obligated to monitor the contents made accessible by the Customer.

3.2.2 The Customer is obligated while using the products and services of Hostpoint to make only permitted contents accessible. The following contents are prohibited: contents which infringe or jeopardize rights of Hostpoint or third parties, in particular intellectual property rights in the wider sense (for example, copyrights or trademarks) or personal rights, provisions of the Unfair Competition Act (UWG), including the contact data obligation of the Customer pursuant to Art. 3 (1) lit. s UWG, or the commercial repute; all contents which constitute a criminal acts (namely in the areas of pornography, depictions of violence, racism, business secrets, libel and fraud) are also prohibited (hereafter jointly referred to as "Prohibited Contents"). When using hosting services, the Customer further undertakes to comply with the Usage Guidelines for Hosting Services.

3.2.3 Hostpoint reserves the right to inspect contents made accessible by the Customer by means of using the hosting services upon receipt of a Notice pursuant to the Code of Conduct – Hosting (hereinafter "CCH") or at the request of courts or authorities. Hostpoint remains entitled to conduct random checks even without having been served with a Notice.

3.2.4 Any disputes between joint holders of an account or the Customer and third parties relating to the use of the account or the information disseminated via the relevant account or via the Customer website are exclusively a matter for the joint holders of the account or the Customer. If Hostpoint receives queries/complaints from individual joint holders of accounts or from third parties in relation to an account or in relation to contents provided via an account or via the Customer website, Hostpoint shall pass the query/complaint to the other joint holder(s) or the Customer to deal with. Hostpoint still has the right to inform third parties of the identity of the Customer at the request of courts or authorities (see Cl. 9.2).

3.2.5 Queries/complaints received from third parties are passed to the Customer in accordance with the notice-and-notice procedure described in the CCH (hereinafter "Notice-and-Notice Procedure"). The Customer shall familiarize himself with the Notice-and-Notice Procedure and with the notice-and-takedown procedure pursuant to the CCH (hereinafter "Notice-and-Takedown Procedure").

3.2.6 Hostpoint is entitled to block access to the Customer website entirely or partly and to cease providing the hosting services if, (i) the requirements of the Notice-and-Takedown Procedure have been fulfilled, (ii) a court or authority has requested Hostpoint to do so, or (iii) Hostpoint could otherwise become subject to civil responsibility or liable for criminal sanctions, or (iv) if a random check has given rise to concrete indication or well-founded suspicion of a breach of the Usage Guidelines or that access is being allowed to Prohibited Contents (see Cl. 3.2.2). Hostpoint also reserves the right to reject and delete e-mails that have viruses and to block Prohibited Contents.

3.2.7 Hostpoint is entitled to invoice the Customer for the expense arising in connection with any measures taken pursuant to Cl. 3.2.3–3.2.6. The assertion of further damages remains reserved. Hostpoint is entitled to require the Customer to provide a security deposit as a precautionary measure to ensure coverage of the expenses and the further damages are covered. Hostpoint is entitled to suspend the services or to terminate the contract without giving notice if the security deposit is not provided or if the Customer does not comply with the instructions given in connection with the measures taken.

HOSTPOINT

4. Data backup

4.1 The Customer bears sole responsibility for taking the appropriate and necessary security measures to recover information and data in the event of loss or unauthorized or unintentional alteration. The security measures the Customer must take depend on the level of protection needed as well as the likelihood and severity of the risk. Hostpoint recommends as a rule that Customers back up their data regularly. The Customer can download its web data and databases through the Control Panel or from links generated by Hostpoint in order to, for example, create its own back up. To back up e-mail data, Hostpoint recommends using a mail client.

4.2 In the case of hosting services (see Cl. 2.2), Hostpoint also offers different protection packages for the protection of databases, files and e-mails of the Customer. The frequency of backups and storage duration of the backup copies made by Hostpoint depend on the data package selected by the Customer (e.g. Flex S or Flex L). The packages currently available, the range of services included in the service package, prices and other conditions of service are described on the Hostpoint website.

4.3 The service packages referred to in Cl. 4.2 are supplementary to the security measures taken by the Customer, in particular the Customer's own backup copies (see Cl. 4.1). Hostpoint assumes no warranty of any kind for the backup of the data stored on its server and points out to its Customers that, depending on the type of data and the chosen data package, the data is backed up at different times and at different intervals. It can therefore not be ruled out that a data loss might occur in a specific case. In exceptional cases it is also possible that due to technical reasons, for instance, due to maintenance work, disruptions in the system or necessary replacement of parts in the server infrastructure, Hostpoint will be unable to perform data backups or restorations for a few hours or on certain days. The obligation to restore lost data does not in any case apply to volatile data such as, for example, temporary data files as well as e-mails that are filed by the spam filter in the special box for spam mail. This box is not backed up, but is deleted on a regular basis.

5. Invoicing and payment terms

5.1 The payment obligation for chargeable services and products shall commence upon conclusion of the contract or upon using the service.

5.2 Hostpoint generally invoices the Customer for the selected contractual term in advance. The invoice is payable by the due date stated on the invoice.

5.3 If the Customer breaches the aforementioned payment terms, Hostpoint shall be authorized to charge 8% late interest and, in addition, as of the second reminder it is entitled to charge dunning fees in the amount to cover costs. Hostpoint is also authorized to terminate the service pursuant to Cl. 11.2.3. In addition, Hostpoint has the right to suspend the service after the first unsuccessful reminder to the Customer.

5.4 The parties waive their right to offset mutual claims against each other.

6. Warranty

6.1 Hostpoint strives to provide the hosting services carefully and professionally. Hostpoint cannot however guarantee that the Customer website will be available continuously on the internet and that the data requested by the Customer is transmitted correctly over the internet. Hostpoint, in addition, assumes no warranty that the services provided by Hostpoint and any third parties used will put the Customer in the position of achieving the financial purpose or other purpose intended by him.

6.2 Reports by the Customer of hosting service malfunctions service must contain a written (by registered letter or e-mail with subsequent acknowledgment of receipt by Hostpoint) notice of defect with a comprehensible description of the defects claimed. The Customer must also set Hostpoint a reasonable grace period of at least 30 days to remedy the defects specified in the notice of defect. After the grace period has passed without the situation being remedied, the Customer is authorized to immediately terminate the contract. Hostpoint shall reimburse the Customer for any previously paid fee pro rata for the period in which the Customer no longer uses the service due to the termination. Any kind of additional compensation is excluded subject to Cl. 7 of these GTC.

6.3 The applications provided in the Hostpoint Control Panel (see Cl. 2.4) shall be installed and used at the Customer's own responsibility and risk. Hostpoint shall assume no warranty in this regard. In particular, Hostpoint gives no assurance or warranty as to the completeness, accuracy, consistency, reliability, proper functioning, marketability, quality, suitability for a specified intended purpose or for certain results, absence of defects etc. with regard to the applications.

7. Liability of Hostpoint

7.1 Hostpoint shall be fully liable to the Customer for direct proven loss or damage caused by willful intent or gross negligence by Hostpoint.

7.2 Liability for medium or ordinary negligence shall be limited to the amount of CHF 100,000.00 per calendar year.

7.3 Liability shall be expressly excluded for slight negligence and for indirect loss or damage or consequential damage. Consequential loss or damage includes, without limitation, lost profits, lost production, harm to reputation, and damages resulting from a loss of data.

7.4 Any kind of liability for damages resulting from the abusive use of or unauthorized access to Hostpoint's communications infrastructure or the Customer website by third parties is also excluded. Examples of this includes, but is not limited to, any interference by means of using computer viruses or DDoS attacks, as well as any change by hackers or unauthorized sending of e-mails. The exclusion of liability also applies to damages incurred by the Customer as a result of measures taken by Hostpoint necessary to defend against such third-party attacks (e.g. blocking access to the Customer's website to protect Hostpoint's infrastructure and the websites of other Customers from DDoS attacks).

7.5 The above exclusions and limitations of the liability of Hostpoint shall not apply in the case of death, physical injury and impairment to health and in the case of mandatory statutory regulations, including the regulations in the Product Liability Act.

8. Liability of the Customer

The Customer shall be fully liable to Hostpoint for loss or damage caused by willful intent or gross negligence. The Customer's liability for slight negligence is expressly excluded.

9. Confidentiality and data protection

9.1 Hostpoint and the Customer mutually undertake to safeguard the confidentiality of all information and data not generally known which becomes accessible to them in preparing for and implementing the contract. This duty shall remain even after the contract has come to an end as long as there is a legitimate interest therein.

HOSTPOINT

9.2 Hostpoint and the Customer shall be responsible for ensuring data protection and data security in their respective spheres of influence and responsibility. Furthermore, Hostpoint is entitled to inform Customers about ongoing developments and new services from Hostpoint. The Customer can indicate that they do not wish to receive such information in the Control Panel at any time. Hostpoint only stores personal data provided that and so long as it is required to provide services or Hostpoint is obliged to do so by law.

9.3 In connection with the provision of hosting services, Hostpoint exclusively processes the Customer's data in order to fulfill the contract. If Hostpoint processes personal data for the Customer as a contracted data processor under the applicable data protection law, it only does so in the manner stipulated in the Data Processing Agreement (**"DPA"**) in accordance with Annex 2 of these GTC and exclusively for the Customer's purposes. In this case, the Customer is solely responsible for determining the purpose and means of the processing or use of the personal data by Hostpoint within the context of the contract and in particular for ensuring that such processing does not violate any applicable data protection law.

10. Intellectual property

10.1 Customers shall receive the non-transferable, non-exclusive right to make use of and utilize the service throughout the term of the contract.

10.2 All existing intellectual property rights in and to the services of Hostpoint and all intellectual property rights arising when the contract is implemented (e.g. programs, samples, data, Control Panel) shall remain with Hostpoint or with the third parties used by Hostpoint.

11. Contractual term and termination

11.1 Term – general

These GTC shall apply throughout the entire period during which services are used by the Customer.

11.2 Hosting service contract

11.2.1 The contract for hosting services (see 2.2.) between Hostpoint and the Customer comes into effect when Hostpoint sends the contract documents to the e-mail address that the Customer has provided for the purpose of contract-related communications, when the Customer accepts a Customer-specific offer, or when the Customer makes use of the services. The contract is valid for the period selected by the Customer when placing the order or stated in the Customer-specific offer (1, 6, or 12 months). The contract may be terminated by either party with a notice of 30 days as at the end of the agreed contractual term. The termination notice shall be submitted in writing by registered letter or online by using the Hostpoint ID in the Hostpoint Control Panel. Hostpoint shall also be entitled to serve the termination notice by e-mail to the e-mail address stated by the Customer for contract-related messages. If it is not terminated within the due time the contract shall be automatically renewed in each case for the agreed contractual term.

11.2.2 Right to cancel: The Customer may cancel his order for hosting services within 30 days, without stating reasons, in text form (registered letter, e-mail with subsequent acknowledgment or receipt by Hostpoint or online by using the Hostpoint ID in the Control Panel – provided that the Customer as the result of an existing Customer relationship already has access to the Control Panel). The period shall commence after receipt of this cancellation advice. Timely dispatch of the cancellation suffices to prove that the cancellation period has been complied with. The cancellation must be sent to billing@hostpoint.ch. The Customer must use the contact e-mail address notified to Hostpoint as sender. In his e-mail the Customer must also include the contract documents provided by Hostpoint as an enclosure. The cancellation right shall apply only when an order is made through the Hostpoint website and only for hosting services that are not customized. The cancellation right does not apply to (in particular, without limitation) domain names.

11.2.3 If the Customer breaches contractual provisions (including the Usage Guidelines for Hosting Services), misuses services for illegal purposes, makes Prohibited Contents accessible, or threatens to harm Hostpoint's reputation, Hostpoint is authorized in its own discretion to deactivate the Customer website without delay and/or terminate the contract without notice. The Customer shall owe Hostpoint the charges due up until ordinary termination of the contract as well as compensation for all additional costs incurred in connection with terminating the contract without notice.

11.3 Hostpoint may also terminate the contract with the Customer with immediate effect if proceedings have been initiated against the Customer for bankruptcy or insolvency or if it otherwise becomes clear that the Customer can no longer meet his payment obligations, and if the Customer does not prior to the expiry of the contractual term advance the costs for the next contractual term or provides a corresponding security.

11.4 After the expiry of the contract, Hostpoint is authorized to delete the Customer's data. The Customer is personally responsible for backing up their data in a timely manner. The DPA shall remain in force until the personal data processed is deleted.

12. Amendments to the contractual conditions

12.1 Hostpoint shall endeavor to keep its infrastructure up to date to a standard which corresponds to the security specifications and technical standard that are customary for the industry. The Customer acknowledges that new technical developments, security specifications and/or changes in the range of services of contractual partners of Hostpoint or the open source software used by Hostpoint may result in the range of services being expanded or restricted and may also have an impact on the way the price changes.

12.2 Therefore, Hostpoint explicitly reserves the right to change the contractual conditions, including these GTC and the DPA in Annex 2, at any time. Amendments to the GTC shall be made accessible on the Hostpoint website and shall come into effect when they are activated. Any price increases or restrictions in services that adversely affect the Customer during the contractual term shall be notified by Hostpoint to the Customer in writing by e-mail in the case of hosting service contracts. If the Customer does not accept the amendments, he has the option of informing Hostpoint of this in writing within 30 days of receipt of the message by registered letter or online by using the Hostpoint ID in the Control Panel and terminating the contract as at the end of the month. If there is no written message within this period, the changes shall be deemed to be approved by the Customer.

13. Additional provisions

13.1 In the case of Customers with hosting service contracts, contract-related messages such as the notification of price changes are sent by e-mail to the owner e-mail address defined by the Customer in the Control Panel. The Customer shall be responsible for ensuring that the Customer data saved in the Control Panel (invoice and administration contact and technical contact) throughout the entire term of the contract is up to date, complete and correct. Hostpoint is not obligated to take heed of any Customer data other than the Customer data saved in the Control Panel or to make inquiries itself with regard to correcting this data. Hostpoint is, however, authorized to correct or delete input

in the Control Panel that is patently incorrect or that infringes third-party rights.

13.2 Rights and duties under the hosting service contract can only be transferred to third parties with the written consent of the other party. This provision does not apply to the transfer of the contract from Hostpoint to a legal successor or associated company.

13.3 These GTC and any disputes arising under or in connection with the contractual relationship between Hostpoint and the Customer shall be subject exclusively to **Swiss law,** excluding its conflict of laws rules and the provisions of the UN Convention on Contracts for the International Sale of Goods (CISG).

13.4 The ordinary courts at the **registered office of Hostpoin**t shall have exclusive jurisdiction. Hostpoint also has the option of taking legal action against the Customer at the latter's domicile.

Rapperswil-Jona, July 2024

HOSTPOINT

Annex 1: Guidelines for use of Managed Flex Server services

These Usage Guidelines for hosting services (hereafter "Usage Guidelines") shall apply to all hosting services offered by Hostpoint AG ("Hostpoint"). By using our hosting services, you accept the following Usage Guidelines completely without any alteration.

1. Scope of application and conclusion of contract

1.1 These Usage Guidelines cover the use of hosting services which Hostpoint provides to its Customers (hereafter "Customer"). They are subject to the General Terms and Conditions (GTC) of Hostpoint.

1.2 By using the hosting services, the Customer accepts these Usage Guidelines in addition to the GTC. They shall apply throughout the entire term of use of hosting services.

1.3 If there are discrepancies between provisions of the GTC and the provisions of these Usage Guidelines, the provisions of the GTC shall prevail unless these Usage Guidelines expressly provide otherwise with reference to the corresponding provision of the GTC.

2. Use of the hosting services

2.1 The use of the hosting services may only happen in accordance with the GTC, these Usage Guidelines and the law applicable in Switzerland and abroad. The following actions in particular are prohibited:

- Committing a crime (fraud, computer crime, money laundering, infringement of business secrets, document forgery, violence and threats against authorities and civil servants, unauthorized gaming etc.), participating in a criminal act (collaborating, instigating, aiding and abetting), or the transferral of hosting services for the purpose of the committing of a criminal act by third parties who are under the supervision of the Customer, such as children, employees, subcon- tractors etc. (hereafter "Agents").

- Disseminating or making accessible contents that are against the criminal law or civil law (depictions of violence, so-called soft and hard pornography, incitement to disturb the public peace, disruption of freedom of religion and culture, racial discrimination, libel, defamation, infringement of privacy etc.) by the Customer himself or by his Agents. Soft porn may, however, be made accessible if the Customer installs effective controls which merely enable those over 16 years of age to access corresponding contents.

- Unauthorized receipt, storage or dissemination of contents which are protected by law (copyright, trademark, data protection, design and patent law).

2.2 The Customer is obligated to take suitable precautions to prevent the illegal use of the hosting services and to inform Hostpoint immediately of anything appropriate that is found that would prevent the hosting services from being misused. Notwithstanding the limitations on liability provided in Cl. 8 of the GTC, the Customer shall indemnify Hostpoint in full for all claims made against Hostpoint in connection with the use of the hosting services by the Customer and the individuals under his supervision. The loss or damage to be compensated also includes the costs of a proper legal defense of Hostpoint. The Customer undertakes to assist Hostpoint and the third-party used by it in any proceedings. Hostpoint is entitled to require the Customer to provide a security deposit as a precautionary measure to ensure coverage of the loss or damage. Hostpoint is entitled to suspend the services or to terminate the contract without giving notice if the security deposit is not provided.

2.3 Depending on the Flex Server configuration selected by the Customer, they may also use resource-intensive applications and scripts as well as allow downloads. Forms of use that might jeopardize the normal functioning or the security of Hostpoint's infrastructure, network and its Customers are prohibited. In case of doubt, prior written approval must be obtained from Hostpoint. However, Hostpoint remains entitled at any time to immediately revoke previously granted approval for the sake of protecting its operations and services and may immediately prohibit further use.

Executing the following processes is prohibited in all cases:
- Peer-to-peer software;
- Network scanners;
- Brute force programs/scripts/applications;
- Mailbombs/spam scripts;
- Proxies;
- VoIP software;
- Game servers;
- Bots, webcrawlers, IRC servers, clients;
- Terminal emulations;
- Crypto-mining software.

This list is not exhaustive and it is the responsibility of the Customer, prior to installing an application/script, to check whether activation is permitted based on these Usage Guidelines. The Customer can send a query to Hostpoint for this purpose.

3. Electronic mail

3.1 The Customer is responsible for the content of the messages which he sends while using a Hostpoint service. The Customer shall indemnify Hostpoint if third parties assert claims against Hostpoint in connection with the transmission of messages on the part of the Customer.

3.2 Sending identical e-mails to a large number of addressees is prohibited to the extent that this is done without the prior consent of the addressees (opt-in), without correctly stating the identity of the sender or without a reference to a simple and free opt-out (spamming). By way of exception, sending information concerning goods and services without a prior opt-in of the recipient is permitted if the recipient concerned is already a Customer of

the sender and the message contains information on goods and services similar to the ones already received by the recipient as well as a reference to a simple and free opt-out (Art. 3 (1) lit. o UWG).

3.3 The use of a third-party mail server as a distribution station (relay) for the processing of identical unsolicited messages to a large number of addressees with the domain name registered with us is prohibited.

3.4 Offering banner exchange and e-mail exchange pages is prohibited.

3.5 Advertising websites and services which are operated on the infrastructure provided by Hostpoint, by means of identical, unsolicited messages to a large number of addressees is prohibited (spamvertising).

4. Security guidelines

4.1 A breach of system and network security constitutes a contractual breach for which the Customer shall be liable under civil law. The limitations on liability provided in Cl. 8 of the GTC shall not apply. If the necessary preconditions are met, the Customer shall also be liable under criminal law. The following actions in particular constitute such breaches of system and network security:

- Unauthorized access to or unauthorized use of data, systems and network elements, checking the vulnerability of the system or network competence without prior agreement (scanning) or the attempt to penetrate security measures and authorization measures, without first obtaining the prior written consent of the affected party.
- Unauthorized monitoring of the data traffic without the prior written consent of the competent authorities or the network owner (sniffing).
- Harming of the systems of Hostpoint and its Customers, including by mail bombs, mass mailing or other attempts to overload the system (flooding).
- Hacking management information in TCP/IP packets (packet headers), e.g. the TCP/IP addresses or information in the management section (e.g. address of recipients/senders), in an electronic message.

4.2 The passwords or other identifying parameters notified to the Customer are intended for personal use by the recipient and must be treated as confidential. Hostpoint may rely on the fact that the person using an identification parameter is authorized to do so.

4.3 The Customer and his Agents are obligated to terminate use of the hosting services in accordance with the procedure recommended by Hostpoint (for example, closing the browser by clicking on “Logout”, “Sign off” or “Exit”).

5. Prosecuting breaches

Hostpoint will prosecute breaches of these Usage Guidelines in accordance with the GTC (see in particular Cl. 3.2.2 and 3.2.6 of the GTC).

6. Messages and changes

6.1 The Customer is obligated to inform Hostpoint immediately of the defects, disruptions or interruptions of hosting services, systems or software, including all cases of illegal or non-contractual use of the service by third parties (e.g. hackers), which have come to their attention.

6.2 Messages in connection with the Usage Guidelines stipulated here must be sent to: info@hostpoint.ch.

6.3 Hostpoint reserves the right to amend these Guidelines in accordance with the principles contained in the GTC.

Rapperswil-Jona, July 2024

HOSTPOINT

Annex 2: Order-Related Data Processing Agreement (DPA)

Hostpoint AG (**"Hostpoint"**) provides clients with hosting services for one or more of the client's websites or applications. In provision of these hosting services, Hostpoint stores personal data on behalf of and for the purposes of the client (**"Order Processing"**).

1. Object and application area of the order-related DPA

1.1 This order-related data processing agreement (**"DPA"**) regulates the obligations, roles and responsibilities of Hostpoint and the client (**"Contracting Parties"**) in terms of order processing.

2. Relation to the Hosting Service Contract

2.1 The provisions of this DPA supplement the provisions of the Hosting Service Contract. They do not limit the rights and responsibilities of the Contracting Parties in terms of the provision or use of Hosting Services. However, concerning the subject matter, the provisions of the DPA take precedence over the conditions of the Hosting Service Contract, unless otherwise expressly agreed in the Hosting Service Contract.

3. Application area of the DPA

3.1 This DPA is valid in reference to Order Processing within the framework of the services provided by Hostpoint in accordance with the Hosting Service Contract.

3.2 This DPA explicitly does not apply to the processing of personal data for which Hostpoint determines the purpose and means of processing and is therefore subject to the Swiss Federal Act on Data Protection (FADP) or to any other applicable data protection laws (in particular, the EU General Data Protection Regulation (GDPR)). Such processing of personal data for which Hostpoint is responsible (e.g. the processing of personal data in the context of domain services or for the purposes of invoicing or communication with the client) will be carried out by Hostpoint in compliance with Hostpoint's data protection statement and the applicable data protection laws.

4. Information for order processing

4.1 The object and purpose of the Order Processing is the provision of Hosting Services by Hostpoint for clients. Order Processing consists of storage, provision, transfer and deletion of personal hosting data in accordance with the provisions set out in the Hosting Service Contract.

4.2 Order Processing concerns personal data that the client stores according to their choice of infrastructure used by Hostpoint for the provision of services, and data pertaining to people to whom the client grants access to its website or application, in particular personal data that is usually collected for the access, listing and use of websites and applications. This includes log data that is collected automatically for informational use of a website or application (e.g. the IP address and operating system of the user's device and the date and time of browser access), data entered by users and personalized usage data collected from clients (hereafter **"Personal Hosting Data"**).

5. Roles and areas of responsibility

5.1 The client confirms and Hostpoint recognizes that the client is and remains responsible for the processing of Personal Hosting Data in accordance with the applicable data protection laws. The client therefore assumes the role of controller. Cases in which the client itself is the processor of the Personal Hosting Data remain reserved (see clause 5.4).

5.2 Hostpoint acknowledges that the client, in its role as controller, is required to contractually bind Hostpoint to some of its obligations arising from the FADP or, where applicable, the GDPR (or any other applicable data protection laws) when using Hosting Services.

5.3 Hostpoint takes on the role of the processor in terms of the processing of personal data. Insofar as Hostpoint is not subject to the GDPR (or to any other of the applicable data protections laws) for this Order Processing, Hostpoint assumes this role only on the basis of its contractual obligations under this DPA and is not subject to the GDPR (or any other applicable data protections laws) for this reason alone.

5.4 If the client is the processor (i.e. if the client is authorized to make storage space available to its customers under the Hosting Service Contract), the client confirms that its customer (i.e. the controller) has authorized the client to issue instructions to Hostpoint for sub-processing as per a separate agreement.

6. Hostpoint's obligations

6.1 Hostpoint is obliged to process Personal Hosting Data only for the provision of Hosting Services in accordance with the service description and contractual obligations, and in accordance with this DPA.

6.2 Hostpoint is also entitled to process the client's Personal Hosting Data insofar as is implied for the fulfillment of service obligations arising from the Hosting Service Contract and this DPA. On request, Hostpoint is ready to implement further directives from the client for Order Processing. The client must immediately confirm verbal directives (at least in text form such as via e-mail). Hostpoint will notify the client immediately if it believes that a directive violates data protection regulations. Hostpoint is authorized to defer the execution of the respective directive until it is confirmed or changed by the client. Hostpoint can also refuse to execute the respective directive if it is not implementable and objectively reasonable for Hostpoint within the framework of the contractually concluded Hosting Services, it gives rise to

further costs or results in an alteration to the scope of services, or Hostpoint could not fulfill its legal or regulatory obligations in the event of its execution.

6.3 Hostpoint ensures compliance with the provisions set out in this DPA by employees entrusted with Order Processing and other Hostpoint personnel with access to Personal Hosting Data. Hostpoint is obliged to ensure that persons with access to Personal Hosting Data observe proper confidentiality (and also beyond the duration of their professional activities for Hostpoint).

6.4 Hostpoint is obliged to meet appropriate technical and organizational measures in the interests of confidentiality, integrity and contractual availability of Personal Hosting Data. In particular, Hostpoint implements access and admission controls and processes for the regular review, assessment and evaluation of the effectiveness of technical and organizational measures. In the selection of measures, Hostpoint takes the state of the art, the cost of implementation and the type, scope, circumstances and purposes of processing into consideration, as well as the varying probability of occurrence and the severity of risk for the data subject. The respectively applicable measures are listed in Addendum A of this DPA.

6.5 Hostpoint is obligated to inform its clients in writing without delay if it becomes aware of a data security breach that affects Personal Hosting Data. In this case, Hostpoint must inform the client of the type and extent of the breach along with possible corrective measures. The Contracting Parties enter into the necessary measures jointly to ensure protection of Personal Hosting Data and to mitigate any possible disadvantageous consequences for persons affected by the breach. Moreover, Hostpoint is obliged to make sufficient information to the client available on application in writing, in order that the client can fulfill its obligations in accordance with applicable data protection laws related to the registration, investigation and documentation of data security breaches.

6.6 Hostpoint agrees to assist its clients, upon written request and subject to separate appropriate remuneration, and within the scope of its operational resources and capabilities, with the fulfillment of data subject rights (in particular, rights of access, rectification and erasure) by the client (related to Personal Hosting Data) according to the respective applicable data protection laws (including Chapter III of the GDPR, if applicable, and the corresponding provisions of the FADP).

6.7 If a data subject contacts Hostpoint directly with requests related to the fulfillment of data subject rights, Hostpoint will refer them to the client. Hostpoint is obliged to notify the client in writing without delay if it receives a request (such as a request for access or erasure) from a data subject relating to Personal Hosting Data. The prerequisite for this is that a link to the client can be established based on the information provided by the data subject.

6.8 By written request and in return for separate, appropriate remuneration, and taking into account its operational resources and capabilities, Hostpoint is prepared to assist clients with data protection impact assessments and consultations with supervisory authorities.

6.9 Hostpoint will release or delete Personal Hosting Data after the end of the Hosting Service Contract in accordance with the provisions of the contract.

7. Use of subcontractors for data processing

7.1 If a client uses services from Hostpoint that affect Personal Hosting Data and are provided by third parties, Hostpoint will remain the client's contractor and fulfill associated obligations arising from the DPA. The third-party service provider, which is integrated in Hostpoint's service, is Hostpoint's subcontractor. But there may also be cases in which Hostpoint brokers a direct contract between the third-party service provider and the client, making the third-party service provider the client's direct processor. In such cases, it is the client's responsibility to reach any agreements with the third-party service provider that may be required under applicable data protection laws.

7.2 At the time of conclusion of the contract, Hostpoint was not using subcontractors. However, Hostpoint is authorized to use subcontractors for the provision of Hosting Services by Hostpoint. If Hostpoint wishes to use subcontractors or to replace subcontractors engaged at a future point in time, it will notify the client of this in a suitable manner, in writing, at least sixty (60) days in advance (e.g. via an e-mail or a notification function in the event of changes to the list, insofar as this is made available on the internet). The client can object in writing to an expansion or modification of the list within fifteen (15) days; the client shall only do this for reasons of data protection and justified interests; if the parties cannot reach agreement within fifteen (15) days, the client can terminate the data processing and the performance of the Hosting Service Contract affected by it without notice, provided that it shows that the objection is necessary under data protection law; stricter regulations on the use of subcontractors for the benefit of the client in the Hosting Service Contract remain reserved.

7.3 Hostpoint will only delegate the processing of Personal Hosting Data to subcontractors that have committed to processing in accordance with the FADP and, if applicable, Art. 28(3) of the GDPR.

8. Disclosure abroad

8.1 Hostpoint is obliged not to disclose personal data or transfer it to other countries except:

I. to the client itself, to its affiliated companies, or to third parties in fulfillment of a directive from the client or as set forth in the main contract (this does not apply to transfers to subcontractors of Hostpoint or other third parties used by it);

II. in the event that no stricter provisions are agreed in the Hosting Service Contract, to a recipient in a country with an adequate data protection level;

III. in the event that no stricter provisions are agreed in the Hosting Service Contract, to a recipient in a country without an adequate data protection level, insofar as the requisite conditions for lawful disclosure or transfer of personal data have been established in accordance with the FADP and, where applicable, the GDPR; or

IV. this has been agreed with the client in the Hosting Service Contract or elsewhere.

9. Client obligations

9.1 The client is responsible for the legality of processing of Personal Hosting Data, including the permissibility of the contracted or subcontracted DPA.

9.2 The client will, within its area of responsibility (such as in its own systems and applications), autonomously take appropriate technical and organizational measures to protect Personal Hosting Data.

9.3 The client agrees to immediately inform Hostpoint if it identifies any violations of applicable data protection laws in Hostpoint's provision of services.

HOSTPOINT

10. Rights of information and verification

10.1 Hostpoint is required, on written request, to provide the client with all the information that it reasonably needs to prove compliance with this DPA to data subjects or data protection or other supervisory authorities.

10.2 Hostpoint will enable the client or a third-party representative that has signed a non-disclosure agreement with the client to verify Hostpoint's compliance with this DPA. If evidence is submitted showing that Hostpoint has violated the DPA, it must implement suitable corrective measures immediately and at no cost.

10.3 The above rights of information and verification given to the client exist only if the Hosting Service Contract does not grant the client other rights of information and verification that comply with the relevant requirements of applicable data protection laws. Furthermore, these rights of information and verification are subject to the principle of proportionality and the protection of Hostpoint's legitimate interests (in particular, security and confidentiality interests). Unless the Contracting Parties agree otherwise, the client will bear all costs of information and verification, including Hostpoint's proven internal costs.

11. General provisions

11.1 Terms specific to data protection law, such as "personal data", "processing", "controller", "processor", "data protection impact assessment", etc. have the meaning ascribed to them in the GDPR or the FADP, depending on the context.

Rapperswil-Jona, July 2024

HOSTPOINT

Addendum A: Technical and Organizational Measures (TOM)

The following contains the description of the technical and organizational measures implemented by Hostpoint to ensure an appropriate level of security ("TOM"), taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of data subjects:

A. Measures of pseudonymisation and encryption of Personal Data

- Additional information for attributing Personal Data to a specific data subject is kept in separate and secure systems which are only accessible by a limited number of individuals.
- When encrypting Personal Data, algorithms and length of keys are kept proportionated to level of sensitivity of the data.
- Encryption keys are kept secure and only given to a limited number of individuals.

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

- Data protection aspects are established as an integral part of corporate risk management.
- Staff is trained and bound by confidentiality and data secrecy.
- Staff is informed about possible consequences of breaching security rules and procedures.
- Work instructions on access control, communication security and operational security are provided to staff.
- Components critical to system operation can be replaced within the required time in the event of their collapse, for example, by backup components, redundant systems or data mirroring.
- Where necessary, separate storage locations are used for operating systems and data.

C. 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

- A backup strategy is defined based on the nature of the data and its frequency of change.
- The same security measures are applied to the backup systems as to the productive systems.
- Individuals entrusted with restoring data are specially trained for this task.

D. Measures for user identification and authorisation

- Access to information systems is protected by industry-standard identification and authentication procedures.
- User accounts and user permissions are managed by designated individuals (administrators).
- The restrictive, need-based authorisation concept is managed by a minimum number of administrators.
- Access to Personal Data is restricted to employees who have a legitimate need to access such Personal Data within the scope of their individual job function or role.
- Guidelines are developed and implemented on the following topics: "secure passwords", "deletion/destruction", "clean desk", "mobile device".
- Multi factor authentication is used to access systems where possible.

E. Measures for the protection of data during transmission

- Remote access takes place only over encrypted lines.
- Electronic transfer of data and transmission of Personal Data is carried out with industry-standard encryption methods. For e-mails, at least line encryption (TLS) is offered and used where supported.

F. Measures for the protection of data during storage

- Access to specific data is restricted to those who need to Process that data.
- Where relevant, different customer data is stored in different databases.
- Data storage devices, workstations, notebooks, smartphones and tablets are encrypted with industry-standard encryption methods.
- External storage media that contain sensitive Personal Data are encrypted and kept under lock and key.
- Data stored in the Data Centre is protected against physical access (see paragraph G) and encrypted where possible.
- Rights to enter, change and delete data are assigned on the basis of an authorisation concept.

HOSTPOINT

G. Measures for ensuring physical security of locations at which Personal Data are Processed

- Systems and services are protected against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access.
- A burglar alarm system including 24/7 alarm is installed.
- Keys and key cards are allocated to individuals.
- Entrance or reception is staffed 24/7.
- Buildings and entrances are under constant video surveillance.
- Visitors and external personel are always accompanied by employees.
- For systems that are housed, hosted and maintained by external service providers, corresponding measures to be implemented and maintained by these service providers are arranged.

H. Measures for ensuring event logging

- Access authorisations and retrieval of data are logged.
- Allocation of keys and key cards are logged.
- Visitors' access is logged.
- Security incidents and data breaches are logged. Records are maintained that include nature of the data breach, categories and approximate number of data subjects concerned, categories and approximate number of Personal Data records concerned, time period, consequences of the data breach, procedure for recovering data, measures taken to mitigate adverse effects, name(s) of the person(s) who reported the data breach and name(s) of the person(s) to whom the data breach was reported.
- Logs allow traceability of individual users.

I. Measures for internal IT and IT security governance and management

- All systems and software are regularly updated.
- Security fixes are installed timely.
- Security advisories and Vulnerability disclosures are monitored, evaluated and mitigated timely.
- A formalized procedure for handling security incidents is in place.
- Remote access by external parties (e. g. suppliers) is monitored.

J. Measures for ensuring data minimization

- Personal Data is only collected to the extent necessary to fulfil the intended purposes.
- Data protection-friendly default settings are used.
- Personal Data held is reviewed periodically and deleted if not used anymore and if no legal or contractual requirements or technical constraint prohibit the deletion of such Personal Data.

K. Measures for ensuring data quality

- Where appropriate, data entry is subject to plausibility tests.
- Where appropriate, users are presented with the opportunity to verify data entered.

L. Measures for ensuring limited data retention

- Where appropriate and possible, retention periods are defined.
- Retired documents and data in productive systems, are archived and shelved where retention is required.

M. Measures for allowing data portability and ensuring erasure

- Data portability requests are sent to the correct units without delay and addressed promptly so that statutory deadlines are met in any case.
- Appropriate measures are implemented to ensure the removal of Personal Data from Provider's systems upon termination of the Principal Agreement.

N. Partners and Sub-Processors

In the event that Hostpoint engages sub-processors, it shall ensure that the sub-processors are bound to implement and maintain adequate TOMS (taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of data subjects and satisfying the requirements of the applicable data protection laws), with such TOMS meeting at least all of the following requirements:

- Prevent unauthorized persons from gaining access to data processing systems on which Personal Data is processed;
- Prevent data processing systems from being accessed, copied, changed, destroyed or deleted by unauthorized persons;
- Ensure that, in the course of electronic transmission or during the transport or storage on a data carrier, Personal Data cannot be read, copied, altered or removed by unauthorized persons, and that it is possible to verify and establish to which recipients Personal Data are to be transmitted to by data transmission equipment;
- Ensure that it is possible to verify and establish whether and by whom Personal Data have been entered into, altered or removed from any data processing system;
- Ensure that Personal Data is processed in accordance with the instructions of Hostpoint;
- Ensure that appropriate measures are implemented for the removal of Personal Data from the sub-processor's systems upon termination of the relevant existing agreement;
- Ensure that Personal Data is protected against accidental destruction, alteration or loss or unauthorized access;
- Guarantee that data that has been collected for different purposes can be processed separately;
- Guarantee that the effectiveness of technical and organizational measures for ensuring the security of the processing of Personal Data is regularly tested, assessed and evaluated by the sub-processor; and
- Ensure adequate organizational measures to protect Personal Data.

Rapperswil-Jona, July 2024