

request()

DATU APSTRĀDES LĪGUMS (DPA)

Pēdējo reizi atjaunots: 2026. gada 15. oktobrī

1. Līguma priekšmets un piemērošanas joma

Šis Datu apstrādes līgums (turpmāk – Līgums) nosaka kārtību, kādā SIA Request, vienotais reģistrācijas numurs: 40203423105, juridiskā adrese: Stabu iela 109 - 1, Rīga, LV-1009, Latvija (turpmāk – Apstrādātājs) veic personas datu apstrādi Klienta (turpmāk – Pārzinis) vārdā, nodrošinot hostinga un infrastruktūras pakalpojumus (turpmāk – Pakalpojumi) zīmola request.host ietvaros.

Pārzinis ir pieņemtajā pasūtījumā norādītais Klients, kas nosaka apstrādes nolūkus. Ja Klients ir cita pārziņa apstrādātājs, tas darbojas sava pilnvarojuma ietvaros un Apstrādātājs ir apakšapstrādātājs; atsauces uz Pārzini attiecīgi attiecas uz Klientu. Pārziņa kontaktinformācija ir pieņemtajā pasūtījumā vai Klientu portālā norādītā informācija ar vēlākajiem paziņotajiem labojumiem.

Šis Līgums ir starp Apstrādātāju un Klientu noslēgtā līguma “Lietošanas noteikumi” (turpmāk – Noteikumi) neatņemama sastāvdaļa. Šajā Līgumā Apstrādātājs un Klients tiek saukti par pusēm (turpmāk katrs atsevišķi – Puse, abi kopā – Puses). Līgums stājas spēkā ar derīgu rakstveida vai elektronisku pieņemšanu Noteikumos paredzētajā kārtībā.

Puses apņemas ievērot Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (turpmāk – Regula) un citus piemērojamus normatīvos aktus. Citi termini lietoti Noteikumu vai Regulas izpratnē.

DATA PROCESSING AGREEMENT (DPA)

Last updated: October 15, 2026

1. Subject Matter and Scope of the Agreement

This Data Processing Agreement (hereinafter – the Agreement) defines the procedure by which SIA Request, registration number: 40203423105, legal address: Stabu iela 109 - 1, Riga, LV-1009, Latvia (hereinafter – the Processor) processes personal data on behalf of the Customer (hereinafter – the Controller) while providing hosting and infrastructure services (hereinafter – the Services) under the brand request.host.

The Controller is the Customer identified in the accepted order and determines the purposes of processing. Where the Customer is another controller's processor, it acts within its authorization and the Processor acts as a sub-processor; references to the Controller apply to the Customer accordingly. The Controller's contact details are those specified in the accepted order or the Customer Portal, as subsequently notified and updated.

This Agreement is an integral part of the agreement “Terms of Service” (hereinafter – the Terms) concluded between the Processor and the Customer, hereinafter referred to separately as – the Party and collectively as – the Parties. This Agreement takes effect through valid written or electronic acceptance in accordance with the Terms.

The Parties undertake to comply with Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter – the Regulation) and other applicable laws and regulations. Other terms have the meanings given in the Terms or the Regulation.

SIA Request veiktā personas datu apstrāde saviem klientu kontu, norēķinu un citiem patstāvīgi noteiktiem nolūkiem ir aprakstīta Privātuma politikā.

2. Apstrādes objekts, veids un nolūks

Apstrādātājs apstrādā personas datus Pārziņa vārdā saskaņā ar Regulas 4. panta 2. punktu un tikai atbilstoši dokumentētiem Pārziņa norādījumiem, tostarp attiecībā uz datu nodošanu uz trešajām valstīm. Norādījumus veido pieņemtais Pakalpojumu plāns, Noteikumi, Līgums, pilnvarotie iestatījumi un vēlākie rakstveida vai elektroniskie pieprasījumi. Ja apstrādi pieprasa Apstrādātājam piemērojamie Savienības vai dalībvalsts tiesību akti, Apstrādātājs iepriekš informē Pārziņi, izņemot gadījumus, kad attiecīgie tiesību akti to aizliedz svarīgu sabiedrības interešu dēļ.

Apstrādes objekts

Personas dati, ko Pārziņis izvietoj Apstrādātāja hostinga infrastruktūrā un serveru instancēs, tostarp tīmekļa vietnēs, lietotnēs, datubāzēs, failos, saistītajos žurnālfailos un rezerves kopijās, kā arī saturs, kas nodots saskaņotai migrācijai vai atbalstam.

Apstrādes veids un nolūks

Hostinga un infrastruktūras pakalpojumu nodrošināšana, uzturēšana, drošība un datu glabāšana Pakalpojumu plānā noteiktajā apjomā. Apstrāde ietver glabāšanu, organizēšanu, izgūšanu, pārsūtīšanu, kopēšanu, atjaunošanu, tehnisko piekļuvi un dzēšanu. DNS un tīmekļa datplūsmas apstrāde notiek tikai atbilstoši atļautajām funkcijām.

Apstrādātājs piekļūst personas datiem tikai tādā apjomā, kas nepieciešams Pakalpojumu nodrošināšanai, uzturēšanai, drošībai vai tehniskajam atbalstam. Šie dati netiek izmantoti Apstrādātāja reklāmai vai nesaistītiem komerciāliem nolūkiem.

Personas datu veidi

Jebkuri dati, ko Pārziņis izvēlas apstrādāt Pakalpojumu ietvaros (piemēram, vārdi un uzvārdi, e-pasti, kontu dati, tiešsaistes identifikatori, IP adreses, pirkumu vēsture, saziņa, tīmekļa vietņu saturs un sistēmas žurnālfaili). Pārziņis nosaka faktisko saturu un pirms apstrādes informē par īpašām aizsardzības prasībām, tostarp īpašu kategoriju vai ar sodāmību saistītiem datiem;

The processing of personal data by SIA Request for its own customer-account, billing and other independently determined purposes is described in the Privacy Policy.

2. Object, Nature, and Purpose of Processing

The Processor shall process personal data on behalf of the Controller in accordance with Article 4(2) of the Regulation and only on documented instructions from the Controller, including with regard to transfers of personal data to third countries. Instructions comprise the accepted Service Plan, the Terms, this Agreement, authorized settings, and subsequent written or electronic requests. Where processing is required by Union or Member State law applicable to the Processor, the Processor shall first inform the Controller, unless that law prohibits this on important grounds of public interest.

Object of Processing

Personal data hosted by the Controller on the Processor's hosting infrastructure and server instances, including in websites, applications, databases, files, associated logs and backups, and content supplied for agreed migration or support.

Nature and Purpose of Processing

Provision, maintenance and security of hosting and infrastructure services, including data storage, to the extent specified in the Service Plan. Processing includes storage, organization, retrieval, transmission, copying, restoration, technical access, and deletion. DNS and website-traffic processing takes place only through the authorized functions.

The Processor accesses personal data only to the extent necessary for the provision, maintenance, security or support of the Services. These data shall not be used for the Processor's advertising or unrelated commercial purposes.

Types of Personal Data

Any data the Controller chooses to process within the Services (e.g., names, emails, account details, online identifiers, IP addresses, purchase history, communications, website content, and system logs). The Controller determines the actual content and shall identify particular protection requirements, including for special-category or criminal-conviction data, before processing; any necessary additional

nepieciešamās papildu vienošanās noslēdz pirms attiecīgās apstrādes.

Datu subjektu kategorijas

Pārziņa tīmekļa vietņu apmeklētāji, klienti, darbinieki un citas personas, kuru datus Pārzinis apstrādā Pakalpojumu ietvaros.

Apstrādes ilgums

Visu Pakalpojumu sniegšanas laiku līdz brīdim, kad dati un to kopijas tiek atdoti vai dzēsti saskaņā ar šā Līguma 8. nodaļu.

Norādījumu tiesiskums

Pārzinis apliecina, ka tam ir tiesisks pamats visu nodoto datu apstrādei, un nodrošina nodoto datu un norādījumu tiesiskumu, nepieciešamo informēšanu un pilnvarojumu. Apstrādātājam nav pienākuma pārbaudīt visu saturu, taču tas nekavējoties informē Pārzini, ja, pēc tā domām, norādījums pārkāpj Regulu vai citus piemērojamos Savienības vai dalībvalsts datu aizsardzības noteikumus. Attiecīgā norādījuma izpildi var apturēt līdz jautājuma atrisināšanai.

3. Datu nodošana uz trešajām valstīm

Hostinga infrastruktūras atrašanās vietas izvēlas Apstrādātājs, izmantojot Līguma 6. nodaļā norādīto apakšapstrādātāju infrastruktūru Vācijā, Somijā, Amerikas Savienotajās Valstīs vai Singapūrā. Ar šo Līgumu Pārzinis dod dokumentētu norādījumu izvietot un pārvietot hostinga vidi šajās valstīs un starp tām, ievērojot Līguma nosacījumus. Atsevišķi saskaņotu glabāšanas reģionu vai atrašanās vietas ierobežojumu maina tikai ar Pārziņa dokumentētu atļauju. Tīmekļa vietņu rezerves kopijas glabājas Backblaze B2 EU-Central reģionā Amsterdamā, Nīderlandē. Apstrādātājs administrē Pakalpojumus no Rīgas, Latvijā. Šīs glabāšanas vietas nenožīmē, ka visa piegādātāju piekļuve, atbalsts vai atļautā tīkla apstrāde notiek tikai Eiropas Ekonomikas zonā (EEZ).

Jebkura datu nodošana ārpus EEZ, tostarp attālinātas piekļuves nodrošināšana, notiek tikai saskaņā ar dokumentētiem Pārziņa norādījumiem un Regulas V nodaļas nosacījumiem. Apstrādātājs piemēro attiecīgu lēmumu par aizsardzības līmeņa pietiekamību vai atbilstošas garantijas, tostarp nepieciešamās Eiropas Komisijas līguma standartklauzulas, novērtējumu un papildu pasākumus. Pārzinim sniedz informāciju par

arrangements shall be agreed beforehand.

Categories of Data Subjects

The Controller's website visitors, customers, employees, and other individuals whose data the Controller processes within the Services.

Duration of Processing

For the entire duration of the Service provision until data and its copies are returned or deleted in accordance with Section 8 of this Agreement.

Legality of Instructions

The Controller confirms that a legal basis exists for the processing of all transferred data and shall ensure lawful data and instructions, necessary notices and authorization. The Processor need not inspect all content but shall immediately inform the Controller if, in its opinion, an instruction infringes the Regulation or other applicable Union or Member State data-protection provisions. The Processor may suspend that instruction pending resolution.

3. Data Transfer to Third Countries

The Processor selects hosting infrastructure locations using the infrastructure of the sub-processors listed in Section 6 of this Agreement in Germany, Finland, the United States or Singapore. This Agreement constitutes the Controller's documented instruction to deploy and relocate the hosting environment within and between these countries, subject to this Agreement. A separately agreed storage region or location restriction shall be changed only with the Controller's documented authorization. Website backups are stored in Backblaze B2's EU-Central region in Amsterdam, Netherlands. The Processor administers the Services from Riga, Latvia. These storage locations do not mean that all supplier access, support or authorized network processing occurs only within the European Economic Area (EEA).

Any transfer outside the EEA, including remote access, shall take place only on documented instructions from the Controller and in accordance with Chapter V of the Regulation. The Processor shall apply an applicable adequacy decision or appropriate safeguards, including the necessary European Commission standard contractual clauses, assessment and supplementary measures. The Controller shall receive information about the

attiecīgajiem saņēmējiem, valstīm un garantijām, kā arī iespēju saņemt to kopiju, ievērojot tiesiskus konfidencialitātes ierobežojumus. Apakšapstrādātāja atļauja neaizstāj nodošanai nepieciešamās garantijas.

4. Tehniskie un organizatoriskie pasākumi

Apstrādātājs nodrošina Pārziņa datu pienācīgu aizsardzību saskaņā ar Regulas 32. pantu, kombinējot savus tehniskos un organizatoriskos pasākumus ar tiem, kurus pārvalda apakšapstrādātāji. Pasākumus piemēro atbilstoši apstrādes riskiem, ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūkus, tehnikas attīstību un ieviešanas izmaksas, lai nodrošinātu sistēmu un Pakalpojumu konfidencialitāti, integritāti, pieejamību un noturību.

Joma	Atbildība	Pasākumu apraksts
Fiziskā drošība	Apakšapstrādātājs	Infrastrukturā piegādātāji nodrošina datu centru fiziskās piekļuves un aparatūras aizsardzību. Apstrādātājs izvērtē šo pasākumu atbilstību.
Pieejamība	Apstrādātājs / Apakšapstrādātājs	Infrastrukturā piegādātāji nodrošina elektroapgādes un vides aizsardzību. Apstrādātājs standarta tīmekļa vietņu rezerves kopijas veido katru dienu, glabā atsevišķi no aktīvās vides un parastā kārtībā saglabā ne ilgāk kā 30 kalendāra dienas no izveidošanas. Atdošanu un dzēšanu nosaka Līguma 8. nodaļa.
Piekļuves kontrole	Apstrādātājs / Pārzinis	Administratīvo piekļuvi piešķir tikai pilnvarotām personām, izmantojot pakalpojumu piekļuves datus un lietotāju atļaujas. Pārzinis pārvalda savus lietotājus, piekļuves datus un lietotņu aizsardzību, ciktāl attiecīgie darbi nav ietverti pārvaldītajos Pakalpojumos.
Datu izolācija	Apstrādātājs	Apstrādātājs nodrošina loģisku Klientu datu un hostinga vides nošķiršanu.

relevant recipients, countries and safeguards and access to a copy, subject to lawful confidentiality restrictions. Sub-processor authorization does not replace the required transfer safeguards.

4. Technical and Organizational Measures

The Processor ensures the appropriate protection of the Controller's data in accordance with Article 32 of the Regulation by combining its own technical and organizational measures with those managed by the sub-processors. Measures shall be appropriate to the processing risks, taking account of the nature, scope, context, and purposes of processing, the state of the art and implementation costs, to ensure the confidentiality, integrity, availability, and resilience of systems and services.

Area	Responsibility	Description of Measures
Physical Security	Sub-processor	Infrastructure providers supply physical-access and hardware protections at data centers. The Processor assesses the suitability of these measures.
Availability	Processor / Sub-processor	Infrastructure providers supply power and environmental protections. The Processor makes standard website backups daily, stores them separately from the active environment and ordinarily retains them for no more than 30 calendar days from creation. Return and deletion are governed by Section 8 of this Agreement.
Access Control	Processor / Controller	Administrative access is restricted to authorized persons, using service credentials and user permissions. The Controller manages its users, credentials and application protection to the extent that this work is outside the managed Services.
Data Isolation	Processor	The Processor applies logical separation of Customer data and hosting environments.

Datu šifrēšana	Apstrādātājs	Hostinga administrēšanai un rezerves kopiju pārsūtīšanai izmanto šifrētus savienojumus.
Datu integritāte	Apstrādātājs	Apstrādātājs uztur pamatserverus un Vadības paneli, piemēro riskos balstītus drošības atjauninājumus, ugunsdmūru un tīkla piekļuves ierobežojumus.
Uzraudzība	Apstrādātājs	Apstrādātājs nodrošina tehnisko uzraudzību, attiecīgos drošības žurnālfailus un incidentu novēršanas pasākumus.

Apstrādātājs periodiski izvērtē pasākumu efektivitāti un nepieciešamo atjaunošanas spēju atbilstoši apstrādes riskiem. Pasākumus var atjaunināt, būtiski nesamazinot kopējo aizsardzības līmeni; būtiskas saskaņotās apstrādes izmaiņas veic tikai ar nepieciešamo atļauju.

5. Apstrādātāja pienākumi

Konfidencialitāte

Apstrādātājs nodrošina, ka visas personas, kurām ir piekļuve personas datiem (tostarp darbinieki, līgumslēdzēji un citas pilnvarotas personas), ir saistītas ar līgumisku vai likumā noteiktu konfidencialitātes pienākumu. Šis pienākums turpinās arī pēc pilnvarojuma, sadarbības vai Līguma izbeigšanas. Piekļuvi piešķir tikai pienākumu izpildei nepieciešamajā apjomā.

Sadarbība

Apstrādātājs sadarbojas ar Pārziņi personas datu aizsardzības pārkāpumu ierobežošanā un novēršanā un veic atbilstošus pasākumus.

Datu subjektu pieprasījumi

Apstrādātājs palīdz Pārziņim izpildīt Datu subjektu pieprasījumus saskaņā ar Regulas 3. nodaļu, ņemot vērā apstrādes raksturu un izmantojot atbilstošus pasākumus, ciktāl tas iespējams. Tas ietver datu izgūšanas nodrošināšanu un nepieciešamo tehnisko palīdzību. Ja Datu subjekts vērsas tieši pie Apstrādātāja par Klienta datiem, pieprasījumu bez nepamatotas kavēšanās pārsūta Pārziņim un pēc

Data Encryption	Processor	Hosting administration and backup transfers use encrypted connections.
Data Integrity	Processor	The Processor maintains host systems and the Control Panel, applying risk-based security updates, firewalls and network-access restrictions.
Monitoring	Processor	The Processor applies technical monitoring, relevant security logs and incident-response measures.

The Processor periodically evaluates the effectiveness of the measures and the necessary restoration capability according to the processing risks. Measures may be updated without materially reducing the overall level of protection; material changes to agreed processing require the necessary authorization.

5. Obligations of the Processor

Confidentiality

The Processor ensures that all persons authorized to access personal data (including employees, contractors, and other authorized persons) are bound by contractual or statutory confidentiality obligations. This obligation continues after the termination of their authorization, engagement or the Agreement. Access shall be limited to what their duties require.

Cooperation

The Processor shall cooperate with the Controller in containing and remedying personal data breaches and shall take appropriate measures.

Data Subject Requests

The Processor assists the Controller in fulfilling Data Subject requests pursuant to Chapter III of the Regulation, taking account of the nature of processing and using appropriate measures insofar as possible. This includes enabling data retrieval and providing necessary technical assistance. If a Data Subject contacts the Processor directly concerning Customer data, the request shall be forwarded to the

būtības atbild tikai ar pilnvarojumu vai ja to pieprasa normatīvie akti.

Atbilstības nodrošināšana

Apstrādātājs, ņemot vērā apstrādes raksturu un pieejamo informāciju, palīdz Pārzinim nodrošināt atbilstību Regulas 32. līdz 36. pantā noteiktajām prasībām, tostarp attiecībā uz drošību, pārkāpumu paziņošanu, ietekmes uz datu aizsardzību novērtējumu un iepriekšēju apspriešanos.

Pārkāpumu paziņošana

Apstrādātājs bez nepamatotas kavēšanās informē Pārzini, ja tas uzzina par personas datu aizsardzības pārkāpumu, sniedzot pieejamo informāciju par pārkāpuma raksturu, skartajiem datiem un personām, iespējamām sekām, veiktajiem pasākumiem un kontaktpersonu. Ja nepieciešams, informāciju papildina pakāpeniski. Pārzinis atbild par saviem paziņojumiem iestādēm un Datu subjektiem; tas neskar Apstrādātāja patstāvīgos likumiskos pienākumus.

6. Apstiprinātie apakšapstrādātāji

Pārzinis piešķir vispārēju rakstisku atļauju Apstrādātājam piesaistīt šādus apakšapstrādātājus personas datu apstrādei, ievērojot šajā Līgumā noteikto kārtību.

Apakšapstrādātājs	Apstrādes apraksts
Hetzner Online GmbH	Serveru un infrastruktūras pakalpojumu sniedzējs Vācijā.
Hetzner Finland Oy	Hetzner Online GmbH iesaistīts datu centra un infrastruktūras pakalpojumu sniedzējs, ja tiek izmantota infrastruktūra Somijā.
Hetzner US LLC	Hetzner Online GmbH iesaistīts serveru nomas pakalpojumu sniedzējs, ja tiek izmantota infrastruktūra Amerikas Savienotajās Valstīs.
NTT Global Data Centers Americas Inc.	Hetzner Online GmbH iesaistīts serveru izvietojanas datu centrā pakalpojumu sniedzējs, ja tiek izmantota infrastruktūra Amerikas Savienotajās Valstīs.
QTS Investment Properties Hillsboro LLC	Hetzner Online GmbH iesaistīts serveru izvietojanas datu centrā pakalpojumu sniedzējs, ja tiek izmantota infrastruktūra Amerikas Savienotajās Valstīs.

Controller without undue delay; substantive responses require authorization or a legal duty.

Compliance Assistance

Taking into account the nature of the processing and the information available, the Processor shall assist the Controller in ensuring compliance with the obligations set out in Articles 32 to 36 of the Regulation, including security, breach notification, data protection impact assessments, and prior consultation.

Breach Reporting

The Processor shall notify the Controller without undue delay upon becoming aware of a personal data breach, providing available information about its nature, affected data and individuals, likely consequences, response measures, and a contact. Information may be supplemented in stages where necessary. The Controller remains responsible for its notifications to authorities and Data Subjects, without affecting the Processor's separate statutory duties.

6. Approved Sub-processors

The Controller provides general written authorization for the Processor to engage the following sub-processors for the processing of personal data, subject to the conditions set out in this Agreement.

Sub-processor	Description of Processing
Hetzner Online GmbH	Server and infrastructure service provider in Germany.
Hetzner Finland Oy	Data center and infrastructure service provider engaged by Hetzner Online GmbH where infrastructure in Finland is used.
Hetzner US LLC	Server rental provider engaged by Hetzner Online GmbH where infrastructure in the United States is used.
NTT Global Data Centers Americas Inc.	Colocation provider engaged by Hetzner Online GmbH where infrastructure in the United States is used.
QTS Investment Properties Hillsboro LLC	Colocation provider engaged by Hetzner Online GmbH where infrastructure in the United States is used.

Hetzner Singapore Pte LTD	Hetzner Online GmbH iesaistīts serveru nomas pakalpojumu sniedzējs, ja tiek izmantota infrastruktūra Singapurā.
NTT Global Data Centers SG1 Pte LTD	Hetzner Online GmbH iesaistīts serveru izvietojuma datu centrā pakalpojumu sniedzējs, ja tiek izmantota infrastruktūra Singapurā.
Backblaze Inc.	Amerikas Savienoto Valstu pakalpojumu sniedzējs B2 rezerves kopiju glabāšanai EU-Central reģionā Amsterdamā, Nīderlandē.
Interxion Netherlands B.V.	Backblaze klientu failu apstrādes ķēdē iesaistīts datu centra pakalpojumu sniedzējs Amsterdamā, Nīderlandē.
Datastax Inc.	Backblaze klientu failu apstrādes ķēdē attiecīgajām funkcijām iesaistīts datubāzes konsultāciju sniedzējs Amerikas Savienotajās Valstīs.
Rookout Inc.	Backblaze klientu failu apstrādes ķēdē attiecīgajām funkcijām iesaistīts sistēmu atklāšanas pakalpojumu sniedzējs Amerikas Savienotajās Valstīs.
Cloudflare Inc.	Amerikas Savienoto Valstu pakalpojumu sniedzējs pilnvarotai DNS pārvaldībai un, tikai ja ieslēgtas attiecīgās funkcijas, starpniekservera, satura piegādes un drošības apstrādei globālajā tīklā.

Hetzner Singapore Pte LTD	Server rental provider engaged by Hetzner Online GmbH where infrastructure in Singapore is used.
NTT Global Data Centers SG1 Pte LTD	Colocation provider engaged by Hetzner Online GmbH where infrastructure in Singapore is used.
Backblaze Inc.	United States provider of B2 backup storage in the EU-Central region in Amsterdam, Netherlands.
Interxion Netherlands B.V.	Data center service provider in Amsterdam, Netherlands, within Backblaze's Customer Files processing chain.
Datastax Inc.	United States database consulting provider for the relevant functions within Backblaze's Customer Files processing chain.
Rookout Inc.	United States system debugging provider for the relevant functions within Backblaze's Customer Files processing chain.
Cloudflare Inc.	United States provider of authorized DNS management and, only when the relevant functions are enabled, proxy, content-delivery, and security processing through its global network.

Ja Cloudflare tiek izmantots tikai DNS pakalpojumiem, tīmekļa vietnes datplūsma netiek pārsūtīta caur Cloudflare starpniekserveri. Apstrādātājs nodrošina Pārzinim aktuālu informāciju par iesaistīto apstrādes ķēdes dalībnieku identitāti, adresēm, kontaktinformāciju, funkcijām, atrašanās vietām un garantijām, kā arī sniedz atjauninājumus.

Apstrādātājs nodrošina, ka apakšapstrādātājiem ar līgumu tiek noteikti tādi paši datu aizsardzības pienākumi kā šajā Līgumā, tostarp atbilstošas drošības garantijas, un paliek pilnībā atbildīgs Pārzinim par šo pienākumu izpildi.

Apstrādātājs informē Pārzini par plānotu apakšapstrādātāja pievienošanu vai aizstāšanu vismaz 14 kalendāra dienas pirms attiecīgās apstrādes sākšanas, nosūtot paziņojumu uz Pārziņa reģistrēto e-pasta adresi un sniedzot informētām iebildumam nepieciešamo informāciju.

Where Cloudflare is used only for DNS services, website traffic is not routed through Cloudflare's proxy. The Processor shall provide and keep updated the identities, addresses, contact details, functions, locations, and safeguards of the engaged processing-chain providers.

The Processor ensures that sub-processors are contractually bound by the same data protection obligations as set out in this Agreement, including appropriate security guarantees, and remains fully liable to the Controller for the performance of those obligations.

The Processor informs the Controller of any intended addition or replacement of a sub-processor at least 14 calendar days before the relevant processing begins, by sending a notice to the Controller's registered email address and providing sufficient information for an informed objection.

Ja Pārzinis šajā termiņā pamatotu datu aizsardzības iemeslu dēļ iebilst pret jaunu apakšapstrādātāju un Puses nespēj panākt vienošanos sarunu ceļā, Pārzinim ir tiesības izbeigt skarto Pakalpojumu pirms apstrīdētās apstrādes sākšanas, saņemot samērīgu neizmantotās priekšapmaksas atmaksu. Tas neierobežo citas obligātās tiesības. Ja savlaicīgs iebildums nav saņemts, apstrādi var sākt vispārējās atļaujas ietvaros.

7. Pārbaudes un audita tiesības

Apstrādātājs sniedz visu informāciju, kas nepieciešama Regulas 28. pantā noteikto pienākumu izpildes apliecināšanai, un pieļauj un palīdz veikt Pārziņa vai tā pilnvarota auditora nepieciešamos auditus, tostarp pārbaudes, saskaņā ar Regulas 28. panta 3. punkta h) apakšpunktu. Vispirms parasti izmanto standarta dokumentāciju, rakstiskas atbildes un attiecīgo apakšapstrādātāju pieejamos audita pārskatus un sertifikātus. Šāda informācija neaizstāj turpmāku pārbaudi, ja tā ir nepieciešama.

Auditu veic samērīgi, ar saprātīgu iepriekšēju paziņojumu, darba laikā un ievērojot konfidencialitāti, drošību un citu Klientu datu aizsardzību, izņemot gadījumus, kad apstākļi vai kompetenta iestāde prasa citādi. Šie nosacījumi nedrīkst liegt efektīvu pārbaudi. Par palīdzību, kas būtiski pārsniedz standarta dokumentāciju, Puses var atsevišķi vienoties par samērīgu maksu; tā nedrīkst padarīt likumisko tiesību izmantošanu neiespējamu vai neefektīvu.

8. Datu dzēšana un atdošana

Pēc Pakalpojumu sniegšanas beigām Apstrādātājs pēc Pārziņa izvēles atdod vai dzēš visus personas datus un dzēš esošās kopijas, izņemot glabāšanu, ko pieprasa Savienības vai dalībvalsts tiesību akti.

Ja nav agrāka tiesiska Pārziņa norādījuma, piemēro Noteikumu 9. nodaļā noteikto datu izgūšanas kārtību. Parasti dati izgūšanai ir pieejami 14 kalendāra dienas pēc Pakalpojumu izbeigšanas. Piemērojamās Pakalpojumu sniedzēja maiņas gadījumā tos saglabā izgūšanai vismaz 30 kalendāra dienas pēc pārejas perioda beigām vai ilgāk, ja tas saskaņots vai nepieciešams saskaņā ar normatīvajiem aktiem. Pēc

If the Controller objects to a new sub-processor on reasonable data protection grounds within that period and the Parties are unable to resolve the objection through negotiation, the Controller shall have the right to terminate the affected Service before the disputed processing begins, receiving a proportionate refund of unused prepaid fees. Other mandatory rights remain unaffected. Without a timely objection, processing may proceed under the general authorization.

7. Inspection and Audit Rights

The Processor shall provide all information necessary to demonstrate compliance with Article 28 of the Regulation and shall allow for and contribute to necessary audits, including inspections, by the Controller or its mandated auditor, in accordance with Article 28(3)(h) of the Regulation. The Parties shall ordinarily begin with standard documentation, written responses, and the available audit reports and certificates of the relevant sub-processors. Such information does not replace further verification where necessary.

Audits shall be proportionate, on reasonable notice, during business hours, and subject to confidentiality, security and the protection of other Customers' data, except where circumstances or a competent authority require otherwise. These arrangements shall not prevent effective verification. The Parties may separately agree reasonable charges for assistance that substantially exceeds standard documentation; such charges shall not prevent or make ineffective the exercise of statutory rights.

8. Deletion and Return of Personal Data

After the conclusion of the Services, the Processor shall, at the Controller's choice, return or delete all personal data and shall delete existing copies, except retention required by Union or Member State law.

Without an earlier lawful instruction from the Controller, the data-retrieval procedures set out in Section 9 of the Terms shall apply. Ordinarily, data remain available for retrieval for 14 calendar days after termination of the Services. For applicable provider switching, data shall remain available for retrieval for at least 30 calendar days after the transition period, or longer where agreed or legally

izgūšanas perioda aktīvos datus dzēš.

Atlikušās rezerves kopijas nošķir no parastās apstrādes un dzēš ne vēlāk kā 30 kalendāra dienās no katras kopijas izveidošanas. Izbeigšana vai izgūšana nesāk jaunu 30 dienu termiņu. Agrākus tiesiskus atdošanas vai dzēšanas norādījumus izpilda arī attiecībā uz kopijām. Atjaunošanas gadījumā dzēšanas norādījumus piemēro atkārtoti. Apstrādātājs nodrošina šo pienākumu izpildi arī pie apakšapstrādātājiem un pēc pieprasījuma apstiprina atdošanas un dzēšanas izpildi.

Likumiski nepieciešamo glabāšanu ierobežo ar tās apjomu, nolūku un ilgumu, informējot Pārziņi, ciktāl to pieļauj normatīvie akti. Līguma noteikumi par datu aizsardzību ir piemērojami līdz datu atdošanai vai dzēšanai.

9. Piemērojamais likums un atbildība

Līguma sastādīšanā ņemti vērā un tam piemērojami spēkā esošie Latvijas Republikas normatīvie akti.

Visi strīdi un nesaskaņas, kas rodas vai var rasties Pakalpojumu izpildes gaitā vai sakarā ar šo Līgumu, vispirms risināmi savstarpēju pārrunu ceļā, ievērojot Noteikumu 13. nodaļā noteikto strīdu risināšanas kārtību un obligātās tiesības.

Šim Līgumam piemērojami Noteikumu 11. nodaļā noteiktie atbildības ierobežojumi tikai tiktāl, ciktāl tie ir tiesiski piemērojami, tostarp tajā noteiktais ierobežojums komercdarbības Klientiem. Tie neierobežo Datu subjektu tiesības saskaņā ar Regulas 82. pantu, uzraudzības iestāžu pilnvaras, obligātās līguma standartklauzulu tiesības vai citus neizslēdzamus pienākumus. Katra Puse paliek atbildīga par tai piemērojamiem likumiskajiem pienākumiem.

10. Citi noteikumi

Apstrādātājam ir tiesības veikt izmaiņas Līgumā, lai nodrošinātu tā atbilstību spēkā esošajiem normatīvajiem aktiem vai atspoguļotu izmaiņas Pakalpojumu sniegšanas procesā, ievērojot Noteikumu 14. nodaļā noteikto kārtību.

required. Active data shall be deleted after the retrieval period.

Remaining backups shall be isolated from ordinary processing and deleted no later than 30 calendar days from each copy's creation. Termination or retrieval does not start a new 30-day period. Earlier lawful return or deletion instructions shall be fulfilled, including for copies. Deletion instructions shall be reapplied following restoration. The Processor shall ensure that sub-processors perform these duties and shall confirm completion of return and deletion on request.

Legally required retention shall be limited to its scope, purpose, and duration, with notice to the Controller where permitted by law. The Agreement's data protection provisions shall continue to apply until data are returned or deleted.

9. Governing Law and Responsibility

This Agreement has been drafted in accordance with and is governed by the applicable laws and regulations of the Republic of Latvia.

All disputes and disagreements arising or that may arise during the execution of the Services or in connection with this Agreement shall first be addressed through mutual negotiations, subject to the dispute-resolution procedures and mandatory rights set out in Section 13 of the Terms.

The limitations of liability set out in Section 11 of the Terms apply to this Agreement only insofar as lawful, including the limitation applicable to business Customers. They do not restrict Data Subject rights under Article 82 of the Regulation, supervisory powers, mandatory standard-contractual-clause rights, or other obligations that cannot be excluded. Each Party remains responsible for its statutory duties.

10. Other Provisions

The Processor shall have the right to make changes to the Agreement in order to ensure its compliance with current laws and regulations or to reflect changes in the provision of Services, in accordance with Section 14 of the Terms.

Par būtiskām izmaiņām Pārzinis tiek informēts Noteikumu 14. nodaļā noteiktajā kārtībā un termiņā. Aktuālā Līguma versija ir pieejama tīmekļa vietnē www.request.host. Apakšapstrādātāju izmaiņām piemēro Līguma 6. nodaļu; saglabā nepieciešamos Pārziņa norādījumus un citus apstrādes priekšnoteikumus.

Pretrunu gadījumā starp Līgumu un Noteikumiem Līguma nosacījumi par datu aizsardzību ir noteicošie. Piemērojamās līguma standartklauzulas ir noteicošas pār pretrunīgiem līguma nosacījumiem.

Šis Līgums ir pieejams Apstrādātāja tīmekļa vietnē arī angļu valodas versijā (www.request.host/data-processing-agreement). Neatbilstību vai pretrunu gadījumā starp latviešu un angļu valodas versijām latviešu valodas versija (www.request.host/lv/datu-apstrades-ligums) būs noteicošā visos aspektos, ievērojot piemērojamo normatīvo aktu obligātās prasības.

Jautājumu gadījumā par Līgumu vai piemērojamajiem noteikumiem par datu aizsardzību ar Apstrādātāju var sazināties, nosūtot vēstuli uz Apstrādātāja juridisko adresi: Stabu iela 109 - 1, Rīga, LV-1009, Latvija vai e-pastā: info@request.host

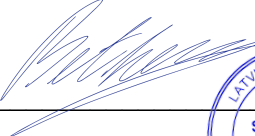
The Controller shall be notified of material changes in accordance with the procedures and notice period set out in Section 14 of the Terms. The current version of the Agreement is available on the website www.request.host. Changes to sub-processors are governed by Section 6 of this Agreement; necessary Controller instructions and other processing prerequisites remain applicable.

In the event of any conflict between the Agreement and the Terms, the Agreement's provisions on data protection shall prevail. Applicable standard contractual clauses shall prevail over conflicting contractual provisions.

This Agreement is also available on the Latvian language version of the Processor's website (www.request.host/lv/datu-apstrades-ligums). In the event of any inconsistency or conflict between the English and Latvian versions, the Latvian version (www.request.host/lv/datu-apstrades-ligums) shall prevail in all respects, subject to the mandatory requirements of applicable law.

In case of any questions regarding the Agreement or the applicable provisions on data protection, the Processor may be contacted by sending a letter to the Processor's legal address: Stabu iela 109 - 1, Riga, LV-1009, Latvia or by email: info@request.host

Apstiprinu:


D. Bethers
Valdes loceklis



Approved:


D. Bethers
Board Member

