

# GDPR provozní příručka

## Postupy pro žádosti fyzických osob, incidenty, retenci a ukončení služby GPcloud.app

Příručka převádí smluvní a bezpečnostní závazky GPcloud.app do opakovatelných interních postupů. Každý požadavek nebo incident musí mít vlastní evidenční číslo, odpovědnou osobu, časovou osu, doložené rozhodnutí a uzavírací kontrolu. Bez vyplnění rolí a kontaktů nelze tento dokument považovat za zavedený proces.

## 1 Vlastnictví procesu

| Role                       | Odpovědnost                                                   | Osoba nebo kontakt                |
|----------------------------|---------------------------------------------------------------|-----------------------------------|
| Vlastník ochrany údajů     | Řídí žádosti, incidenty, evidenci a právní konzultace.        | Jakub Jursík, info@gpcloud.app    |
| Technický správce          | Zajišťuje logy, exporty, omezení přístupu, obnovu a výmaz.    | Jakub Jursík, info@gpcloud.app    |
| Obchodní a smluvní kontakt | Ověřuje zákazníka, smlouvu, kontakty a rozsah služby.         | Jakub Jursík, info@gpcloud.app    |
| Bezpečnostní pohotovost    | Přijímá hlášení mimo běžnou podporu a spouští triáž.          | info@gpcloud.app; telefon doplnit |
| Právní konzultant          | Posuzuje oznamovací povinnosti, spory a nestandardní žádosti. | [DOPLNIT]                         |

Jedna osoba může zastávat více rolí, ale každá role musí mít určeného zástupce. Přístup k evidenci žádostí a incidentů je omezen na osoby, které jej potřebují.

## 2 Rozlišení role GPcloud

| Situace                                                              | Role GPcloud | Hlavní postup                                                                               |
|----------------------------------------------------------------------|--------------|---------------------------------------------------------------------------------------------|
| Údaje zájemců, smluvních kontaktů, fakturace a vlastní podpory       | Správce      | GPcloud ověří žadatele, rozhodne o žádosti a odpoví přímo.                                  |
| Obsah zákaznické instance, například zaměstnanci, docházka a tickety | Zpracovatel  | Žádost se předá zákazníkovi jako správci; GPcloud poskytne doloženou technickou součinnost. |
| Bezpečnostní incident v zákaznické instanci                          | Zpracovatel  | GPcloud informuje zákazníka bez zbytečného odkladu a předá dostupné podklady.               |
| Incident ve vlastní zákaznické nebo fakturační evidenci GPcloud      | Správce      | GPcloud provede posouzení rizika a rozhodne o oznámeních.                                   |

## 3 Příjem a evidence žádosti fyzické osoby

1. Zapište datum a čas přijetí, kanál, kontaktní údaje žadatele a přesné znění žádosti.
2. Přidělte evidenční číslo ve tvaru GDPR RRRR pořadové číslo a vlastníka případu.
3. Určete, zda GPcloud jedná jako správce nebo zpracovatel a kterého zákazníka se žádost týká.
4. Ověřte totožnost přiměřeně riziku. Nevyžadujte kopii dokladu automaticky; použijte méně invazivní ověření, pokud postačuje.

- Potvrďte přijetí a zaznamenejte zákonnou lhůtu. Standardně se odpovídá bez zbytečného odkladu, nejpozději do jednoho měsíce; případné prodloužení musí být včas odůvodněno.
- Vyhledejte pouze relevantní systémy, minimalizujte zpřístupněné údaje a chraňte práva jiných osob.
- Nechte odpověď schválit vlastníkem ochrany údajů a bezpečně ji doručte.
- Zapište výsledek, datum uzavření, provedené zásahy a místo uložených důkazů.

### Evidenční list žádosti

| Pole                            | Záznam                                                                                                                                                                                                                                               |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Evidenční číslo a datum přijetí | [DOPLNIT]                                                                                                                                                                                                                                            |
| Žadatel a způsob ověření        | [DOPLNIT]                                                                                                                                                                                                                                            |
| Dotčený zákazník nebo systém    | [DOPLNIT]                                                                                                                                                                                                                                            |
| Role GPcloud                    | <input type="checkbox"/> správce <input type="checkbox"/> zpracovatel <input type="checkbox"/> vyžaduje posouzení                                                                                                                                    |
| Typ žádosti                     | <input type="checkbox"/> přístup <input type="checkbox"/> oprava <input type="checkbox"/> výmaz <input type="checkbox"/> omezení <input type="checkbox"/> přenositelnost <input type="checkbox"/> námitka <input type="checkbox"/> odvolání souhlasu |
| Lhůta a vlastník                | [DOPLNIT]                                                                                                                                                                                                                                            |
| Rozhodnutí a provedené kroky    | [DOPLNIT]                                                                                                                                                                                                                                            |
| Datum a způsob odpovědi         | [DOPLNIT]                                                                                                                                                                                                                                            |
| Důkazy a datum uzavření         | [DOPLNIT]                                                                                                                                                                                                                                            |

## 4 Reakce na bezpečnostní incident

Každé podezření se nejprve eviduje jako bezpečnostní událost. Za porušení zabezpečení osobních údajů se označí až po potvrzení, že došlo k náhodnému nebo protiprávnímu zničení, ztrátě, změně, neoprávněnému zpřístupnění nebo přístupu k osobním údajům.

- Zaznamenejte čas zjištění a neprodleně aktivujte vlastníka incidentu.
- Omezte dopad vratným způsobem: zneplatněte kompromitovaný přístup, izolujte dotčenou službu a zachovejte důkazy.
- Určete dotčené systémy, zákazníky, kategorie osob a údajů, přibližný rozsah a časové období.
- Posuďte dopad na důvěrnost, integritu a dostupnost a pravděpodobnost újmy fyzickým osobám.
- Jedná li GPcloud jako zpracovatel, informujte dotčeného zákazníka bez zbytečného odkladu a informace průběžně doplňujte.
- Jedná li GPcloud jako správce a je pravděpodobné riziko pro práva a svobody osob, připravte oznámení dozorovému úřadu. Zákonná lhůta je pokud možno do 72 hodin od okamžiku, kdy se správce o porušení dozvěděl.
- Při pravděpodobném vysokém riziku připravte s právníkem také srozumitelné oznámení dotčeným osobám, není li splněna zákonná výjimka.
- Obnovte bezpečný provoz, ověřte integritu a dostupnost, zdokumentujte příčinu a proveďte nápravná opatření.
- Incident uzavřete až po kontrole účinnosti opatření. Evidujte i případy, které nebyly oznamovány, včetně odůvodnění.

### Evidenční list incidentu

| Pole                                       | Záznam    |
|--------------------------------------------|-----------|
| Číslo, čas zjištění a oznamovatel          | [DOPLNIT] |
| Dotčené systémy a zákazníci                | [DOPLNIT] |
| Kategorie a přibližný počet osob a záznamů | [DOPLNIT] |

| Pole                                       | Záznam                                                                                                                                |
|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Dopad na důvěrnost, integritu a dostupnost | [DOPLNIT]                                                                                                                             |
| Okamžitá opatření a zachované důkazy       | [DOPLNIT]                                                                                                                             |
| Role GPcloud                               | <input type="checkbox"/> správce <input type="checkbox"/> zpracovatel <input type="checkbox"/> obě role                               |
| Hodnocení rizika                           | <input type="checkbox"/> nepravděpodobné <input type="checkbox"/> riziko <input type="checkbox"/> vysoké riziko; odůvodnění [DOPLNIT] |
| Zákazník informován                        | [DOPLNIT čas, kontakt a obsah]                                                                                                        |
| ÚOOÚ a dotčené osoby                       | [DOPLNIT rozhodnutí, čas a důvod]                                                                                                     |
| Příčina, náprava a datum uzavření          | [DOPLNIT]                                                                                                                             |

## 5 Retence a pravidelná kontrola

Retenční lhůty musí odpovídat právnímu účelu, smlouvám a skutečné konfiguraci systémů. Vlastník ochrany údajů provede nejméně jednou ročně kontrolu a po každé významné změně služby.

| Oblast                            | Pravidlo před schválením                                                             | Kontrolní důkaz                                         |
|-----------------------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------|
| Poptávky                          | Navrženě 12 měsíců od posledního kontaktu, není li jiný legitimní důvod.             | Výpis nebo protokol výmazu                              |
| Smlouvy a fakturace               | Podle účetních, daňových a promlčecích povinností po právní revizi.                  | Retenční matice schválená právníkem a účetní            |
| Podpora                           | Navrženě 3 roky po uzavření, delší pouze s doloženým důvodem.                        | Uzavřené tickety a protokol mazání                      |
| Aplikační logy a výstup plánovače | 30 dnů; denní soubory se automaticky odstraní po uplynutí lhůty.                     | Úloha logging.prune denně v 03.05 a kontrola scheduleru |
| Logy webserveru                   | Týdenní rotace a 5 archivních souborů, obvykle přibližně 5 až 6 týdnů.               | Konfigurace hostingu a namátková kontrola               |
| Zákaznická data po ukončení       | Exportní okno 30 dnů, poté řízený výmaz aktivních dat.                               | Předávací a likvidační protokol                         |
| Zálohy                            | Odstranění uplynutím schváleného retenčního cyklu; po dobu retence pouze pro obnovu. | Seznam záloh, Object Lock a retenční test               |
| Žádosti a incidenty               | Po dobu potřebnou k doložení souladu a ochraně práv, po právní revizi.               | Evidence případů a roční kontrola                       |

## 6 Ukončení služby a likvidace dat

- Potvrďte oprávněný požadavek na ukončení, datum konce a osoby oprávněné převzít export.
- Vytvořte dohodnutý export a bezpečně jej předejte; zaznamenejte kontrolní součet a potvrzení převzetí.
- Po uplynutí exportního okna zablokujte účty a integrace a odeberte provozní secrets a licenční dokument.
- Odstraňte aktivní databázi, zákaznické soubory, pracovní exporty a dočasné kopie podle schváleného checklistu.
- Záložní kopie ponechte pouze do vypršení nezměnitelné retenční lhůty; nesmějí být použity k běžnému provozu.
- Vystavte likvidační protokol s tenantem, rozsahem, daty, provádějící a kontrolující osobou a zbývajících zálohami s termínem expirace.

| Kontrola ukončení             | Stav a důkaz                                                                                                   |
|-------------------------------|----------------------------------------------------------------------------------------------------------------|
| Export předán oprávněné osobě | <input type="checkbox"/> ano <input type="checkbox"/> ne <input type="checkbox"/> nepoužije se [DOPLNIT důkaz] |

| Kontrola ukončení                       | Stav a důkaz                                                       |
|-----------------------------------------|--------------------------------------------------------------------|
| Účty a integrace zneplatněny            | <input type="checkbox"/> ano <input type="checkbox"/> ne [DOPLNIT] |
| Aktivní data a dočasné kopie odstraněny | <input type="checkbox"/> ano <input type="checkbox"/> ne [DOPLNIT] |
| Zbývajících záloh a datum expirace      | [DOPLNIT]                                                          |
| Kontrola druhou osobou                  | [DOPLNIT jméno, datum a podpis]                                    |
| Zákazník informován                     | [DOPLNIT datum a způsob]                                           |

## 7 Pravidelné důkazy připravenosti

| Interval   | Kontrola                                                                          | Výstup                                    |
|------------|-----------------------------------------------------------------------------------|-------------------------------------------|
| Měsíčně    | Neuzavřené žádosti a incidenty, selhání záloh a upozornění.                       | Kontrolní zápis                           |
| Čtvrtletně | Oprávnění administrátorů, účty dodavatelů a kontakty pohotovosti.                 | Revize přístupů                           |
| Pololetně  | Test obnovy, exportu a řízeného výmazu na neprodukčních datech.                   | Protokol testu                            |
| Ročně      | Retenční matice, seznam subzpracovatelů, DPA, veřejné informace a rizika.         | Schválená roční revize                    |
| Po změně   | Nový modul, dodavatel, země zpracování, typ údajů nebo bezpečnostní architektura. | Posouzení změny a aktualizované dokumenty |

## 8 Stav zavedení

| Předpoklad              | Aktuální stav                                                                                                                                                     |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Veřejné informace a DPA | Identita provozovatele doplněna; pracovní návrhy čekají na právní revizi.                                                                                         |
| Externí zálohy          | Backblaze B2 v regionu EU Central je aktivní s omezeným klíčem a Object Lock. Integrita, obnova souborů a ostrý databázový restore drill byly ověřeny 9. 9. 2026. |
| Kontaktní role          | Primárně obsazeny: Jakub Jursík, info@gpcloud.app; doplnit zástupce.                                                                                              |
| Retence logů            | Zavedena: aplikační logy a výstup plánovače 30 dnů; webserver přibližně 5 až 6 týdnů.                                                                             |
| Incidentní kanál        | E mail info@gpcloud.app; čeká na telefon a zastupitelnost.                                                                                                        |

## Právní podklady

- Nařízení Evropského parlamentu a Rady EU 2016 679, zejména články 12, 15 až 22, 28, 32 až 34 a 30.
- Metodické informace Úřadu pro ochranu osobních údajů k právům subjektů, správcům a zpracovatelům a bezpečnostním incidentům.
- Smlouva o zpracování osobních údajů a technická a organizační opatření GPcloud.app po jejich právní revizi.