

**Supplementary Privacy Policy
for
the IstroSec Gryphon computer program**

Version: 1.0

Effective Date: January 1st 2026

1. Introduction

This privacy policy ("policy" or "privacy policy") explains how personal data is collected, processed, and protected when using the IstroSec Gryphon computer program ("Gryphon").

These policy for the IstroSec Gryphon computer program are fully subject to the general Privacy Policy of IstroSec, with its registered office at Černyševského 10, 851 01 Bratislava, Slovakia, registered under ID No. 53 849 060 ("IstroSec"), apply in full to this privacy policy for the IstroSec Gryphon computer program, with specific circumstances relating to the processing of personal data when using Gryphon included in this privacy policy.

In this regard, the Gryphon user acknowledges that this privacy policy does not replace the specific obligations of the Gryphon user arising from Articles 13 and 14 of the GDPR when using Gryphon.

2. Types of personal data processed

As part of Gryphon's protection against ransomware attacks, a wide range of personal data may be processed in order to detect types of behavior (activities) indicating that a security incident (e.g., a ransomware attack) is being prepared or is in progress. In this context, the following types of personal data may be processed within Gryphon:

Identification data: e.g., user's first and last name, user name (nickname).

**Doplnkové Zásady ochrany osobných
údajov
k
počítačovému programu IstroSec
Gryphon**

Verzia: 1.0

Dátum účinnosti: 1. januára 2026

1. Úvod

Tieto zásady ochrany osobných údajov („zásady“ alebo „zásady ochrany osobných údajov“) vysvetľujú, ako sú zhromažďované, spracúvané a chránené osobné údaje pri používaní počítačového programu IstroSec Gryphon („Gryphon“).

Na tieto zásady ochrany osobných údajov k počítačovému programu IstroSec Gryphon sa v celom rozsahu aplikujú všeobecné Zásady ochrany súkromia spoločnosti IstroSec, so sídlom na adrese Černyševského 10, 851 01 Bratislava, Slovensko, registrovanú pod číslom IČO 53 849 060 („**IstroSec**“), pričom špecifické okolnosti týkajúce sa spracúvania osobných údajov pri použití Gryphon sú zahrnuté do týchto zásad ochrany osobných údajov.

Používateľ Gryphon v tejto súvislosti berie na vedomie, že tieto zásady ochrany osobných údajov nenahrádzajú osobitné povinnosti používateľa Gryphon vyplývajúce z čl. 13 a 14 GDPR pri používaní Gryphon.

2. Typy spracúvaných osobných údajov

V rámci Gryphon ako ochrany pred útokmi typu ransomvér môže byť spracúvaný široký rozsah osobných údajov v záujme odhalenia typu správania (aktivít) nasvedčujúcich tomu, že sa pripravuje alebo prebieha bezpečnostný incident (napr. ransomvérový útok). V tejto súvislosti môžu byť v rámci Gryphon spracúvané nasledovné typy osobných údajov:

Identifikačné údaje: napr. meno a priezvisko používateľa, označenie používateľa (nickname).

Contact details: e.g., user's place of residence/correspondence address, user's email address, user's telephone number.

Technical and operational data from end devices: e.g., IP address, MAC address of the device.

Other data: e.g., operating records (e.g., user activities, access attempts, data flows, system errors), metadata (e.g., name, type, file size, date of creation/change).

3. Data Retention

Data processed in connection with the operation of Gryphon (e.g., technical/operational data, MAC address, IP address, license, etc.) is stored for as long as the user uses the service and, after termination of use, is processed in pseudonymized or anonymized form (it is no longer personal data).

Data processed for the purposes of improving and optimizing the service (analytics, abuse prevention) is stored for the duration of the service use and then for 3 years after its termination.

Data processed in connection with inquiries and requests from customers (users) is stored for a maximum of 1 year after the request has been processed.

Data processed in connection with the exercise of the rights of data subjects (e.g., requests for access to data) is stored for 5 years from the date of processing the data subject's request or the expiry of the deadline for processing the request, and for 1 year from the expiry of the relevant 5-year period.

4. Data Security

Within Gryphon and related personal data processing operations, appropriate technical and organizational measures have been implemented to ensure security commensurate with the risks. These measures include:

Kontaktné údaje: napr. bydlisko / korešpondenčná adresa používateľa, emailová adresa používateľa, telefónne číslo používateľa.

Technické a operatívne údaje z koncových zariadení: napr. IP adresa, MAC adresa zariadenia.

Ďalšie údaje: napr. prevádzkové záznamy (napr. aktivity používateľov, pokusy o prístup, toky dát, chyby systému), metadáta (napr. názov, typ, veľkosť súboru, dátum vytvorenia / zmeny).

3. Uchovávanie údajov

Údaje spracúvané v súvislosti s prevádzkou Gryphon (napr. technické/operatívne údaje, MAC adresa, IP adresa, licencia a podobne) sa uchovávajú počas obdobia, kým používateľ využíva službu, a po ukončení využívania sa spracúvajú vo forme pseudonymizovanej alebo anonymizovanej (viac sa nejedná o osobné údaje).

Údaje spracúvané pre účely zlepšovania a optimalizácie služby (analytika, prevencia zneužitia) sa uchovávajú počas obdobia využívania služby a následne 3 roky po jej ukončení.

Údaje spracúvané v súvislosti s dopytmi, požiadavkami zákazníkov (používateľov) sa uchovávajú maximálne 1 rok po vybavení požiadavky.

Údaje spracúvané v súvislosti s výkonom práv dotknutých osôb (napr. žiadosť o prístup k údajom) sa uchovávajú po dobu 5 rokov od vybavenia žiadosti dotknutej osoby alebo márneho uplynutia lehoty na vybavenie žiadosti a 1 rok od uplynutia príslušnej lehoty 5 rokov.

4. Bezpečnosť údajov

V rámci Gryphon a súvisiacich spracovateľských operácií s osobnými údajmi pri jeho používaní boli implementované primerané technické a organizačné opatrenia pre zaručenie bezpečnosti zodpovedajúcej rizikám. Medzi tieto opatrenia patria:

- encryption of data during transmission and storage ("encryption in transit and at rest"),
- role-based access policies (RBAC) – access is restricted to authorized users only,
- monitoring of incidents and audits of processing operations,
- data backup and recovery capability,
- regular testing and evaluation of security measures.
- šifrovanie údajov pri prenosoch a uchovávaní („encryption in transit and at rest“),
- prístupové politiky založené na role (RBAC) – prístup patrí len oprávneným používateľom,
- monitorovanie incidentov a auditov spracovateľských operácií,
- zálohovanie údajov a možnosť obnovy,
- pravidelné testovanie a hodnotenie bezpečnostných opatrení.

5. Changes to This Privacy Policy and Language Versions

IstroSec may occasionally update or revise this Privacy Policy. Any changes will be announced through an updated version posted on the IstroSec website.

In the event of any inconsistency between a translated version of this Privacy Policy and the English-language version, the Slovak-language version shall prevail and be considered the authoritative text.

6. Contact Details

For more information about IstroSec's privacy practices or this Privacy Policy, please contact us at:

Email: gdpr@istrosec.com

We appreciate your assistance in keeping your personal data accurate. If you believe that any data we process about you is incorrect, please let us know at gdpr@istrosec.com.

5. Zmeny týchto zásad ochrany osobných údajov a jazykové verzie

Spoločnosť IstroSec môže tieto zásady ochrany osobných údajov príležitostne aktualizovať alebo revidovať. Akékoľvek zmeny budú oznámené prostredníctvom aktualizovanej verzie uverejnenej na webovej stránke spoločnosti IstroSec.

V prípade akýchkoľvek nezrovnalostí medzi preloženou verziou týchto zásad ochrany osobných údajov a anglickou verziou má prednosť slovenská verzia, ktorá sa považuje za záväzný text.

6. Kontaktné údaje

Pre viac informácií o postupoch spoločnosti IstroSec v oblasti ochrany osobných údajov alebo o týchto zásadách ochrany osobných údajov nás kontaktujte na adrese:

E-mail: gdpr@istrosec.com

Ďakujeme vám za pomoc pri udržiavaní správnosti vašich osobných údajov. Ak sa domnievate, že akékoľvek údaje, ktoré o vás spracúvame, sú nesprávne, informujte nás o tom na adrese gdpr@istrosec.com.