# Sažetak Opštih sigurnosnih politika Osiguravajuće grupe Sava

Ljubljana, april 2025.

**Kazalo**

# 1 UVOD

Ovaj dokument sažima ključne opšte sigurnosne politike Osiguravajuće grupe Sava (u daljnjem tekstu OGS) prilagođene za javnu objavu za potrebe dobavljača. Namijenjen je svim ugovornim partnerima koji u svojem radu i za izvršenje ugovorenih usluga pristupaju ili koriste bilo koje ICT resurse (npr. aplikacije, telekomunikacijsku opremu, zbirke podataka i dr.).

Ovaj sažetak uključuje sljedeći sadržaj:

- pravilno korišćenje svih izvora informacija, odnosno ICT resursa,
- upravljanje informacijskim resursima, odnosno ICT resursima,
- elektroničko poslovanje,
- zaštita opreme i informacijskih resursa, odnosno ICT resursa.

Donošenjem Opštih sigurnosnih OGS politika dobavljač (ugovorni partner) se obvezuje da će u izvršenju ugovornih obveza poštovati sigurnosne zahtjeve informacijske tehnologije u skladu sa važećim dobrim praksama, minimalnim standardima i načelima struke te važećim propisima.

# 2 SVRHA I OPSEG SIGURNOSNIH POLITIKA

Svrha je sigurnosnih politika u OGS:

- osiguranje sigurnog i primjerenog korišćenja ICT resursa,
- informiranje korisnika o rizicima povezanim sa korišćenjem ICT resursa,
- definisanje mjera bezbijednosti informacija od neovlaštenog otkrivanja ili zlouporabe.

Ugovorni korisnici moraju sve ICT resurse OGS-a koristiti savjesno, učinkovito i odgovorno.

OGS u najvećoj mogućoj mjeri štiti svoje zaposlenike i svoju imovinu od nezakonitih ili štetnih namjernih ili nenamjernih aktivnosti pojedinaca.

Neodgovarajuće korišćenje informacijske tehnologije izlaže OGS i njezine korisnike rizicima kao što su zaraze informacijske tehnologije računalnim virusima, prijetnje mrežnim sistemima i uslugama te zlouporaba informacija i podataka pohranjenih u informacijskom sistemu OGS-a.

# 3 OPŠTI ZAHTJEVI

- Dobavljač se mora pridržavati svih važećih zakona i propisa, uključujući i Opštu uredbu o zaštiti podataka (GDPR) i Uredbu o digitalnoj operativnoj otpornosti za finansijski sektor (DORA).
- Dobavljač mora da imenuje lice za kontakt za sigurnosne komunikacije i odgovor na incidente.

# 4 UPRAVLJANJE PRISTUPOM

- Dobavljač mora da uspostavi stroge kontrole kako bi spriječio pristup neovlaštenih lica ICT sistemima OGS-a.
- Dobavljač mora da uspostavi stroge kontrole, čime osigurava da ICT sistemima OGS-a pristupaju samo ovlaštena lica koja su propisno provjerena i osposobljena.
- Upravljanje pristupom odnosi se na sve oblike pristupa ICT resursima, što, između ostalog, uključuje:
    - korisnički pristup putem korisničkih sučelja (GUI),
    - pristup putem programskih sučelja (API),
    - pristupe sistemu/uslugama (servisni računi),

  - administratorske i povlaštene pristupe,
  - skripte, cron poslove (angl. cron job) i automatizovane integracije,
  - udaljene pristupe (VPN, RDP, SSH i dr.),
  - pristupe putem mobilnih uređaja ili oblaka.
- Zaštita pristupa ICT sistemima OGS-a, između ostalog, uključuje i višefaktorsku autentifikaciju (MFA) i primjenu načela najmanje privilegije (angl. least privilege).
- Svi pristupi sistemima i podacima povezanim sa OGS-om bilježe se i prate zbog osiguranja revizijskog traga.
- Dobavljač mora da održava ažuriran popis ovlaštenih lica s podacima za pristup ICT sistemima OGS-a i redovito ga pregledava.

## 5 ZAŠTITA PODATAKA

- Dobavljač mora da osigura cjelovitost, povjerljivost i raspoloživost podataka.
- Svi podaci moraju tijekom prijenosa biti šifrirani primjenom kriptografskog protokola TLS 1.2 ili novije verzije.
- Svi podaci koji miruju, uključujući sigurnosne kopije, moraju biti šifrirani primjenom AES-256 standarda ili ekvivalentnog standarda.
- Dobavljač mora osigurati da se radna računala koja se koriste za obavljanje ugovorne usluge redovito sigurnosno ažuriraju, imaju instaliran isključivo legalni softver i da su zaštićena redovito ažuriranim antivirusnim sistemom.
- Dobavljač mora da osigura minimalnu obradu i pohranu podataka, pri čemu smije obrađivati i pohranjivati samo one podatke koji su prijeko potrebni da se izvrši ugovorna obveza.
- Dobavljač mora izbjegavati nepotrebno pohranjivanje podataka i osigurati da se podaci izbrišu ili anonimiziraju odmah nakon što prestane potreba za pohranjivanjem.
- Nakon prestanka ugovornog odnosa dobavljač mora podatke sigurno da izbriše ili u cijelosti vrati OGS-u.

## 6 UPRAVLJANJE INCIDENTIMA

- Dobavljač mora imati politiku upravljanja incidentima koja uključuje otkrivanje, izvještavanje i rješavanje sigurnosnih incidenata.
- Sigurnosni incidenti dobavljača koji utječu na OGS moraju biti prijavljeni OGS-u u roku od 24 sata.
- Dobavljač mora da omogući OGS-u sudjelovanje u rješavanju incidenta koji ima utjecaj na njegov ICT sistem, uključujući omogućavanje pristupa relevantnoj dokumentaciji.

## 7 OTPORNOST I KONTINUITET

- Dobavljač mora da uspostavi plan za kontinuirano poslovanje (angl. Business Continuity Plan – BCP) i plan oporavka od katastrofa (angl. Disaster Recovery Plan – DRP), koji uključuju periodično testiranje.
- Planove je potrebno testirati jednom godišnje, a rezultate na zahtjev podijeliti sa OGS-om.

## 8 UPRAVLJANJE PODIZVOĐAČIMA POVEZANIM S UGOVORENOM USLUGOM

- Dobavljač mora dobiti pisanu suglasnost naručioca (OGS), prije nego što uključi podizvođače ili treća lica.
- Dobavljač mora da osigura da svi podizvođači ispunjavaju iste zahtjeve kao i on sam.

## 9 REVIZIJA PROCJENA RIZIKA

- Dobavljač mora provoditi redovite procjene rizika povezanih s njegovim uslugama i uključiti naručioca (OGS) u procjenu gdje je to primjereno.
- Naručioc (OGS) o dobavljaču priprema vlastitu procjenu rizika, što može da uključuje slanje sigurnosnih upitnika dobavljaču i provođenje neovisnih pregleda sigurnosnih mjera.
- Dobavljač mora da, na zahtjev naručioca, dostavi izvještaje o svojim revizijama i testiranjima, dati odgovore na sigurnosne upitnike i razumno surađivati u provođenju neovisnih pregleda.
- Naručioc (OGS) ima pravo na redovite revizije i neovisne preglede sigurnosnih mjera dobavljača.
- Dobavljač mora na zahtjev OGS-a pružiti dokaze o sukladnosti, kao što su certifikati, izvještaji ili rezultati u svezi sa sigurnosnim testovima.

## 10 OBRAZOVANJE I PODIZANJE SVIJESTI

- Dobavljač mora redovito obučavati svoje zaposlenike koji rade za naručioca (OGS) o dobrim praksama informacijske sigurnosti i drugim sadržajima, ako to zahtijeva naručioc (OGS).

## 11 PREKID SURADNJE

- Nakon prekida ugovora dobavljač mora da osigura sigurno isključenje usluga iz ICT sistema OGS-a, uključujući ukidanje pristupa i sigurno brisanje svih podataka OGS-a.
- Nakon prestanka ugovora dobavljač mora da dostavi izjavu ili drugi dokaz o brisanju podataka.

## 12 AŽURIRANJA I PROMJENE

- OGS zadržava pravo na ažuriranje ovog dokumenta, čime se osigurava odgovor na promjene u rizicima, tehnologiji ili propisima. Dobavljač će biti obaviješten o ažuriranjima i moratiće u razumnom roku osigurati usklađenost.

## 13 POJMOVI I KRATICE

| Br. | Pojam/kratica | Opis |
|---|---|---|
| 3 | **OGS** | Osiguravajuća grupa Sava |
| 4 | **IKT** | Informacijsko-komunikacijska tehnologija – tehnologija koja omogućuje prikupljanje, obradu i razmjenu podataka |
| 5 | **MFA** | Multi-Factor Authentication – višerazinska provjera autentičnosti za povećanje sigurnosti pristupa |
| 7 | **AES-256** | Advanced Encryption Standard (256-bit) – kriptografski algoritam šifriranja za zaštitu podataka koji miruju |
| 8 | **TLS 1.2** | Transport Layer Security 1.2 – kriptografski protokol za sigurnu komunikaciju u mrežama |