

request()

PRIVĀTUMA POLITIKA

Pēdējo reizi atjaunota: 2026. gada 15. oktobrī

1. Privātuma politikas mērķis un piemērošanas joma

SIA Request, vienotais reģistrācijas numurs: 40203423105, juridiskā adrese: Stabu iela 109 - 1, Rīga, LV-1009, Latvija (turpmāk – Pārzinis) Privātuma politikas (turpmāk – Politika) mērķis ir informēt Pārziņa klientus, potenciālos klientus, sadarbības partnerus un citas personas par Pārziņa veiktajām darbībām saistībā ar fizisko personu, kuras var tieši vai netieši identificēt (turpmāk – Datu subjekts) personas datu apstrādi un aizsardzību zīmola request.host ietvaros.

Politikā ir norādīts, kādi Datu subjekta personas dati tiek apstrādāti, t.sk. iegūti, nodoti, laboti, uzglabāti, dzēsti u.tml., šādas datu apstrādes mērķi un tiesiskais pamats saskaņā ar 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), kā arī datu uzglabāšanas termiņi un Datu subjekta tiesības.

Politika ir attiecināma uz fizisko personu datu apstrādi neatkarīgi no tā, kādā formā un/vai vidē Datu subjekts sniedz vai Pārzinis iegūst personas datus (piemēram, Pārziņa tīmekļa vietnē, papīra formātā, mutiski, elektroniski e-pastā vai telefoniski, Pārziņa sociālo tīklu profilos u.tml.).

Pārzinim pēc saviem ieskatiem ir tiesības veikt izmaiņas Politikā. Politika ir pieejama Pārziņa tīmekļa vietnē – www.request.host (turpmāk – Vietne), kā arī birojā un tiek piemērota no Politikas apstiprināšanas datuma.

PRIVACY POLICY

Last updated: October 15, 2026

1. Purpose and Scope of this Privacy Policy

The purpose of this Privacy Policy (hereinafter – the Policy) by SIA Request, registration number: 40203423105, legal address: Stabu iela 109 - 1, Riga, LV-1009, Latvia (hereinafter – the Controller) is to inform the Controller's customers, potential customers, cooperation partners and other persons about the Controller's activities related to the processing and protection of personal data of natural persons who can be directly or indirectly identified (hereinafter – the Data Subject) under the brand request.host.

The Policy specifies what personal data of the Data Subject is processed, including obtained, transferred, corrected, stored, deleted, etc., the purposes of such data processing and the legal basis for such processing in accordance 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), as well as the data retention periods and the rights of the Data Subject.

The Policy shall apply to the processing of personal data regardless of the form and/or medium in which the Data Subject provides or the Controller obtains the personal data (e.g. on the website of the Controller, in writing, orally, electronically by email or telephone, on the Controller's social network profiles, etc.).

The Controller shall have the right to make changes to the Policy at its sole discretion. The Policy is available on the Controller's website – www.request.host (hereinafter – the Website), as well as at the office and is applicable from the date of approval of the Policy.

Politika attiecas uz Pārziņa paša vajadzībām veikto kontu, norēķinu, atbalsta, saziņas, drošības un Vietnes datu apstrādi, tostarp klientu portālā www.accounts.request.host un hostinga vadības panelī www.console.request.host.

2. Informācija par pārzini

Datu apstrādes pārzinis ir SIA Request (turpmāk – Request), vienotais reģistrācijas numurs: 40203423105, juridiskā adrese: Stabu iela 109 - 1, Rīga, LV-1009, Latvija, e-pasta adrese: info@request.host

Šajā punktā norādīto kontaktinformāciju var izmantot jautājumiem par personas datu apstrādi un Datu subjekta tiesību īstenošanu.

3. Personas datu kategorijas, datu subjektu kategorijas, apstrādes mērķi un tiesiskais pamats

Pārzinis parasti apstrādā šādu Datu subjektu personas datus:

- Klienti un to pārstāvji;
- Potenciālie klienti un to pārstāvji;
- Sadarbības partneri un to pārstāvji;
- Vietnes apmeklētāji, kontu lietotāji un citas personas, kas sazinās ar Pārzini.

Pārzinis apstrādā fizisko personu datus likumīgi, godprātīgi un Datu subjektam pārredzamā veidā, lai:

- Sniegtu hostinga un infrastruktūras pakalpojumus klientiem;
- Nodrošinātu un uzlabotu Pārziņa sniegto pakalpojumu kvalitāti;
- Izpildītu uz Pārzini likumā attiecināmus pienākumus;
- Aizsargātu savas un Datu subjekta legītīmās intereses.

Pārziņa legītīmās intereses ir: veikt un administrēt komercdarbību un attiecības ar uzņēmumu klientiem un to pārstāvjiem, saņemt maksājumus, nodrošināt pakalpojumu kvalitāti un drošību, novērst ļaunprātīgu vai nelikumīgu pakalpojumu izmantošanu un aizsargāt tiesības un tiesiskās intereses. Pārzinis

The Policy concerns the Controller's own account, billing, support, communication, security and Website processing, including in the customer portal at www.accounts.request.host and the hosting control panel www.console.request.host.

2. Information About the Controller

The Controller is SIA Request (hereinafter – Request), registration number: 40203423105, legal address: Stabu iela 109 - 1, Riga, LV-1009, Latvia, email address: info@request.host

The contact details in this Section may be used for privacy enquiries and the exercise of Data Subject rights.

3. Categories of Personal Data, Categories of Data Subjects, Purposes of Processing and Legal Basis

The Controller will normally process the personal data of the following Data Subjects:

- Customers and their representatives;
- Potential customers and their representatives;
- Cooperation partners and their representatives;
- Website visitors, account users and other persons communicating with the Controller.

The Controller shall process the data of natural persons lawfully, fairly and in a manner that is transparent to the Data Subject in order to:

- Provide hosting and infrastructure services to customers;
- Ensure and improve the quality of the services provided by the Controller;
- Comply with the obligations imposed on the Controller by law;
- Protect the Controller's legitimate interests and the legitimate interests of the Data Subject.

The legitimate interests of the Controller are: to carry out and administer its business activities and relationships with business customers and their representatives, receive payments, ensure service quality and security, prevent abuse or unlawful use of services, and protect legal rights and interests. The

izvērtē apstrādes nepieciešamību un samēro šīs intereses ar Datu subjekta tiesībām un pamatotām gaidām.

Pārzinis parasti veic šādu personas datu kategoriju apstrādi:

- Personas vārds, uzvārds, profesionālā loma un pārstāvības informācija;
- Adrese, tālruna numurs, e-pasta adrese un uzņēmuma kontaktinformācija;
- Bankas konta un nodokļu informācija, nodokļu pārbaudes, maksājumu un darījumu atsauces, statuss un ierobežota kartes informācija;
- Pasūtījumu, abonementu un norēķinu dati, kā arī iegūtie un saglabātie līgumiskie apliecinājumi;
- Konta un organizācijas identifikatori, dalība, piekļuves tiesības un profila attēls;
- Saziņa un atbalsta pieprasījumi;
- IP adreses, ierīces vai pārlūkprogrammas informācija, piekļuves žurnāli un cita tehniskā informācija, kas nepieciešama pakalpojumu sniegšanai un uzturēšanai.

Personas identifikācijas datus pieprasa tikai tad, ja tie nepieciešami konkrētam pamatotam mērķim.

Pārziņa īstenotās fizisku personu datu apstrādes tiesiskais pamats var būt:

- Regulas 6. panta 1. punkta a) apakšpunkts, kas nosaka, ka datu apstrāde ir likumīga, ja Datu subjekts ir devis piekrišanu savu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem;
- Regulas 6. panta 1. punkta b) apakšpunkts, kas nosaka, ka datu apstrāde ir likumīga, ja apstrāde ir vajadzīga līguma, kura līgumslēdzēja puse ir Datu subjekts, izpildei vai pasākumu veikšanai pēc Datu subjekta pieprasījuma pirms līguma noslēgšanas;
- Regulas 6. panta 1. punkta c) apakšpunkts, kas nosaka, ka datu apstrāde ir likumīga, ja apstrāde ir vajadzīga, lai izpildītu uz Pārzini attiecināmu juridisku pienākumu;
- Regulas 6. panta 1. punkta f) apakšpunkts, kas nosaka, ka datu apstrāde ir likumīga, ja apstrāde ir vajadzīga Pārziņa vai trešās personas leģitīmo

Controller assesses necessity and balances these interests against the Data Subject's rights and reasonable expectations.

The Controller will normally process the following categories of personal data:

- Name, surname, professional role and authority to act;
- Address, telephone number, email address and company contact information;
- Bank-account and tax information, tax checks, payment and transaction references, status and limited card information;
- Order, subscription and billing information, and contractual confirmations obtained and retained;
- Account and organization identifiers, memberships, permissions and profile image;
- Correspondence and support requests;
- IP addresses, device or browser information, access logs and other technical information necessary for providing and maintaining the services.

Personal identification information is requested only where necessary for a justified purpose.

The legal basis for the processing of natural persons' data by the Controller may be:

- Article 6(1)(a) of the Regulation, which states that processing is lawful if the Data Subject has given his or her consent to the processing of his or her personal data for one or more specified purposes;
- Article 6(1)(b) of the Regulation, which states that processing is lawful if the processing is necessary for the performance of a contract to which the Data Subject is a party or for taking measures at the request of the Data Subject prior to entering into the contract;
- Article 6(1)(c) of the Regulation, which states that processing is lawful if the processing is necessary for compliance with a legal obligation to which the Controller is subject;
- Article 6(1)(f) of the Regulation, which states that processing is lawful if the processing is necessary for the pursuit of the legitimate

interēšu ievērošanai, izņemot, ja Datu subjekta intereses vai pamattiesības un pamatbrīvības, kurām nepieciešama personas datu aizsardzība, ir svarīgākas par šādām interesēm, jo īpaši, ja Datu subjekts ir bērns.

Pārzinis veic identitātes, kontaktinformācijas, konta un pasūtījumu datu apstrādi ar mērķi izskatīt pieprasījumus, sagatavot piedāvājumus un noslēgt vai izpildīt līgumu ar fizisku personu, pamatojoties uz Regulas 6. panta 1. punkta b) apakšpunktu. Uzņēmumu klientu un partneru pārstāvju saziņa un attiecību administrēšana balstās uz Regulas 6. panta 1. punkta f) apakšpunktu.

Maksājumu, abonementu, atmaksu, atbalsta un nepieciešamo pakalpojumu paziņojumu administrēšana balstās uz Regulas 6. panta 1. punkta b) apakšpunktu fiziskas personas līgumam vai f) apakšpunktu uzņēmumu attiecību un finanšu interēšu aizsardzībai. Rēķinus, grāmatvedības un nodokļu datus apstrādā, izpildot juridiskus pienākumus saskaņā ar Regulas 6. panta 1. punkta c) apakšpunktu. Sistēmu aizsardzība, ļaunprātīgas izmantošanas un incidentu izmeklēšana un prasījumu aizstāvība balstās uz f) apakšpunktu vai c) apakšpunktu, ja apstrādi prasa likums.

Izvēles mārketinga saziņa un nebūtiskas tehnoloģijas, kuru izmantošanai nepieciešama piekrišana, balstās uz Regulas 6. panta 1. punkta a) apakšpunktu, ievērojot arī elektroniskās saziņas noteikumus. Nepieciešamie konta, norēķinu un drošības paziņojumi nav atkarīgi no piekrišanas mārketingam.

Datus iegūst no Datu subjekta, tā pārstāvētā klienta vai organizācijas, pilnvarotām kontaktpersonām, attiecīgiem publiskiem uzņēmumu vai nodokļu reģistriem un pakalpojumu nodrošināšanā iesaistītajām sistēmām un sniedzējiem. Tehniskie dati rodas arī pakalpojumu izmantošanas laikā.

Maksājumu kartes datus apstrādā Stripe LLC grupas uzņēmumi (turpmāk – Stripe) integrētajā maksājumu saskarnē. Pārzinis nodod Stripe nepieciešamo maksātāja vārdu vai nosaukumu, kontaktpersonas vārdu, e-pastu, adresi un darījuma informāciju, un apstrādā maksājumu atsauces, statusu un ierobežotu kartes informāciju, piemēram, pēdējos četrus ciparus un derīguma termiņu. Pārzinis neglabā pilnu kartes numuru vai drošības kodu.

interests of the Controller or of a third party, except where the interests or fundamental rights and freedoms of the Data Subject which require the protection of personal data override such interests, in particular where the Data Subject is a child.

The Controller shall process identity, contact, account and order data to assess enquiries, prepare offers and enter into or perform an individual's contract on the basis of Article 6(1)(b) of the Regulation. Communication with business customers' or partners' representatives and administration of those relationships is based on Article 6(1)(f) of the Regulation.

Administration of payments, subscriptions, refunds, support and necessary service notices is based on Article 6(1)(b) of the Regulation for an individual's contract or Article 6(1)(f) for business relationships and legitimate financial interests. Invoicing, accounting and tax data is processed to comply with legal obligations under Article 6(1)(c). System protection, investigations of misuse and incidents, and the defence of claims rely on Article 6(1)(f) or Article 6(1)(c) where required by law.

Optional marketing communications and non-essential technologies requiring consent are based on Article 6(1)(a) of the Regulation, also subject to electronic-communications rules. Necessary account, billing and security notices do not depend on marketing consent.

Information comes from the Data Subject, the customer or organization represented, authorized contacts, relevant public business or tax registers, and systems and providers involved in delivering services. Technical data is also generated through use of the services.

Card details are processed by Stripe LLC group companies (hereinafter – Stripe) through the integrated payment interface. The Controller supplies necessary buyer names, contact names, email, address and transaction information, and processes payment references, status and limited card details such as the last four digits and expiry date. The Controller does not store the full card number or security code.

Nepieciešamo līguma vai rēķina datu nesniegšana var liegt noslēgt vai izpildīt līgumu. Tehniskie, piekļuves un maksājumu kontroles pasākumi var darboties automātiski. Ja šāds pasākums rada strīdīgu ierobežojumu, Datu subjekts var sazināties ar Pārziņi, lai pārskatītu apstākļus un noskaidrotu turpmāko rīcību, tostarp attiecībā uz maksājumu sniedzēju. Regulas 22. pantā paredzētās tiesības ir piemērojamas, ja izpildās tā nosacījumi.

Attiecībā uz personas datiem, kurus klients izvieto un apstrādā Pārziņa nodrošinātajos serveros un infrastruktūrā, Pārziņis darbojas kā apstrādātājs vai apakšapstrādātājs atbilstoši klienta norādījumiem. Šādu datu apstrādi neregulē šī Politika, bet gan atsevišķs Datu apstrādes līgums, kas pieejams Pārziņa tīmekļa vietnē (www.request.host/lv/datustrades-ligums). Pieprasījumi par klienta veikto šādu datu apstrādi parasti adresējami klientam.

4. Personas datu uzglabāšanas termiņš

Pārziņis glabā personas datus tikai tik ilgi, cik nepieciešams attiecīgajam mērķim vai juridiska pienākuma izpildei. Konta un klienta administrēšanas datus glabā attiecību laikā un nepieciešamo slēgšanas darbību pabeigšanai. Rēķinus, darījumu un nodokļu pierādījumus glabā attiecīgajai grāmatvedības vai nodokļu dokumentu kategorijai noteikto likumisko termiņu.

Saziņu un atbalsta ierakstus glabā pieprasījuma atrisināšanai un nepieciešamo līgumisko pierādījumu saglabāšanai. Piekļuves un drošības žurnālus glabā atbilstoši kļūmju, ļaunprātīgas izmantošanas vai incidentu izmeklēšanas vajadzībām un riskam. Detalizētus maksājumu sistēmu paziņojumus un diagnostikas datus glabā tikai nepieciešamajai maksājumu salāgošanai, problēmu izmeklēšanai vai pierādījumiem, ierobežojot piekļuvi un dzēšot vai aizklājot nevajadzīgās detaļas.

Piekrišanas un iebildumu ierakstus glabā, ciktāl nepieciešams apliecināt atbilstību un ievērot saziņas izvēles. Prasījumu pierādījumus glabā piemērojamajā noilguma termiņā vai līdz procesa pabeigšanai. Nevajadzīgos datus dzēš vai anonimizē; ierobežoti pieejamas rezerves kopijas dzēš to glabāšanas cikla ietvaros. Klienta izvietoto datu atdošanu, dzēšanu un rezerves kopijas regulē Lietošanas noteikumi un Datu apstrādes līgums.

Failure to supply necessary contractual or invoicing information may prevent a contract being entered into or performed. Technical, access and payment controls may operate automatically. If a control results in a disputed restriction, the Data Subject may contact the Controller to review the circumstances and establish the appropriate resolution, including with a payment provider. Article 22 rights apply where its conditions are met.

Regarding personal data that a customer hosts and processes on the servers and infrastructure provided by the Controller, the Controller acts as a processor or subprocessor under the customer's instructions. Such processing is governed by a separate Data Processing Agreement, rather than this Policy, available on the Controller's website (www.request.host/data-processing-agreement). Requests about the customer's use of that data should normally be addressed to the customer.

4. Duration of Storage of Personal Data

The Controller retains personal data only as long as necessary for the relevant purpose or legal obligation. Account and customer-administration data is retained during the relationship and necessary closure tasks. Invoices, transaction and tax evidence are retained for the statutory period applicable to the relevant accounting or tax document category.

Correspondence and support records are retained to resolve the matter and preserve necessary contractual evidence. Access and security logs are retained according to fault, misuse or incident investigation needs and risk. Detailed payment-system messages and diagnostics are retained only for necessary reconciliation, investigation or evidence, with restricted access and removal or redaction of unnecessary detail.

Consent and objection records are retained as necessary to demonstrate compliance and respect communication choices. Claim evidence is retained for the applicable limitation period or until proceedings conclude. Unneeded data is deleted or anonymized; restricted backup copies expire through their retention cycle. Customer-hosted data, its return, deletion and backups are governed by the Terms of Service and Data Processing Agreement.

5. Personas datu nodošana ārpus Eiropas Savienības vai Eiropas Ekonomikas zonas valstīm

Pārziņa apstrādātie personas dati var tikt nodoti pakalpojumu sniedzējiem, kas tos apstrādā Eiropas Savienībā, Eiropas Ekonomikas zonā (EEZ) vai ārpus tās, tostarp ASV. Servera vai rezerves kopijas atrašanās EEZ pati par sevi nenozīmē, ka arī visi saistītie konta, maksājumu, saziņas, atbalsta vai uzraudzības dati tiek apstrādāti tikai EEZ.

Nodošanai piemēro Regulas V nodaļas prasības, izmantojot attiecīgu lēmumu par aizsardzības līmeņa pietiekamību vai atbilstošas garantijas, tostarp Eiropas Komisijas standarta līguma klauzulas un nepieciešamos papildu pasākumus. ES un ASV datu privātuma regulējumu izmanto tikai aptvertam sertificētam saņēmējam un apstrādei. Informāciju par saņēmēju valstīm un piemērotajām garantijām, tostarp šo garantiju kopijas, var pieprasīt Pārzinim, ievērojot piemērojamos konfidencialitātes ierobežojumus. Noteikumu pieņemšana vai reģiona izvēle nav vispārēja piekrišana datu nodošanai.

6. Personas datu saņēmēju kategorijas

Fiziskās personas dati, ja tam ir tiesisks pamats un ciktāl tas nepieciešams attiecīgajam mērķim, var tikt nodoti iestādēm un tiesām, bankām un maksājumu sniedzējiem, profesionālajiem konsultantiem, Pārziņa saziņas, dokumentu, grāmatvedības un citas nepieciešamās programmatūras un tehniskā atbalsta sniedzējiem, infrastruktūras, rezerves kopiju, tīkla un drošības sniedzējiem, pakalpojumu uzraudzības un tehnisko žurnālu sniedzējiem, un e-pasta piegādes sniedzējiem. Vietnes analītikas un reklāmas sniedzējiem datus nodod, ja ir atļauta attiecīgo tehnoloģiju izmantošana.

Personas datiem var piekļūt arī pilnvarots personāls, kam tie nepieciešami attiecīgā uzdevuma izpildei.

Apstrādātājus piesaista ar atbilstošiem datu aizsardzības un konfidencialitātes nosacījumiem. Stripe darbojas kā apstrādātājs noteiktiem Pārziņa uzdevumā sniegtiem pakalpojumiem un kā pārzinis paša noteiktiem mērķiem, tostarp krāpšanas novēršanai un juridisko pienākumu izpildei. Plašāka informācija: www.stripe.com/legal/privacy-center. Klienta izvietoto datu apakšapstrādātājus norāda Datu apstrādes līgumā. Saņēmēja piederība

5. Transfer of Personal Data Outside the European Union or the European Economic Area

Personal data processed by the Controller may be transferred to service providers processing it within or outside the European Union or European Economic Area (EEA), including in the United States. EEA server or backup storage does not by itself mean that all associated account, payment, communication, support or monitoring data is processed exclusively in the EEA.

Transfers comply with Chapter V of the Regulation through an applicable adequacy decision or appropriate safeguards, including European Commission standard contractual clauses and necessary supplementary measures. The EU-US Data Privacy Framework applies only to a covered certified recipient and processing. Information about recipient countries and applicable safeguards, including copies of those safeguards, may be requested from the Controller, subject to applicable confidentiality protections. Accepting terms or selecting a region is not blanket transfer consent.

6. Categories of Recipients of Personal Data

Where there is a legal basis and to the extent necessary for the relevant purpose, personal data may be transferred to authorities and courts, banks and payment providers, professional advisers, the Controller's communication, document, accounting and other necessary software and technical-support providers, infrastructure, backup, network and security providers, service-monitoring and technical-log providers, and email-delivery providers. Website analytics and advertising providers receive data where the use of the relevant technologies has been permitted.

Personal data may also be accessed by authorized personnel requiring it for the relevant task.

Processors are engaged under appropriate data-protection and confidentiality arrangements. Stripe acts as a processor for certain services supplied on the Controller's behalf and as a controller for its own purposes, including fraud prevention and legal compliance. Further information: www.stripe.com/legal/privacy-center. Subprocessors for customer-hosted data are identified in the Data

uzskaitītai kategorijai pati par sevi neattaisno datu izpaušanu.

7. Personas datu apstrādes drošība

Pārzinis nodrošina, ka personas dati tiek apstrādāti tādā veidā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus.

Šie riskam atbilstošie pasākumi ietver piekļuves ierobežojumus, autentifikāciju, drošu saziņu, sistēmu uzturēšanu, konfidencialitāti un atbilstošu rezerves kopiju un incidentu apstrādes kārtību. Piekļuvi piešķir tikai personām un sniedzējiem, kam tā nepieciešama pilnvarotam mērķim.

Pasākumus izvērtē atbilstoši datiem, sistēmām un riskiem. Neviena glabāšanas vai nosūtīšanas metode nav pilnīgi brīva no riska; tas neierobežo Pārziņa datu aizsardzības pienākumus.

8. Datu subjekta piekļuve personas datiem

Datu subjektam ir tiesības saņemt no Pārziņa apstiprinājumu par to, vai attiecībā uz Datu subjektu tiek vai netiek apstrādāti personas dati, un, ja tiek, Datu subjektam ir tiesības piekļūt attiecīgajiem datiem un saņemt Regulas 15. panta 1. punktā norādīto informāciju.

Datu subjektam ir tiesības prasīt, lai Pārzinis bez nepamatotas kavēšanās labotu neprecīzus Datu subjekta personas datus. Ņemot vērā apstrādes nolūkus, Datu subjektam ir tiesības panākt, lai nepilnīgi personas dati tiktu papildināti, tostarp sniedzot papildu paziņojumu.

Datu subjektam saskaņā ar Regulas 17. panta noteikumiem ir tiesības panākt, lai Pārzinis bez nepamatotas kavēšanās dzēstu Datu subjekta personas datus, ja pastāv kāds no minētajā pantā norādītajiem apstākļiem.

Datu subjektam ir tiesības panākt, lai Pārzinis ierobežotu apstrādi, ja pastāv kāds no Regulas 18. pantā norādītajiem apstākļiem.

Processing Agreement. Membership of a listed recipient category does not itself justify disclosure.

7. Security of Processing of Personal Data

The Controller shall ensure that personal data is processed in such a way as to ensure appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, by means of appropriate technical or organizational measures.

These risk-appropriate measures include access restrictions, authentication, secure communication, system maintenance, confidentiality and appropriate backup and incident-handling arrangements. Access is limited to people and providers requiring it for an authorized purpose.

Measures are reviewed in light of the data, systems and risks. No storage or transmission method is entirely risk-free; this does not limit the Controller's data-protection obligations.

8. Data Subject's Access to Personal Data

The Data Subject shall have the right to obtain confirmation from the Controller as to whether or not personal data is being processed in relation to the Data Subject and, if so, the Data Subject shall have the right to access the relevant data and to obtain the information referred to in Article 15(1) of the Regulation.

The Data Subject shall have the right to request that the Controller rectifies inaccurate personal data of the Data Subject without undue delay. Taking into account the purposes of the processing, the Data Subject shall have the right to have incomplete personal data completed, including by providing a supplementary statement.

The Data Subject shall have the right, in accordance with the provisions of Article 17 of the Regulation, to obtain the erasure of personal data concerning him or her by the Controller without undue delay where one of the circumstances specified in that Article applies.

The Data Subject shall have the right to obtain restriction of processing by the Controller where one of the circumstances specified in Article 18 of the Regulation applies.

Datu subjektam Regulas 20. pantā noteiktajos gadījumos ir tiesības saņemt Pārzinim sniegtos personas datus strukturētā, plaši izmantotā un mašīnlasāmā formātā un tos nodot citam pārzinim. Ja tas ir tehniski iespējams, Datu subjekts var panākt šo datu tiešu nodošanu no Pārziņa citam pārzinim. Šīs tiesības attiecas uz automatizētu apstrādi, kas balstās uz piekrišanu vai līgumu.

Datu subjektam ir tiesības iebilst pret leģitīmajās interesēs balstītu apstrādi savas konkrētās situācijas dēļ. Pārzinis šādu apstrādi pārtrauc, ja nepastāv piemērojami svarīgāki pamati vai nepieciešamība celt, īstenot vai aizstāvēt prasījumus. Pret tiešo mārketingu Datu subjekts var iebilst jebkurā laikā bez pamatojuma.

Datu subjektam ir tiesības atsaukt savu piekrišanu savu personas datu apstrādei, ja tāda tikusi sniegta. Piekrišanas atsaukšana neietekmē pirms atsaukšanas veiktās apstrādes likumību.

Pieejamos personiskā konta datus var mainīt hostinga vadības panelī (www.console.request.host); norēķinu informācijas labošanai Datu subjekts var sazināties ar Pārzini.

Lai atvieglotu un sekmētu Datu subjekta pieprasījumu apstrādi, Datu subjekts var vērsties pie Pārziņa rakstveidā, tostarp parastā e-pastā vai pa pastu, izmantojot Politikas 2. punktā norādīto kontaktinformāciju. Paraksts vai personu apliecinošs dokuments nav automātiski nepieciešams; samērīgu papildu pārbaudi var pieprasīt pamatotu šaubu gadījumā par identitāti.

Atbildi sniedz bez nepamatotas kavēšanās, parasti viena mēneša laikā. Regulas atļautos gadījumos termiņu var pagarināt līdz diviem papildu mēnešiem, pirmajā mēnesī paziņojot iemeslus. Pieprasījumi parasti ir bez maksas; likumīgu atteikumu vai maksu pamato.

Datu subjektam ir arī tiesības ar sūdzību vērsties Latvijas Republikas Datu valsts inspekcijā, ja Datu subjekts uzskata, ka Pārzinis aizskar Datu subjekta tiesības un tiesiskās intereses fizisko personu datu aizsardzības jomā. Informācija par sūdzības iesniegšanu ir pieejama tīmekļa vietnē www.dvi.gov.lv. Datu subjekts var vērsties arī citā kompetentā uzraudzības iestādē, tostarp savas

The Data Subject shall have the right, in the circumstances specified in Article 20 of the Regulation, to receive personal data provided to the Controller in a structured, commonly used, machine-readable format and transmit it to another controller. Where technically feasible, the Data Subject may have those data transmitted directly from the Controller to another controller. This right concerns automated processing based on consent or contract.

The Data Subject shall have the right to object to legitimate-interest processing on grounds relating to his or her situation. The Controller shall cease such processing unless applicable overriding grounds or the establishment, exercise or defence of claims justify it. The Data Subject may object to direct marketing at any time without justification.

The Data Subject shall have the right to withdraw his or her consent to the processing of his or her personal data, if such consent has been given. Withdrawal of consent shall not affect the lawfulness of processing before withdrawal.

Available personal account details may be changed via the hosting control panel (www.console.request.host); the Data Subject may contact the Controller to correct billing information.

In order to facilitate the processing of the Data Subject's requests, the Data Subject may contact the Controller in writing, including by ordinary email or post, using the contact details specified in Section 2 of this Policy. A signature or identity document is not automatically required; proportionate additional verification may be requested where identity is reasonably in doubt.

Responses are provided without undue delay, ordinarily within one month. A lawful extension of up to two further months may apply, with reasons notified within the first month. Requests are ordinarily free; any lawful refusal or fee is explained.

The Data Subject shall also have the right to lodge a complaint with the Data State Inspectorate of the Republic of Latvia if the Data Subject considers that the Controller infringes the Data Subject's rights and legitimate interests in the field of data protection of natural persons. Information on submitting a complaint is available at www.dvi.gov.lv/en. The Data Subject may also contact another competent

dzīvesvietas, darba vietas vai iespējamā pārkāpuma dalībvalstī.

9. Sīkdatnes un līdzīgas tehnoloģijas

Klientu portāls un hostinga vadības panelis izmanto autentifikācijai, drošībai, sesijām un lietotāja pieprasītām funkcijām nepieciešamās tehnoloģijas un saskarnes izvēļu glabāšanu. Integrētā Stripe maksājumu saskarne var izmantot sīkdatnes un līdzīgas tehnoloģijas maksājumu autentifikācijai un krāpšanas novēršanai. Vietnes tehnoloģijas un izvēles var atšķirties no portāla vai vadības paneļa tehnoloģijām. Nebūtisko Vietnes analītikas un reklāmas tehnoloģiju izmantošanu pārvalda ar Vietnes piekrišanas iestatījumiem atsevišķi no portāla nepieciešamajām funkcijām.

Plašāka informācija un attiecīgās izvēles ir norādītas Sīkdatņu politikā (www.request.host/lv/sikdatnu-politika). Vietnes piekrišanu var mainīt vai atsaukt ar tur pieejamo pogu "Pārvaldīt sīkdatņu iestatījumus". Tehnoloģijas, kurām nepieciešama piekrišana, izmanto tikai pēc tās saņemšanas. Pārlikprogrammas iestatījumos var arī bloķēt vai dzēst sīkdatnes; nepieciešamo tehnoloģiju bloķēšana var ietekmēt funkciju darbību.

10. Jurisdikcijai specifiski paziņojumi

Kalifornijas patērētāju privātuma likuma (CCPA) paziņojums: Ciktāl personas datu apstrādei piemērojams CCPA, Kalifornijas iedzīvotāju papildu tiesības un attiecīgā informācija ir norādīta CCPA paziņojumā (www.request.host/privacy-policy/ccpa-notice), kas pieejams Pārziņa tīmekļa vietnē angļu valodā.

Personīgās informācijas aizsardzības un elektronisko dokumentu likuma (PIPEDA) paziņojums: Ciktāl personas datu apstrādei piemērojams PIPEDA, Kanādas iedzīvotāju papildu tiesības un attiecīgā informācija ir norādīta PIPEDA paziņojumā (www.request.host/privacy-policy/pipeda-notice), kas pieejams Pārziņa tīmekļa vietnē angļu valodā.

11. Nobeiguma jautājumi

Šī Privātuma politika pēc nepieciešamības var tikt mainīta, aktuālajai Politikas versijai tiekot publicētai Pārziņa tīmekļa vietnē. Par būtiskām izmaiņām informē atbilstošā veidā. Pirms datu izmantošanas

supervisory authority, including in the Member State of habitual residence, work or alleged infringement.

9. Cookies and Similar Technologies

The customer portal and the hosting control panel use technologies needed for authentication, security, sessions and requested functions, and storage of interface preferences. The integrated Stripe payment interface may use cookies and similar technologies for payment authentication and fraud prevention. Website technologies and choices may differ from those of the portal or control panel. Optional Website analytics and advertising technologies are managed through Website consent settings, separately from necessary portal functions.

Further information and relevant choices are set out in the Cookies Policy (www.request.host/cookies-policy). Website consent may be changed or withdrawn using its "Manage Your Cookie Preferences" button. Technologies requiring consent are used only after consent. Browser settings also allow cookies to be blocked or deleted; blocking necessary technologies may affect functionality.

10. Jurisdiction-Specific Notices

California Consumer Privacy Act (CCPA) Notice: Where the CCPA applies to the processing of personal data, additional rights and disclosures for California residents are set out in the CCPA Notice (www.request.host/privacy-policy/ccpa-notice), available on the Controller's website.

Personal Information Protection and Electronic Documents Act (PIPEDA) Notice: Where PIPEDA applies to the processing of personal data, additional rights and disclosures for Canadian residents are set out in the PIPEDA Notice (www.request.host/privacy-policy/pipeda-notice), available on the Controller's website.

11. Closing Remarks

This Privacy Policy may be amended as necessary, with the current version of the Policy being published on the Controller's website. Material changes shall be appropriately notified. Necessary information and the

jaunam mērķim sniedz nepieciešamo informāciju un nodrošina piemērojamo tiesisko pamatu.

Šī Privātuma politika ir pieejama Pārziņa tīmekļa vietnē arī angļu valodas versijā (www.request.host/privacy-policy). Neatbilstību vai pretrunu gadījumā starp latviešu un angļu valodas versijām latviešu valodas versija (www.request.host/lv/privatuma-politika) būs noteicošā visos aspektos, ievērojot piemērojamo normatīvo aktu obligātās prasības.

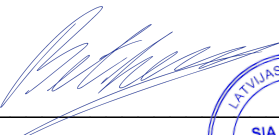
Jautājumu gadījumā par veikto personas datu apstrādi ar Pārziņu var sazināties, nosūtot vēstuli uz Pārziņa juridisko adresi: Stabu iela 109 - 1, Rīga, LV-1009, Latvija vai e-pastā: info@request.host

applicable legal basis shall be addressed before data is used for a new purpose.

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

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

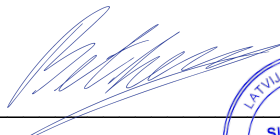
Apstiprinu:



D. Bethers
Valdes loceklis



Approved:



D. Bethers
Board Member

