ZÁSADY OCHRANY SOUKROMÍ / PRIVACY POLICY

Kosmik Compute s.r.o.

Version 2.1 | Effective date / Účinnost: 19 August 2026 / 19. 8. 2026

CESKY	ENGLISH
Tyto Zásady ochrany soukromí ("Privacy Policy") vysvětlují, jak Kosmik Compute s.r.o. zpracovává osobní údaje a zachází s obsahem zákazníků v souvislosti s webem, app.koscompute.com, API, billingem, supportem a AI compute službami.	This Privacy Policy explains how Kosmik Compute s.r.o. processes personal data and handles customer content in connection with its website, app.koscompute.com, APIs, billing, support and AI compute services.

1. KDO JSME	1. WHO WE ARE
1.1 Správce pro vlastní obchodní a provozní činnosti: Kosmik Compute s.r.o., IČO 29645301, Karla Dvořáčka 608/1, 683 23 Ivanovice na Hané, Česká republika. Kontakt: info@koscompute.com.	1.1 Controller for our own business and operational activities: Kosmik Compute s.r.o., Company ID 29645301, Karla Dvořáčka 608/1, 683 23 Ivanovice na Hané, Czech Republic. Contact: info@koscompute.com.
1.2 Kosmik Compute jmenoval pověřence pro ochranu osobních údajů (DPO). Kontakt na DPO: prostřednictvím info@koscompute.com nebo poštou na sídlo společnosti s označením pro pověřence pro ochranu osobních údajů.	1.2 Kosmik Compute has appointed a Data Protection Officer (DPO). DPO contact: via info@koscompute.com or by postal mail to our registered office marked for the attention of the Data Protection Officer.

2. PŮSOBNOST	2. SCOPE
2.1 Tato Privacy Policy se vztahuje na návštěvníky webu, zákazníky a zájemce, držitele účtů a administrátory organizací, osoby kontaktující support a osoby, jejichž údaje zákazník odešle do Služeb.	2.1 This Privacy Policy applies to website visitors, customers and prospects, account holders and organisation administrators, persons contacting support, and individuals whose data is submitted to the Services by a customer.
2.2 Rozlišujeme zejména (a) vlastní account, billing, security a business records, u nichž Kosmik Compute zpravidla jedná jako správce, a (b) Customer Content zpracovávaný na doložený pokyn zákazníka, u něhož Kosmik Compute zpravidla jedná jako zpracovatel nebo další zpracovatel.	2.2 We distinguish in particular between (a) our own account, billing, security and business records, for which Kosmik Compute generally acts as controller, and (b) Customer Content processed on the customer's documented instructions, for which Kosmik Compute generally acts as processor or subprocessor.

3. ROLE PODLE PRÁVA O OCHRANĚ OSOBNÍCH ÚDAJŮ	3. ROLES UNDER DATA PROTECTION LAW
3.1 Pro Customer Content zpracovávaný podle doložených pokynů zákazníka jedná Kosmik Compute jako zpracovatel nebo další zpracovatel. Účely zpracování Customer Content neurčujeme samostatně.	3.1 For Customer Content processed on a customer's documented instructions, Kosmik Compute acts as processor or subprocessor. We do not independently determine the purposes of processing Customer Content.

3.2 Pro správu účtů, organizací, billing, daně, fraud prevention, bezpečnost vlastních systémů, web, komunikaci, právní compliance a vlastní business records jedná Kosmik Compute jako samostatný správce v rozsahu, v němž určuje účely a prostředky zpracování.	3.2 For account and organisation administration, billing, tax, fraud prevention, security of our own systems, website operation, communications, legal compliance and our own business records, Kosmik Compute acts as an independent controller to the extent it determines the purposes and means of processing.
3.3 Pokud Kosmik Compute zpracovává osobní údaje jménem self-service zákazníka, použije se Self-Service Data Processing Addendum (DPA), který je součástí Kosmik Compute API Terms. Individuální data-processing ujednání se použije pouze v rozsahu individuální smlouvy uzavřené s konkrétním zákazníkem nebo dokumentu do ní výslovně začleněného.	3.3 Where Kosmik Compute processes personal data on behalf of a self-service customer, the Self-Service Data Processing Addendum (DPA), which forms part of the Kosmik Compute API Terms, applies. Individual data-processing terms apply only to the extent contained in an individual agreement with the specific customer or in a document expressly incorporated into that agreement.

4. DEFINICE	4. DEFINITIONS
4.1 "Customer Content" znamená data odeslaná do AI compute Služeb nebo vytvořená Službami pro zákazníka, zejména prompty, completions, text, soubory, audio, obrazy, video, generated media, tool payloads a jiný request/response obsah.	4.1 "Customer Content" means data submitted to or generated through our AI compute Services for a customer, including prompts, completions, text, files, audio, images, video, generated media, tool payloads and other request/response content.
4.2 "Operational Metadata" znamená technická, security, routingová, billingová, meteringová a usage data o requestu, která neobsahují Customer Content.	4.2 "Operational Metadata" means technical, security, routing, billing, metering and usage data about a request that excludes Customer Content.
4.3 "ZDR Endpoint" znamená endpoint označený jako Zero Data Retention, na kterém je Customer Content zpracováván pouze přechodně pro aktivní request a není zapisován do persistentního storage, content logs, analytics, monitoring, backups, durable queues ani externích modelových nebo cloud-inference providerů.	4.3 "ZDR Endpoint" means an endpoint designated Zero Data Retention where Customer Content is processed only transiently for the active request and is not written to persistent storage, content logs, analytics, monitoring, backups, durable queues, or external model or cloud-inference providers.
4.4 "Business Records" znamenají account, billing, tax, support, legal, security a compliance záznamy potřebné k provozu společnosti. Business Records nesmí obsahovat Customer Content z inference request path, ledaže jej zákazník vědomě vloží do supportu nebo jiné komunikace mimo tento path.	4.4 "Business Records" means account, billing, tax, support, legal, security and compliance records needed to operate the business. Business Records must not contain Customer Content from the inference request path unless the customer deliberately includes it in support or another communication outside that path.

5. JAKÉ ÚDAJE ZPRACOVÁVÁME	5. DATA WE PROCESS
5.1 Podle způsobu interakce můžeme zpracovávat identifikační a kontaktní údaje, například jméno, e-mail, společnost, IČO, DIČ, fakturační údaje a roli; account data, například organizaci, oprávnění, API key metadata a autentizační události; a billing a transaction data,	5.1 Depending on how you interact with us, we may process identification and contact data such as name, email, company, company ID, VAT ID, billing details and role; account data such as organisation membership, permissions, API key metadata and authentication

například kredity, platby, faktury, payment references a tax records.	events; and billing and transaction data such as credits, payments, invoices, payment references and tax records.
5.2 Dále můžeme zpracovávat technická a device data, zejména IP adresu, user agent, timestamps a device/browser information; service usage data, zejména request count, endpoint nebo model ID, Pricing Timestamp, token counts, request/response size, latency, HTTP status, error class, rate-limit decision, routing target a cost allocation; support data; a nezbytné website interaction data.	5.2 We may also process technical and device data, including IP address, user agent, timestamps and device/browser information; service usage data, including request count, endpoint or model ID, Pricing Timestamp, token counts, request/response size, latency, HTTP status, error class, rate-limit decision, routing target and cost allocation; support data; and necessary website interaction data.
5.3 Customer Content zpracováváme pouze tehdy, když jej zákazník nebo jeho uživatel odešle do Služeb nebo je prostřednictvím Služeb vygenerován. Customer Content může obsahovat jakékoli osobní údaje, které zákazník oprávněně odešle, včetně zvláštních kategorií osobních údajů a zdravotnické dokumentace.	5.3 We process Customer Content only when a customer or its user submits it to the Services or it is generated through the Services. Customer Content may contain any personal data lawfully submitted by the customer, including special categories of personal data and medical or health records.
5.4 Registrační a běžné account formuláře Kosmik Compute nejsou určeny ke sběru zdravotních údajů jako account data. Údaje o zdraví se mohou objevit v Customer Content pouze v důsledku use case zákazníka nebo pokud je zákazník vědomě vloží do support komunikace.	5.4 Kosmik Compute registration and ordinary account forms are not designed to collect health data as account data. Health data may appear in Customer Content as a result of the customer's use case or if the customer deliberately includes it in support communications.

6. ÚČELY A PRÁVNÍ ZÁKLADY	6. PURPOSES AND LEGAL BASES
6.1 Jako správce zpracováváme osobní údaje zejména pro vytvoření a správu účtů a organizací, autentizaci, poskytování a zabezpečení Služeb, billing a kredity, účetnictví a daně, fraud a abuse prevention, support, business communications, právní compliance a ochranu nebo uplatnění právních nároků.	6.1 As controller, we process personal data primarily to create and manage accounts and organisations, authenticate users, provide and secure the Services, administer billing and Credits, meet accounting and tax obligations, prevent fraud and abuse, provide support, conduct business communications, comply with law, and establish, exercise or defend legal claims.
6.2 Tam, kde se použije GDPR, opíráme vlastní controller processing zejména o plnění smlouvy nebo kroky před jejím uzavřením, plnění právních povinností, naše oprávněné zájmy na provozu a ochraně Služeb a souhlas tam, kde jej právo vyžaduje.	6.2 Where GDPR applies, our controller processing relies primarily on performance of a contract or pre-contract steps, compliance with legal obligations, our legitimate interests in operating and protecting the Services, and consent where required by law.
6.3 U Customer Content zpracovávaného jménem zákazníka neurčuje Kosmik Compute vlastní právní základ pro účel zákazníka. Zákazník jako správce nebo oprávněný zpracovatel odpovídá za právní základ, informační povinnosti a oprávnění předat osobní údaje Kosmik Compute.	6.3 For Customer Content processed on a customer's behalf, Kosmik Compute does not determine the customer's lawful basis for its purpose. The customer acting as controller or authorised processor is responsible for the lawful basis, required notices and authority to provide personal data to Kosmik Compute.

6.4 Customer Content nepoužíváme pro advertising, marketing profiling, product ranking, model training, model fine-tuning, model improvement nebo model evaluation, není-li zákazníkem samostatně a výslovně písemně instruováno jinak.	6.4 We do not use Customer Content for advertising, marketing profiling, product ranking, model training, model fine-tuning, model improvement or model evaluation unless separately and expressly instructed otherwise in writing by the customer.
7. ÚDAJE O ZDRAVÍ A JINÉ ZVLÁŠTNÍ KATEGORIE	**7. HEALTH DATA AND OTHER SPECIAL CATEGORIES**
7.1 ZDR Endpointy mohou technicky zpracovávat Customer Content obsahující zvláštní kategorie osobních údajů, včetně údajů o zdraví, genetických nebo biometrických údajů, pokud zákazník takové údaje zákonně odešle. Kosmik Compute tyto údaje zpracovává jako processor/subprocessor pouze podle doložených pokynů zákazníka.	7.1 ZDR Endpoints may technically process Customer Content containing special categories of personal data, including health, genetic or biometric data, where the customer lawfully submits such data. Kosmik Compute processes such data as processor/subprocessor only on the customer's documented instructions.
7.2 Zákazník odpovídá zejména za právní základ podle článku 6 GDPR a, je-li relevantní, podmínku podle článku 9 GDPR, pravidla pro údaje podle článku 10 GDPR, data minimisation, access controls, DPIA a sektorové požadavky. Samotný ZDR režim nenahrazuje tyto povinnosti.	7.2 The customer is responsible, in particular, for a lawful basis under Article 6 GDPR and, where relevant, a condition under Article 9 GDPR, rules applicable to Article 10 data, data minimisation, access controls, DPIAs and sector-specific requirements. ZDR does not replace these obligations.
7.3 Pokud zákazník potřebuje zvláštní certifikaci nebo smlouvu vyžadovanou jiným právním režimem, například HIPAA Business Associate Agreement, musí být takový režim s Kosmik Compute samostatně sjednán; tato Privacy Policy jej sama nevytváří.	7.3 If a customer requires specific certification or a separate agreement under another legal regime, such as a HIPAA Business Associate Agreement, that regime must be separately agreed with Kosmik Compute; this Privacy Policy does not itself create it.
8. ZERO DATA RETENTION COMMITMENT	**8. ZERO DATA RETENTION COMMITMENT**
8.1 Standardní inference endpointy nabízené v self-service režimu jsou ZDR Endpointy, pokud nejsou před použitím zřetelně označeny jako non-ZDR. U ZDR Endpointů se Customer Content zpracovává pouze přechodně po dobu aktivního request lifecycle.	8.1 Standard inference endpoints offered through the self-service Services are ZDR Endpoints unless clearly designated as non-ZDR before use. On ZDR Endpoints, Customer Content is processed only transiently for the active request lifecycle.
8.2 U ZDR Endpointů Customer Content není zapisován do persistent storage, application logs, reverse-proxy logs, model-server logs, GPU-worker logs, debug logs, trace logs, analytics systems, monitoring systems, support systems, backups, durable queues, object storage ani persistent cache layers.	8.2 On ZDR Endpoints, Customer Content is not written to persistent storage, application logs, reverse-proxy logs, model-server logs, GPU-worker logs, debug logs, trace logs, analytics systems, monitoring systems, support systems, backups, durable queues, object storage or persistent cache layers.
8.3 Customer Content ze ZDR Endpointu není odesílán externím model providers, cloud inference providers, logging, analytics, monitoring, support, storage nebo	8.3 Customer Content from a ZDR Endpoint is not sent to external model providers, cloud inference providers, logging, analytics, monitoring, support, storage or backup

backup providers způsobem, který by jim zpřístupnil Customer Content.	providers in a manner that exposes Customer Content to them.
8.4 Customer Content ze ZDR Endpointu není používán k model training, fine-tuning, improvement, evaluation, ranking nebo benchmarkingu ani k manuálnímu review za účelem zlepšování modelů.	8.4 Customer Content from a ZDR Endpoint is not used for model training, fine-tuning, improvement, evaluation, ranking or benchmarking, or for manual review for model improvement.
8.5 Customer Content je po dokončení, selhání, timeoutu nebo zrušení requestu odstraněn z request-processing memory. ZDR znamená žádnou pozitivní retenci Customer Content po aktivním request lifecycle.	8.5 Customer Content is discarded from request-processing memory after the request completes, fails, times out or is cancelled. ZDR means no positive retention of Customer Content after the active request lifecycle.
8.6 Volitelný endpoint nebo funkce, která vyžaduje persistentní Customer Content nebo jiné non-ZDR zacházení, musí být před použitím zřetelně označena jako non-ZDR nebo ekvivalentně popsána. Příslušná retention a processing informace bude zákazníkovi zpřístupněna před použitím této funkce.	8.6 An optional endpoint or feature requiring persistent Customer Content or other non-ZDR handling must be clearly designated as non-ZDR or equivalently described before use. Applicable retention and processing information will be made available to the customer before the feature is used.

9. TECHNICKÝ ZDR BASELINE	9. TECHNICAL ZDR BASELINE
9.1 ZDR requesty jsou přijímány přes encrypted transport, autentizovány a kontrolovány proti account status, permissions, quota, rate limits a abuse controls. Customer Content může během aktivního requestu existovat pouze v RAM, GPU memory, process buffers, network buffers a stream buffers potřebných ke zpracování.	9.1 ZDR requests are accepted over encrypted transport, authenticated and checked against account status, permissions, quota, rate limits and abuse controls. During the active request, Customer Content may exist only in RAM, GPU memory, process buffers, network buffers and stream buffers necessary for processing.
9.2 Logging je content-excluding by design. Log schemas nemají obsahovat prompt text, completion text, generated output, file content, extracted text, embeddings Customer Content, reversible content hashes ani unsanitized exception traces obsahující Customer Content.	9.2 Logging is content-excluding by design. Log schemas must not contain prompt text, completion text, generated output, file content, extracted text, embeddings of Customer Content, reversible content hashes or unsanitized exception traces containing Customer Content.
9.3 Monitoring a observability používají Operational Metadata a resource metrics. Automatizované security nebo abuse controls mohou Customer Content přechodně vyhodnotit během aktivního requestu, ale nesmějí jej persistovat jako čitelný obsah, content embedding nebo content fingerprint.	9.3 Monitoring and observability use Operational Metadata and resource metrics. Automated security or abuse controls may transiently evaluate Customer Content during the active request but must not persist it as human-readable content, a content embedding or content fingerprint.
9.4 Failed, timed-out, cancelled, malformed a rejected requesty podléhají stejnému no-persistence pravidlu jako úspěšné requesty. Support tools nedostávají Customer Content automaticky z request path.	9.4 Failed, timed-out, cancelled, malformed and rejected requests are subject to the same no-persistence rule as successful requests. Support tools do not automatically receive Customer Content from the request path.

10. OPERATIONAL METADATA A BILLING DATA	10. OPERATIONAL METADATA AND BILLING DATA
10.1 Pro provoz, security, fraud prevention, debugging, reliability, metering a billing můžeme uchovávat omezená Operational Metadata, například request ID, account/organisation ID, API key hash nebo identifier, endpoint/model ID, server timestamps včetně Pricing Timestamp, request/response size, token counts, latency, HTTP/service status, error class, routing target, rate-limit decision, cost allocation, IP address a user agent tam, kde je to potřebné.	10.1 For operation, security, fraud prevention, debugging, reliability, metering and billing, we may retain limited Operational Metadata such as request ID, account/organisation ID, API key hash or identifier, endpoint/model ID, server timestamps including Pricing Timestamp, request/response size, token counts, latency, HTTP/service status, error class, routing target, rate-limit decision, cost allocation, IP address and user agent where needed.
10.2 Pro billing může systém uchovávat nebo rekonstruovat cenovou verzi Models API účinnou k Pricing Timestamp a aplikovat ji na naměřené jednotky podle tokenizeru a metering pravidel příslušného modelu. Tato data nevyžadují uložení raw promptu ani raw Výstupu.	10.2 For billing, the system may retain or reconstruct the version of Models API pricing effective at the Pricing Timestamp and apply it to measured units according to the tokenizer and metering rules for the relevant model. This does not require storage of the raw prompt or raw Output.
10.3 Operational Metadata nesmí obsahovat raw prompty, completions, generated outputs, uploaded file content, audio/image/video content, extracted text, customer-content embeddings, reversible hashes Customer Content, screenshots Customer Content ani support transcripts automaticky naplněné z Customer Content.	10.3 Operational Metadata must not contain raw prompts, completions, generated outputs, uploaded file content, audio/image/video content, extracted text, Customer Content embeddings, reversible hashes of Customer Content, screenshots of Customer Content or support transcripts automatically populated from Customer Content.

11. RETENCE	11. RETENTION
11.1 Customer Content na ZDR Endpointech není uchováván po dokončení, selhání, timeoutu nebo zrušení requestu. Prompt a completion content logs se nevytvářejí; uploaded files a generated media ze ZDR requestu se po request lifecycle neuchovávají; persistent content cache a durable queues s Customer Content se nepoužívají.	11.1 Customer Content on ZDR Endpoints is not retained after request completion, failure, timeout or cancellation. Prompt and completion content logs are not created; uploaded files and generated media from ZDR requests are not retained after the request lifecycle; persistent content caches and durable queues containing Customer Content are not used.
11.2 Operational Metadata pro security, abuse prevention, debugging a reliability se standardně uchovávají až 30 dnů, ledaže security incident, fraud investigation, právní povinnost, dispute nebo legal claim odůvodňuje delší uchování relevantních metadata.	11.2 Operational Metadata for security, abuse prevention, debugging and reliability is generally retained for up to 30 days unless a security incident, fraud investigation, legal obligation, dispute or legal claim justifies longer retention of the relevant metadata.
11.3 Aggregated usage, pricing snapshot references a billing records se uchovávají po dobu potřebnou pro billing, účetnictví, daně, payment, audit a právní účely. Account records se uchovávají po dobu existence účtu a přiměřenou dobu poté; support data do vyřešení věci a přiměřenou follow-up, audit nebo legal period; legal/compliance records podle právní povinnosti nebo platného legal hold.	11.3 Aggregated usage, pricing-snapshot references and billing records are retained as needed for billing, accounting, tax, payment, audit and legal purposes. Account records are retained for the life of the account and a reasonable period afterwards; support data until the matter is resolved and for a reasonable follow-up, audit or legal period; and legal/compliance records as required by law or a valid legal hold.

11.4 U non-ZDR funkce se použije retention informace zpřístupněná pro danou funkci před jejím použitím.	11.4 For a non-ZDR feature, the retention information made available for that feature before use applies.

12. LOGGING A INCIDENT HANDLING	12. LOGGING AND INCIDENT HANDLING
12.1 Na ZDR Endpointech jsou prompt logs, completion logs a content debug captures vypnuty a request/response bodies jsou vyloučeny z persistent access, reverse-proxy, model-server a GPU-worker logs. Exception traces mají být sanitizovány tak, aby neobsahovaly Customer Content.	12.1 On ZDR Endpoints, prompt logs, completion logs and content debug captures are disabled, and request/response bodies are excluded from persistent access, reverse-proxy, model-server and GPU-worker logs. Exception traces are designed to be sanitised so they do not contain Customer Content.
12.2 Pokud je Customer Content ze ZDR Endpointu omylem zapsán do persistentního systému, považujeme událost za security incident a přijmeme přiměřená opatření k containment, omezení přístupu, deletion nebo isolation tam, kde je to právně a technicky možné, root-cause analysis, remediation a právně požadovaným oznámením.	12.2 If Customer Content from a ZDR Endpoint is accidentally written to a persistent system, we treat the event as a security incident and take appropriate containment, access restriction, deletion or isolation steps where legally and technically possible, conduct root-cause analysis and remediation, and make legally required notifications.

13. INFRASTRUKTURA A DATACENTRUM	13. INFRASTRUCTURE AND DATACENTRE
13.1 ZDR Customer Content je zpracováván na infrastruktuře kontrolované Kosmik Compute fyzicky umístěné v České republice, není-li pro konkrétní produkt nebo endpoint předem výslovně uvedeno jinak.	13.1 ZDR Customer Content is processed on Kosmik Compute-controlled infrastructure physically located in the Czech Republic unless expressly stated otherwise in advance for a particular product or endpoint.
13.2 Fyzický datacenter/colocation provider může poskytovat zejména facility, rackspace, power, cooling a connectivity pro servery kontrolované Kosmik Compute. Samotné poskytování těchto fyzických služeb bez logického přístupu k Customer Content neznamená, že je takový provider oprávněn Customer Content zpracovávat. Aktuální facility a případní Subprocessoři relevantní pro Customer Content jsou uvedeni v aktuálním Subprocessor & Infrastructure Notice zveřejněném na webu Kosmik Compute.	13.2 A physical datacentre/colocation provider may provide facility, rack space, power, cooling and connectivity for Kosmik Compute-controlled servers. Providing those physical services without logical access to Customer Content does not itself authorise that provider to process Customer Content. Then-current facilities and any Subprocessors relevant to Customer Content are identified in the current Subprocessor & Infrastructure Notice published on the Kosmik Compute website.
13.3 Informace o facility, certifikacích třetích stran a infrastruktuře zveřejněné mimo tuto Privacy Policy jsou informační a mohou být průběžně aktualizovány. Tvrzení o certifikaci konkrétního dodavatele nepředstavuje tvrzení, že Kosmik Compute sama drží stejnou certifikaci, není-li to výslovně uvedeno.	13.3 Information about facilities, third-party certifications and infrastructure published outside this Privacy Policy is informational and may be updated from time to time. A statement concerning a particular supplier's certification does not represent that Kosmik Compute itself holds the same certification unless expressly stated.

14. SUBPROCESSOŘI A EXTERNÍ ROUTING	14. SUBPROCESSORS AND EXTERNAL ROUTING

14.1 Aktuální seznam Subprocessorů relevantních pro Customer Content a aktuální facility informace udržujeme v Subprocessor & Infrastructure Notice zveřejněném na webu Kosmik Compute nebo v jeho nástupnickém oznámení. Změny Subprocessorů pro processor processing se řídí DPA.	14.1 We maintain the then-current list of Subprocessors relevant to Customer Content and current facility information in the Subprocessor & Infrastructure Notice published on the Kosmik Compute website or its successor notice. Changes to Subprocessors for processor processing are governed by the DPA.
14.2 Endpoint označený jako ZDR nebude routovat Customer Content externímu model nebo cloud-inference providerovi ani jiné třetí straně způsobem neslučitelným se ZDR commitments. Pokud by konkrétní funkce vyžadovala odlišný režim, bude před použitím označena jako non-ZDR nebo jinak jasně popsána.	14.2 An endpoint designated ZDR will not route Customer Content to an external model or cloud-inference provider or another third party in a manner inconsistent with the ZDR commitments. If a particular feature requires different handling, it will be designated non-ZDR or otherwise clearly described before use.
14.3 Pro Business Records a controller operations můžeme využívat payment a billing providers, email/communications providers, professional advisers, auditors, accountants, legal counsel a security, fraud-prevention nebo compliance providers, v rozsahu potřebném pro jejich službu a v souladu s právem.	14.3 For Business Records and controller operations, we may use payment and billing providers, email/communications providers, professional advisers, auditors, accountants, legal counsel and security, fraud-prevention or compliance providers to the extent necessary for their services and in accordance with law.
14.4 Pokud přidáme Subprocessora, který bude zpracovávat Customer Personal Data jménem zákazníka, budeme postupovat podle DPA a zveřejněného Subprocessor & Infrastructure Notice. Samotná aktualizace seznamu v souladu s DPA nevyžaduje změnu této Privacy Policy.	14.4 If we add a Subprocessor that will process Customer Personal Data on behalf of a customer, we will follow the DPA and the published Subprocessor & Infrastructure Notice. Updating that list in accordance with the DPA does not itself require an amendment to this Privacy Policy.

15. MEZINÁRODNÍ PŘENOSY	15. INTERNATIONAL TRANSFERS
15.1 ZDR Customer Content není přenášen mimo Evropský hospodářský prostor, není-li pro konkrétní endpoint nebo individuální smlouvu předem výslovně uvedeno jinak a použit odpovídající právní mechanismus.	15.1 ZDR Customer Content is not transferred outside the European Economic Area unless expressly stated otherwise in advance for a specific endpoint or individual agreement and an appropriate legal mechanism is used.
15.2 Pro Business Records nebo controller operations mohou někteří poskytovatelé zpracovávat údaje mimo EHP. Je-li to vyžadováno, používáme odpovídající safeguards, například adequacy decision, Standard Contractual Clauses nebo jiný uznaný mechanismus.	15.2 For Business Records or controller operations, some providers may process data outside the EEA. Where required, we use appropriate safeguards such as an adequacy decision, Standard Contractual Clauses or another recognised mechanism.

16. ZABEZPEČENÍ	16. SECURITY
16.1 Používáme technická a organizační opatření navržená k ochraně osobních údajů, Customer Content a infrastruktury, zejména encrypted transport, network segmentation, firewall controls, least-privilege a role-based administrative access, secrets management,	16.1 We use technical and organisational measures designed to protect personal data, Customer Content and infrastructure, including encrypted transport, network segmentation, firewall controls, least-privilege and role-based administrative access, secrets management,

restricted production access, administrative access logging, patching, dependency a vulnerability management, change control, incident response, periodic access review a backup controls vylučující ZDR Customer Content.	restricted production access, administrative access logging, patching, dependency and vulnerability management, change control, incident response, periodic access review and backup controls excluding ZDR Customer Content.
16.2 Žádná metoda přenosu, hostingu nebo zpracování není absolutně bezpečná. ZDR snižuje riziko minimalizací persistence Customer Content, ale není tvrzením, že security incident je technicky nemožný.	16.2 No method of transmission, hosting or processing is completely secure. ZDR reduces risk by minimising persistence of Customer Content but does not mean that a security incident is technically impossible.

17. COOKIES A WEBSITE DATA	17. COOKIES AND WEBSITE DATA
17.1 Ve výchozím stavu používáme pouze cookies a obdobné technologie nezbytné pro bezpečnost, authentication, session management a funkčnost webu nebo aplikace a preference cookies tam, kde si uživatel zvolí uložení nastavení.	17.1 By default, we use only cookies and similar technologies necessary for security, authentication, session management and website or application functionality, plus preference cookies where a user chooses to save settings.
17.2 Non-essential analytics nebo marketing cookies nepoužijeme bez požadovaného oznámení a, je-li vyžadován, souhlasu. Pokud takové technologie zavedeme, aktualizujeme tuto Privacy Policy a příslušný consent mechanism.	17.2 We will not use non-essential analytics or marketing cookies without required notice and, where required, consent. If we introduce such technologies, we will update this Privacy Policy and the applicable consent mechanism.

18. PRÁVA SUBJEKTŮ ÚDAJŮ	18. DATA SUBJECT RIGHTS
18.1 Podle použitelného práva může mít subjekt údajů právo na přístup, opravu, výmaz, omezení zpracování, námitku, přenositelnost, odvolání souhlasu a podání stížnosti u Úřadu pro ochranu osobních údajů nebo jiného příslušného dozorového orgánu.	18.1 Subject to applicable law, a data subject may have rights of access, rectification, erasure, restriction, objection, portability, withdrawal of consent and the right to lodge a complaint with the Czech Data Protection Authority or another competent supervisory authority.
18.2 U vlastních controller data Kosmik Compute lze žádost zaslat na info@koscompute.com. U Customer Content zpracovávaného jménem zákazníka má být žádost zpravidla adresována příslušnému zákazníkovi jako správci; Kosmik Compute mu poskytne součinnost podle DPA.	18.2 Requests concerning Kosmik Compute's own controller data may be sent to info@koscompute.com. Requests concerning Customer Content processed on behalf of a customer should normally be directed to the relevant customer as controller; Kosmik Compute will assist that customer in accordance with the DPA.
18.3 ZDR Customer Content po dokončení requestu zpravidla nelze vyhledat, exportovat, opravit nebo individuálně vymazat, protože není uchováván. Toto technické omezení je důsledkem samotného no-retention designu.	18.3 ZDR Customer Content generally cannot be retrieved, exported, corrected or individually deleted after request completion because it is not retained. This technical limitation is a consequence of the no-retention design itself.

19. DĚTI	19. CHILDREN

19.1 Web, app.koscompute.com a self-service smluvní vztah jsou určeny B2B zákazníkům, nikoli přímo dětem. Kosmik Compute cíleně nevytváří dětské spotřebitelské účty.	19.1 The website, app.koscompute.com and self-service contractual relationship are intended for B2B customers, not directly for children. Kosmik Compute does not intentionally create child consumer accounts.
19.2 Zákazník však může prostřednictvím API zpracovávat údaje o nezletilých, například jako součást zdravotnické dokumentace, pokud je k tomu jako správce nebo oprávněný zpracovatel oprávněn a splní použitelné povinnosti. Kosmik Compute takové údaje zpracovává pouze podle zákazníkových pokynů.	19.2 A customer may nevertheless process data concerning minors through the API, for example as part of medical records, where it is authorised to do so as controller or authorised processor and complies with applicable obligations. Kosmik Compute processes such data only on the customer's instructions.

20. POVINNOSTI ZÁKAZNÍKA	20. CUSTOMER RESPONSIBILITIES
20.1 Zákazník odpovídá za zákonnost Customer Content, potřebné notices, consents nebo jiné právní základy, minimalizaci dat, přístupová oprávnění, vhodnost use case, DPIA tam, kde je vyžadována, a za to, že jeho vlastní aplikace a koncoví uživatelé dodržují použitelné právní a bezpečnostní požadavky.	20.1 The customer is responsible for the lawfulness of Customer Content, required notices, consents or other lawful bases, data minimisation, access permissions, suitability of the use case, DPIAs where required, and ensuring that its applications and end users comply with applicable legal and security requirements.
20.2 Zákazník by neměl posílat Customer Content do supportu, pokud to není nezbytné pro řešení konkrétního support requestu; obsah dobrovolně poskytnutý supportu je support data a nepodléhá ZDR request-path commitments.	20.2 The customer should not send Customer Content to support unless necessary to resolve a specific support request; content voluntarily provided to support is support data and is not subject to the ZDR request-path commitments.

21. ZMĚNY TÉTO PRIVACY POLICY	21. CHANGES TO THIS PRIVACY POLICY
21.1 Tato Privacy Policy je informační oznámení, nikoli smlouva. Můžeme ji kdykoli aktualizovat tak, aby odpovídala aktuálním Službám, technologiím, právním požadavkům, Subprocessorům a skutečné privacy praxi. Aktuální verzi zveřejníme s novým effective date. Materiální změny informací o zpracování osobních údajů přivedeme aktivně k pozornosti dotčených osob, pokud je to s ohledem na povahu změny přiměřené nebo vyžadované právem.	21.1 This Privacy Policy is a transparency notice, not a contract. We may update it at any time to reflect the then-current Services, technology, legal requirements, Subprocessors and actual privacy practices. The current version will be published with a revised effective date. We will actively bring material changes to personal-data processing information to the attention of affected persons where appropriate in light of the nature of the change or required by law.
21.2 Změna Privacy Policy sama o sobě nemění smluvní práva ani povinnosti podle API Terms nebo DPA a nezakládá samostatné smluvní právo na odstoupení. Materiální oslabení contractual ZDR commitment pro endpoint nadále označený jako ZDR by vyžadovalo odpovídající postup podle API Terms/DPA; alternativně musí být dotčená funkce před použitím označena jako non-ZDR nebo jinak jasně popsána.	21.2 A change to this Privacy Policy does not by itself amend contractual rights or obligations under the API Terms or DPA and does not create a separate contractual withdrawal right. A material weakening of the contractual ZDR commitment for an endpoint that remains designated ZDR would require the applicable process under the API Terms/DPA; alternatively, the affected feature must be designated non-ZDR or otherwise clearly described before use.

22. JAZYK A KONTAKT	22. LANGUAGE AND CONTACT
22.1 Česká a anglická verze mají sdělovat stejnou informaci. V případě rozporu nebo nejasnosti je pro účely tohoto oznámení referenční české znění, aniž jsou tím omezena práva subjektů údajů podle kogentního práva. Tato Privacy Policy není smluvním dokumentem a pravidlo jazykové priority nemění smluvní hierarchii podle API Terms.	22.1 The Czech and English versions are intended to communicate the same information. In the event of conflict or ambiguity, the Czech wording is the reference text for purposes of this notice, without limiting data-subject rights under mandatory law. This Privacy Policy is not a contractual document and this language rule does not alter the contractual hierarchy under the API Terms.
22.2 Privacy requests, dotazy a stížnosti: Kosmik Compute s.r.o., Karla Dvořáčka 608/1, 683 23 Ivanovice na Hané, Česká republika; info@koscompute.com. Pro kontaktování DPO použijte stejný e-mail nebo poštovní adresu s označením pro DPO.	22.2 Privacy requests, questions and complaints: Kosmik Compute s.r.o., Karla Dvořáčka 608/1, 683 23 Ivanovice na Hané, Czech Republic; info@koscompute.com. To contact the DPO, use the same email or postal address marked for the attention of the DPO.

INFORMATIVNI CHANGELOG / INFORMATIVE CHANGELOG

Tato cast neni soucasti smluvniho textu. / This section is not part of the contractual text.

CESKY	ENGLISH
Verze 2.1 výslovně vymezuje Privacy Policy jako informační oznámení, nikoli smluvní dokument; contractual commitments zůstávají v API Terms a DPA.	Version 2.1 expressly treats the Privacy Policy as a transparency notice rather than a contractual document; contractual commitments remain in the API Terms and DPA.
Odstraněna jmenná vazba na konkrétního DPO; zachován stabilní DPO contact channel, aby personální změna nevyžadovala přepis celé Policy.	Removes the named individual DPO dependency while preserving a stable DPO contact channel, so personnel changes do not require a full Policy revision.
Konkrétní datacenter/facility a Subprocessor údaje byly přesunuty do dynamického Subprocessor & Infrastructure Notice; změna seznamu podle DPA sama nevyžaduje změnu Privacy Policy.	Moves specific datacentre/facility and Subprocessor information to the dynamic Subprocessor & Infrastructure Notice; a list update under the DPA does not itself require a Privacy Policy amendment.
Změny Privacy Policy mohou být zveřejňovány průběžně; materiální změny processing information budou aktivně oznámeny, pokud je to přiměřené nebo vyžadované právem. Změna Policy sama nevytváří smluvní odstoupení.	The Privacy Policy may be updated from time to time; material changes to processing information will be actively communicated where appropriate or legally required. A Policy update does not itself create a contractual withdrawal right.
ZDR zůstává popsáno transparentně, ale jeho smluvní základ je výslovně v API Terms a DPA, čímž se omezuje duplicita mezi dokumenty.	ZDR remains transparently described, while its contractual basis is expressly located in the API Terms and DPA, reducing duplication between documents.