ZÁSADY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

pro službu Naxter Cloud na doméně naxter.cz a souvisejících webových nebo aplikačních rozhraních

| | |
|---|---|
| **Správce** | NAXTER DEV s.r.o.<br>IČ: 23025077, DIČ: CZ23025077<br>Na Folimance 2155/15, 120 00 Praha 2 |
| **Kontakt** | info@naxter.cz |
| **Verze dokumentu** | 07.05.2026 |

Tyto zásady zpracování osobních údajů vysvětlují, jaké osobní údaje správce zpracovává v souvislosti s provozem webu, uživatelské části a cloudové aplikace Naxter Cloud, jaké jsou účely a právní důvody zpracování, komu mohou být údaje zpřístupněny, jak dlouho jsou uchovávány a jaká práva mohou uživatelé a další subjekty údajů vůči správci uplatnit.

Služba Naxter Cloud je určena zejména pro správu uživatelských účtů, přihlášení, administraci, správu zařízení, práci s IoT daty, sdílení zařízení, správu dokumentů, obsahu webu, partnerů, kontaktních formulářů, podpory, zabezpečení účtů, nezbytných cookies a souvisejících technických funkcí. Tyto zásady se vztahují na používání služby prostřednictvím webu, aplikace, administrace a souvisejících rozhraní, pokud správce neuveřejní pro konkrétní službu samostatné zásady.

Dokument je sepsán zejména s ohledem na nařízení Evropského parlamentu a Rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů, zákon č. 110/2019 Sb., o zpracování osobních údajů, zákon č. 127/2005 Sb., o elektronických komunikacích, zákon č. 480/2004 Sb., o některých službách informační společnosti, občanský zákoník, zákon o ochraně spotřebitele a další použitelné české a evropské předpisy, včetně pravidel pro digitální služby a umělou inteligenci tam, kde se na konkrétní funkci služby použijí.

## 1. Správce a kontaktní údaje

Správcem osobních údajů je společnost NAXTER DEV s.r.o., IČ: 23025077, DIČ: CZ23025077, se sídlem Na Folimance 2155/15, 120 00 Praha 2, Česká republika.

V záležitostech týkajících se ochrany osobních údajů, uplatnění práv, dotazů, stížností, žádostí o výmaz účtu, žádostí o přístup k údajům nebo žádostí o ruční posouzení zásahu do účtu lze správce kontaktovat na e-mailové adrese info@naxter.cz.

Není-li na webu služby uvedeno jinak, není v těchto zásadách zveřejněn samostatný pověřenec pro ochranu osobních údajů. Kontaktním místem pro ochranu osobních údajů je výše uvedená e-mailová adresa správce.

## 2. Jaké osobní údaje zpracováváme

Rozsah zpracovávaných údajů závisí na tom, jak uživatel službu používá, jaké funkce jsou v konkrétním účtu dostupné, jaká zařízení jsou ke službě připojena a jaké informace uživatel nebo administrátor do služby dobrovolně vloží.

• identifikační a registrační údaje, zejména uživatelské jméno, e-mailovou adresu, interní identifikátor účtu, roli, jazykové nastavení, stav účtu, historii změn účtu a záznamy o potvrzení povinných dokumentů;

• přihlašovací a bezpečnostní údaje, zejména hash hesla, jednorázové tokeny, údaje o obnově hesla, údaje o relaci, stav dvoufázového ověření, lokálně uložený TOTP secret, bezpečnostní logy, záznamy o pokusech o přihlášení a údaje potřebné pro ochranu účtu;

• kontaktní údaje, zejména e-mailovou adresu, volitelně telefonní číslo, obsah kontaktního formuláře, podpůrnou komunikaci a údaje potřebné k odesílání provozních e-mailů;

• údaje o zařízeních a jejich používání, zejména název zařízení, typ, kategorie, nastavení, vlastnictví, sdílení, stav online nebo offline, provozní události, živá data, telemetrické údaje, příkazy, odpovědi zařízení a vazby mezi účtem a zařízením;

• obsah vložený uživatelem nebo administrátorem, zejména dokumenty, popisy, texty, kontaktní fotografie, loga, URL partnerů, veřejné nebo interní části obsahu webu a metadata nahraných souborů;

• údaje z podpory, reklamací, hlášení závad, bezpečnostních oznámení a běžné komunikace se správcem;

• technické, provozní a bezpečnostní údaje, zejména IP adresu, datum a čas požadavku, URL, user-agent, chybové logy, auditní záznamy, údaje o doručování e-mailů, údaje o cookies, localStorage, sessionStorage a údaje z bezpečnostních služeb, například reCAPTCHA;

• údaje z volitelného přihlášení přes třetí stranu, například Google OAuth, pokud je taková funkce ve službě zapnuta a uživatel ji použije.

Osobní údaje získává správce především přímo od uživatele, z jeho používání služby, z připojených zařízení, z administrátorské správy a z technického provozu webu a aplikace. V omezeném rozsahu mohou údaje vznikat také odvozením z provozních a bezpečnostních událostí, například při prevenci zneužití nebo řešení incidentu.

## 3. Zvláštní kategorie údajů, údaje dětí a obsah třetích osob

Správce cíleně nevyžaduje zvláštní kategorie osobních údajů podle čl. 9 GDPR, jako jsou údaje o zdravotním stavu, biometrické údaje za účelem jedinečné identifikace osoby, údaje o politických názorech, náboženském vyznání nebo sexuálním životě. Uživatelé by takové údaje do služby neměli vkládat, pokud to není nezbytné pro konkrétní účel používání služby a mají k tomu odpovídající právní důvod.

Pokud uživatel nebo administrátor takové údaje dobrovolně vloží do volného textu, dokumentu, fotografie nebo jiné části služby, zpracovává je správce pouze v rozsahu nezbytném pro provoz služby, ochranu práv, splnění zákonné povinnosti nebo na základě jiného použitelného právního důvodu.

Služba není primárně určena dětem. Pokud by byla využita osobou mladší 15 let v situaci, ve které je právním důvodem souhlas se zpracováním údajů ve vztahu ke službě informační společnosti, musí být splněny podmínky českého zákona o zpracování osobních údajů a GDPR, zejména požadavek souhlasu nebo schválení zákonného zástupce, pokud se použije.

Uživatel odpovídá za to, že údaje třetích osob, například kontaktní údaje, fotografie, popisy, názvy zařízení nebo údaje obsažené v nahraném dokumentu, vkládá do služby pouze tehdy, má-li k tomu oprávnění a neporušuje tím práva těchto osob.

## 4. Účely zpracování a právní důvody

Správce zpracovává osobní údaje pouze v rozsahu přiměřeném a nezbytném pro konkrétní účely. Hlavní účely zpracování a právní důvody jsou zejména tyto:

• zřízení, vedení a správa uživatelského účtu, přihlášení, obnova hesla, správa relací, jazykové nastavení a zpřístupnění funkcí služby; právním důvodem je zejména plnění smlouvy nebo provedení opatření před jejím uzavřením;

• správa zařízení, zobrazení jejich stavu, nastavení, sdílení, komunikace se zařízeními a související provoz IoT funkcí; právním důvodem je zejména plnění smlouvy a oprávněný zájem na řádném provozu služby;

• evidence povinných dokumentů, souhlasů, potvrzení verzí dokumentů a re-consent procesu při změně pravidel; právním důvodem je plnění smlouvy a oprávněný zájem správce na prokazatelnosti;

• zajištění bezpečnosti, ochrana účtů, prevence zneužití, spamu, automatizovaných útoků, neoprávněného přístupu a podvodného jednání, včetně použití CSRF ochrany, dvoufázového ověření a reCAPTCHA; právním důvodem je oprávněný zájem správce a uživatelů na bezpečném provozu služby;

• zákaznická podpora, reakce na dotazy, řešení závad, reklamací, bezpečnostních podnětů a právních požadavků; právním důvodem je plnění smlouvy, oprávněný zájem nebo splnění právní povinnosti podle povahy požadavku;

• správa veřejného nebo interního obsahu webu, dokumentů, partnerů a administrace; právním důvodem je oprávněný zájem správce na prezentaci a provozu služby, případně plnění smlouvy;

• vedení provozních, bezpečnostních a auditních záznamů, řešení incidentů, obrana právních nároků a dokazování splnění povinností; právním důvodem je oprávněný zájem a v některých případech splnění právní povinnosti;

• odesílání provozních e-mailů, například ověření e-mailu, obnova hesla, upozornění na změnu dokumentu nebo bezpečnostní informace; právním důvodem je plnění smlouvy a oprávněný zájem;

• použití nezbytných cookies a obdobných technologií potřebných pro přihlášení, zabezpečení, session, jazyk a zobrazení informace o cookies; právním důvodem je zajištění provozu služby, plnění smlouvy a oprávněný zájem;

• volitelné marketingové nebo obchodní sdělení, pokud by bylo zavedeno; právním důvodem je souhlas nebo jiný právní důvod podle zákona o některých službách informační společnosti a dalších použitelných předpisů.

## 5. Uživatelský účet, zařízení a IoT data

Používání služby může vyžadovat vytvoření uživatelského účtu, ověření e-mailu a nastavení přístupových údajů. Přístup k účtu a administraci je chráněn rolemi a oprávněními. Uživatel může mít k účtu přiřazena zařízení, jejich nastavení, sdílení s dalšími osobami nebo provozní data získaná při používání zařízení.

Údaje o zařízeních mohou zahrnovat technické identifikátory, název, typ, kategorii, konfiguraci, vazbu na vlastníka, vazbu na sdílené uživatele, online nebo offline stav, provozní události, živá data, telemetrické údaje a příkazy předávané prostřednictvím interní nebo navazující technické služby, například Go/MQTT služby.

Správce zpracovává tato data proto, aby mohl službu provozovat, zobrazit uživateli stav zařízení, umožnit jejich správu, sdílení a bezpečné ovládání, řešit technické problémy a chránit službu proti zneužití. Přístup k údajům o zařízeních má být omezen podle vlastníka, sdílení a role uživatele.

Uživatel bere na vědomí, že názvy zařízení, popisy, poznámky, dokumenty a jiné volné vstupy mohou obsahovat osobní údaje. Do těchto polí by neměly být vkládány údaje, které nejsou pro účel používání služby nezbytné.

## 6. Provozní komunikace, dokumenty, souhlasy a podpora

Správce může uživateli zasílat provozní zprávy, které jsou nezbytné pro poskytování služby, zabezpečení účtu nebo splnění právních povinností. Jde například o ověření e-mailové adresy, obnovu hesla, potvrzení změny účtu, bezpečnostní upozornění, změnu povinných dokumentů nebo informaci o incidentu.

Při registraci, změně podmínek nebo při zpřístupnění nové funkce může správce vyžadovat potvrzení aktuální verze povinného dokumentu. Záznam o potvrzení se ukládá jako snapshot u účtu, včetně verze dokumentu, času potvrzení a vazby na uživatele. Historické potvrzení může být ponecháno pro prokazatelnost, i když uživatel později potvrzuje novější verzi dokumentu.

V rámci kontaktních formulářů, podpory, hlášení závad, reklamací nebo běžné e-mailové komunikace správce zpracovává údaje uvedené ve zprávě a technická metadata potřebná pro doručení a vyřízení požadavku. Obsah komunikace je uchováván pouze po dobu potřebnou k vyřízení požadavku, obraně právních nároků nebo splnění zákonné povinnosti.

## 7. Cookies, reCAPTCHA a technické úložiště

Služba v aktuálním stavu používá pouze nezbytné cookies a obdobné technické prostředky potřebné pro provoz webu, přihlášení, zabezpečení, session, jazykové nastavení a zobrazení informace o cookies. Podle dostupných technických podkladů nejsou ve veřejné části služby používány Google Analytics ani marketingové cookies.

• session cookie, například PHPSESSID nebo jiný název podle produkční konfigurace, slouží pro přihlášení, stav relace a bezpečnost formulářů a trvá zpravidla po dobu relace nebo podle serverového nastavení;

• REMEMBERME slouží k zapamatování přihlášení uživatele a podle aktuální konfigurace je uchovávána po dobu 30 dní;

• locale slouží k zapamatování jazykové volby a je uchovávána zpravidla po dobu 1 roku;

• naxter_cookie_consent slouží k uložení informace o zobrazení nastavení cookies a je uchovávána po dobu 180 dní;

• Google reCAPTCHA nebo cookie _GRECAPTCHA mohou být použity jako bezpečnostní opatření na přihlašovacích, registračních, obnovovacích, kontaktních nebo jiných citlivějších formulářích; doba uložení se řídí nastavením a podmínkami poskytovatele služby.

Cookie lišta nebo tlačítko „Nastavení cookies“ v patičce slouží v aktuálním stavu jako informační panel pro nezbytné cookies. U nezbytných cookies není v liště možnost jejich vypnutí, protože bez nich by služba nemohla řádně fungovat. Pokud by správce v budoucnu přidal analytické, marketingové nebo jiné volitelné cookies, budou před udělením souhlasu vypnuté a uživatel bude mít možnost souhlas později obdobně snadno odvolat.

Služba může ukládat některé technické nebo preferenční informace také do localStorage nebo sessionStorage, například pro uživatelské rozhraní nebo dočasné provozní stavy. Některé šablony mohou načítat externí technické zdroje, například fonty, ikony, Bootstrap, jQuery nebo obdobné knihovny; takové požadavky mohou znamenat předání technických údajů, jako je IP adresa a user-agent, poskytovateli příslušného zdroje.

## 8. Komu mohou být osobní údaje zpřístupněny

Osobní údaje mohou být zpřístupněny pouze v rozsahu nezbytném pro konkrétní účel a pouze osobám nebo dodavatelům, kteří je pro daný účel potřebují. Typicky může jít o tyto kategorie příjemců:

• oprávněné osoby správce, administrátory, technickou podporu, vývojáře nebo další spolupracovníky, kteří se podílejí na provozu, bezpečnosti, údržbě nebo vývoji služby;

• poskytovatele hostingu, serverové infrastruktury, databází, úložišť, záloh, monitoringu a obdobných technických služeb;

• poskytovatele e-mailového odesílání, SMTP služeb, doručování provozních zpráv a podpory;

• externí technické správce, vývojáře, servisní osoby nebo bezpečnostní konzultanty, pokud je jejich zapojení potřebné pro údržbu, incident, migraci nebo rozvoj služby;

• Google služby, zejména reCAPTCHA pro ochranu formulářů a Google OAuth pro volitelné přihlášení přes Google, pokud je příslušná funkce zapnuta;

• poskytovatele externích CDN nebo technických zdrojů, pokud jsou ve webu skutečně načítány;

• účetní, daňové, právní nebo obdobné poradce, pokud je to potřebné pro splnění právních povinností nebo ochranu práv správce;

• orgány veřejné moci, soudy, policii, dozorové orgány nebo jiné oprávněné subjekty, pokud to vyžaduje právní předpis nebo ochrana práv správce či třetích osob.

Správce průběžně vyhodnocuje, kteří příjemci jsou pro provoz služby skutečně používáni. S dodavateli, kteří vystupují jako zpracovatelé osobních údajů, správce uzavírá odpovídající smlouvy nebo využívá smluvní podmínky obsahující zpracovatelská ujednání, pokud to vyžaduje GDPR.

## 9. Předávání osobních údajů mimo EU a EHP

Správce se snaží volit takové technické a smluvní partnery, aby zpracování osobních údajů probíhalo přednostně v Evropské unii nebo Evropském hospodářském prostoru a aby případné přenosy mimo EU nebo EHP byly omezeny na nezbytný rozsah.

K předání mimo EU nebo EHP může dojít zejména tehdy, pokud je konkrétní dodavatel usazen mimo EU nebo EHP, využívá podpůrnou infrastrukturu nebo podzpracovatele mimo EU nebo EHP, nebo pokud to vyplývá z povahy globální technické služby, například reCAPTCHA, Google OAuth, některých CDN, e-mailových, hostingových nebo bezpečnostních služeb.

Pokud k takovému předání dochází nebo může docházet, správce zajistí odpovídající právní mechanismus podle GDPR, zejména rozhodnutí o odpovídající ochraně, standardní smluvní doložky, doplňující technická a organizační opatření nebo jiný mechanismus uznaný právem EU. Předání se vždy omezuje na údaje nezbytné pro konkrétní účel.

## 10. Doba uchování osobních údajů

Správce uchovává osobní údaje pouze po dobu nezbytnou k naplnění konkrétního účelu, k ochraně práv správce a uživatelů a po dobu vyžadovanou právními předpisy. Konkrétní doba se může lišit podle typu údaje, nastavení služby, technických možností mazání a existence právního důvodu pro další uchování.

• údaje aktivního uživatelského účtu se uchovávají po dobu používání služby; po výmazu účtu jsou smazány nebo anonymizovány bez zbytečného odkladu, pokud není nutné ponechat je z důvodu zákonné povinnosti, bezpečnosti nebo právního nároku;

• snapshoty povinných dokumentů a souhlasů se uchovávají po dobu trvání účtu a po dobu potřebnou k prokázání splnění smluvních nebo právních povinností;

• deaktivovaný účet může být omezeně uchováván zpravidla po dobu až 24 měsíců, pokud je to odůvodněno obnovou účtu, bezpečností, provozem služby nebo ochranou práv;

• volitelný telefon se uchovává po dobu trvání účtu nebo do odstranění údaje uživatelem či správcem;

• údaje o zařízeních a jejich nastavení se uchovávají po dobu aktivního účtu, vlastnictví nebo sdílení zařízení; po odstranění zařízení se nepotřebná data smažou nebo anonymizují;

• historická živá nebo telemetrická data zařízení se uchovávají v rozsahu potřebném pro funkčnost, diagnostiku, bezpečnost a očekávání uživatele, zpravidla v řádu 3 až 12 měsíců, pokud konkrétní nastavení služby nestanoví jinak;

• kontaktní formuláře, podpora, reklamace a běžná komunikace se uchovávají zpravidla 12 měsíců od vyřízení, déle jen při sporu, právním nároku, incidentu nebo navazujícím smluvním vztahu;

• provozní logy se uchovávají zpravidla 6 měsíců a bezpečnostní logy zpravidla 12 měsíců, déle pouze při incidentu, podezření na zneužití nebo právním nároku;

• cookie naxter_cookie_consent se uchovává 180 dní, REMEMBERME 30 dní, locale zpravidla 1 rok a session cookie po dobu relace nebo podle serverového nastavení;

• zálohy se uchovávají podle zálohovacího plánu zpravidla 30 až 90 dní; pokud není technicky možné odstranit konkrétní údaj přímo ze zálohy, bude odstraněn při rotaci zálohy nebo znovu po případné obnově.

## 11. Automatizované zpracování, AI a ruční posouzení

Správce v rámci běžného provozu služby nepoužívá výhradně automatizované rozhodování, včetně profilování, které by vůči uživateli mělo právní účinky nebo se jej obdobně významně dotýkalo ve smyslu čl. 22 GDPR.

Některé bezpečnostní funkce mohou být automatizované, například ochrana proti spamu, automatizovaným útokům, podezřelému přihlášení nebo zneužití formulářů prostřednictvím reCAPTCHA, bezpečnostních logů a pravidel aplikace. Tyto procesy slouží k ochraně služby a zpravidla nevedou samy o sobě k rozhodnutí s právními účinky bez možnosti následného přezkumu.

Pokud by správce v budoucnu použil AI systém nebo automatizovaný nástroj pro funkci, která může významně zasahovat do práv uživatele, zajistí odpovídající informování, přiměřená technická a organizační opatření, lidský dohled a možnost přezkumu tam, kde to vyžaduje GDPR, akt o umělé inteligenci nebo jiný použitelný právní předpis.

Pokud by služba umožňovala veřejné šíření uživatelského obsahu nebo jinou činnost spadající pod pravidla digitálních služeb, správce nastaví navazující postupy oznámení, omezení obsahu a

případného přezkumu v souladu s použitelnými pravidly pro digitální služby. Tato ustanovení nemění práva subjektů údajů podle GDPR.

## 12. Jaká práva má uživatel

V rozsahu stanoveném GDPR a dalšími právními předpisy může subjekt údajů vůči správci uplatnit zejména tato práva:

• právo na přístup k osobním údajům a informace o jejich zpracování;

• právo na opravu nepřesných nebo neúplných údajů;

• právo na výmaz, je-li splněn některý ze zákonných důvodů;

• právo na omezení zpracování;

• právo na přenositelnost údajů, pokud se zpracování opírá o souhlas nebo o smlouvu a probíhá automatizovaně;

• právo vznést námitku proti zpracování založenému na oprávněném zájmu;

• právo odvolat souhlas, je-li zpracování na souhlasu založeno; odvoláním souhlasu není dotčena zákonnost zpracování před jeho odvoláním;

• právo nebýt předmětem výhradně automatizovaného rozhodnutí s právními nebo obdobně významnými účinky, pokud pro takové rozhodnutí nejsou splněny zákonné podmínky;

• právo podat stížnost u Úřadu pro ochranu osobních údajů.

Žádosti lze zasílat na e-mail info@naxter.cz. Správce může před vyřízením žádosti přiměřeně ověřit identitu žadatele, zejména proto, aby nedošlo k poskytnutí osobních údajů neoprávněné osobě. Žádost je vyřizována bez zbytečného odkladu, zpravidla nejpozději do 1 měsíce od obdržení. U složitých nebo vícečetných žádostí může být lhůta prodloužena až o další 2 měsíce; o prodloužení a jeho důvodech bude žadatel informován v původní měsíční lhůtě.

Domnívá-li se subjekt údajů, že při zpracování jeho osobních údajů došlo k porušení právních předpisů, může se obrátit na Úřad pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7, web uoou.gov.cz.

## 13. Zabezpečení osobních údajů

Správce přijímá odpovídající technická a organizační opatření k ochraně osobních údajů před neoprávněným přístupem, ztrátou, zneužitím, změnou, zničením nebo jiným porušením zabezpečení. Opatření odpovídají povaze údajů, rizikům zpracování a technickým možnostem služby.

Mezi používaná nebo plánovaná opatření patří zejména omezení přístupu podle rolí, hashování hesel, možnost dvoufázového ověření přes TOTP, CSRF ochrana formulářů, reCAPTCHA pro citlivější veřejné formuláře, provoz přes HTTPS, ochrana secretů mimo veřejné repozitáře, omezení přístupů k logům a zálohám, rotace logů a záloh, pravidelná kontrola bezpečnostních událostí a minimalizace přístupů vývojářů k produkčním datům.

Logy by neměly obsahovat hesla, TOTP secrety, OAuth secrety, API klíče ani celé hodnoty session. Přístupy externích správců mají být osobní, přiměřené účelu, časově omezené a pravidelně kontrolované. Zálohy mají být chráněny proti neoprávněnému přístupu a obnova dat má být pravidelně testována.

Pokud dojde k porušení zabezpečení osobních údajů, správce posoudí riziko pro práva a svobody fyzických osob. Je-li to vyžadováno GDPR, oznámí porušení dozorovému úřadu bez zbytečného odkladu, pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, a v případě vysokého rizika informuje také dotčené osoby.

Žádné technické řešení nemůže zaručit absolutní bezpečnost. Uživatelé by měli chránit své přístupové údaje, používat silná hesla, nepředávat účet třetím osobám a zapnout dvoufázové ověření, pokud je dostupné.

## 14. Změny těchto zásad

Správce je oprávněn tyto zásady v přiměřeném rozsahu měnit, zejména pokud dojde ke změně služby, zpracovávaných údajů, účelů zpracování, dodavatelů, cookies, právních předpisů nebo technických a organizačních opatření.

Nové znění zásad správce zveřejní ve službě nebo o něm uživatele vhodným způsobem informuje. Pokud změna vyžaduje nové potvrzení nebo souhlas, může být uživatel vyzván k potvrzení aktuální verze dokumentu před dalším používáním příslušné funkce služby.

Tyto zásady jsou účinné ve verzi 07.05.2026.