

**tablica sadržaja**

- § 1** Opseg i svrha dokumenta
- § 2** Kompetencije - odgovornost
- § 3** Definicije
- § 4** Ciljevi i načela obrade osobnih podataka
- § 5** Obveze osoba koje imaju pristup osobnim podacima
- § 6** Provedba prava osoba čiji se podaci obrađuju
- § 7** Registar
- § 8** Dijeljenje podataka
- § 9** Povjeravanje podataka
- § 10** Upravljanje pristupom osobnim podacima u WAGAS-u
- § 11** Mjesta obrade osobnih podataka
- § 12** Obrada podataka u IT sustavu
- § 13** Obrada osobnih podataka izvan IT sustava
- § 14** Suočavanje s povredama zaštite osobnih podataka
- § 15** Revizije
- § 16** Kontrola PUODO
- § 17** Završne odredbe
- § 18** Povezani dokumenti

## § 1 Opseg i svrha dokumenta

1. Sigurnosna politika i zaštita osobnih podataka WAGAS S.A. sa sjedištem u Varšavi ("WAGAS"), u daljnjem tekstu "Politika", definira sigurnosna pravila s obzirom na osobne podatke čiji je administrator WAGAS, u skladu s Uredbom Europskog parlamenta i Vijeća (EU) 2016/679 od 27. travnja 2016. o zaštiti fizičkih osoba u pogledu obrade osobnih podataka i slobodnom kretanju takvih podataka i ukidanju Direktive 95/46/WE (Opća Uredba o zaštiti podataka - u daljnjem tekstu "RODO").
2. Politika se primjenjuje na obradu osobnih podataka od strane WAGAS-a čiji su administratori drugi subjekti, osim ako odredbe sporazuma sklopljenih s tim subjektima ne predviđaju drugačije.
3. Politika se primjenjuje na sve procese vezane uz obradu osobnih podataka, kako je osmišljena i provedena od 25. svibnja 2018 godine, kao i provedena prije i na snazi nakon 25. svibnja 2018.
4. Cilj politike je osigurati pravilno izvršavanje obveza koje je WAGAS-u nametnuto odredbama RODO.

## § 2 Kompetencije - odgovornost

1. Upravni odbor WAGAS-a odgovoran je za razvoj, odobravanje i provedbu Politike.
2. Provedbu zadaća vezanih uz zaštitu osobnih podataka u WAGAS-u nadzire Upravni odbor.
3. U slučaju imenovanja službenika za zaštitu podataka, Upravni odbor WAGAS-a će povjeriti obavljanje određenih aktivnosti službeniku za zaštitu podataka. Do imenovanja službenika za zaštitu podataka sve funkcije i dužnosti obavlja Upravni odbor WAGAS-a i osobe koje ovlasti Uprava.
4. Svi zaposlenici i suradnici odgovorni su za primjenu ove Politike koja u obavljanju svojih službenih dužnosti sudjeluje u obradi osobnih podataka.

## § 3 Definicije

1. **Administrator** - WAGAS s obzirom na osobne podatke, za koje postavlja ciljeve i metode njihove obrade.
2. **Informacijska sigurnost** - održavanje povjerljivosti, integriteta, pristupačnosti, usklađenosti informacija.
3. **Osobni podaci (podaci)** - sve informacije o fizičkoj osobi koja je identificirana ili koja se može identificirati ("subjekt podataka"); fizička osoba koja se može identificirati je osoba koja se može izravno ili neizravno identificirati, posebno na temelju identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, internetski identifikator ili jedan ili više specifičnih čimbenika koji određuju fizički, fiziološki, genetski, psihološki, ekonomski, kulturni ili društveni identitet fizičke osobe.
4. **Pristup osobnim podacima - omogućavanje pristupa ili izravno izvršenje operacija nad osobnim podacima.**
5. **Incident** - situacija koja uzrokuje gubitak povjerljivosti, integriteta ili dostupnosti obrađenih osobnih podataka.
6. **Klijent** - tražitelj zaštite osiguranja, osiguratelj ili osiguranik.
7. **Kršenje zaštite osobnih podataka (kršenje)** - kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili neovlaštenog pristupa osobnim podacima koji se prenose, pohranjuju ili na drugi način obrađuju. Za potrebe ove Politike, obrada podataka je također nezakonita.
8. **Mediji za informacije / mediji** - sve vrste medija koji se koriste za snimanje informacija u digitalnom obliku, osobito tvrdih diskova, flash memorija, CD / DVD / Blu-ray diskova, magneto- optičkih diskova, DLD / DDS SSD-ova, memorijskih kartica , pametne kartice itd., koje su u vlasništvu WAGAS-a, ili su u vlasništvu drugih fizičkih osoba, pravnih osoba ili organizacijskih jedinica bez pravne osobnosti, ali se koriste za obradu osobnih podataka u WAGAS-u.
9. **Primatelj osobnih podataka (primatelj)** - fizička ili pravna osoba, javno tijelo ili drugi subjekt kojem se otkrivaju osobni podaci. Javna tijela koja mogu primati osobne podatke kao dio posebnog postupka u skladu s pravom Unije ili pravom države članice ne smatraju se primateljima.
10. **Osobe koje obrađuju osobne podatke** - osobe koje obavljaju bilo kakve operacije na Osobnim podacima ili samo imaju pristup Osobnim podacima.
11. **Treća zemlja** - zemlja koja ne pripada Europskom gospodarskom prostoru.
12. **PUODO** - predsjednik Ureda za zaštitu osobnih podataka - nadzorno tijelo nadležno za pitanja u vezi zaštite osobnih podataka.
13. **Zaposlenik / suradnik** - fizička osoba zaposlena u WAGAS-u na temelju ugovora o radu, kao i na temelju građanskopravnog ugovora, posebice ugovora o mandatu ili određenog ugovora o radu, uključujući pripravnike i vježbenike.
14. **Povjeravanje obrade osobnih podataka (povjeravanje)** - prijenos skupa podataka, njegovog fragmenta, pojedinačnih osobnih podataka ili odobravanje pristupa osobnim podacima prema sporazumu koji je WAGAS sklopio s drugim subjektom sukladno čl. 28 RODO, za obradu od strane ovog subjekta u ime WAGAS-a; također uključuje daljnju obradu podataka koje obrađuje WAGAS u ime drugih subjekata.
15. **Privatnost prema zadanim postavkama (defaultna zaštita podataka)** - osiguravanjem, kroz odgovarajuće tehničke i organizacijske mjere, da se samo Osobni podaci koji su potrebni za postizanje svake specifične svrhe obrade obrađuje po defaultu (to se odnosi na količinu prikupljenih osobnih podataka, opseg njihove obrade, skladištenja i dostupnosti). Ove mjere trebaju osigurati da se osobni podaci ne dijele bez intervencije (volje) pojedinca s neodređenim brojem fizičkih osoba.
16. **Privacy by design (zaštita podataka u fazi projektiranja)** – provedba u fazi projektiranja i obrade odgovarajućih tehničkih i organizacijskih mjera za učinkovitu provedbu načela zaštite podataka, posebno potrebne sigurnosti procesa obrade podataka i zaštite prava osoba, kojih se podaci odnose.
17. **Obrada podataka (obrada)** - operacija ili skup operacija izvedenih na osobnim podacima ili skupovima osobnih podataka na automatiziran ili neautomatiziran način, kao što su prikupljanje, snimanje, organiziranje, pohranjivanje, prilagođavanje ili mijenjanje, preuzimanje, pregledavanje, korištenje, otkrivanje, distribuiranje ili na drugi način dijeljenje, podudaranje ili povezivanje, ograničavanje, brisanje ili uništavanje.
18. **Registar** - Registar aktivnosti obrade podataka iz čl. 30 RODO.
19. **RODO** - Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnom kretanjem takvih podataka i stavljanju izvan snage Direktive 95/46/WE (opći propis o zaštiti podataka).
20. **IT sustav** - skupina tehničkih sredstava i softvera koji surađuju jedni s drugima (infrastruktura i aplikacije) čine cjelovitu i logičku cjelinu odvojenu zbog pružene funkcionalnosti, pod pretpostavkom da je njegova glavna svrha obraditi informacije (uključujući osobne podatke).
21. **Posebne kategorije osobnih podataka** - podaci koji otkrivaju rasno ili etničko podrijetlo, političke stavove, vjerska ili ideološka uvjerenja, članstvo u sindikatima, genetske podatke, biometriju, podatke o zdravlju, seksualnosti ili seksualnoj orijentaciji.
22. **Pružanje podataka** – predaja ovlaštenom primatelju osobnih podataka odabranom prema posebnim kriterijima, na temelju pozitivno ocijenjene prijave ili sporazuma, u papirnatom obliku, na drugom informacijskom mediju ili dopuštanjem pristupa odabranim podacima u IT sustavu, za njihovu zasebnu obradu od strane Primatelja, Administratora ili procesora.

23. **Mobilni uređaj** - prijenosni elektronički uređaj koji omogućuje obradu informacija bez održavanja žičane veze s mrežom, posebice mobilni telefon, pametni telefon, dlančnik, tablet, MDA (Mobile Digital Assistant), čija je tipična upotreba primanje i slanje elektroničke pošte i pregledavanje Web stranice koje koriste mobilne aplikacije, isključujući prijenosna računala i elektronske nosače informacija.
24. **Uklanjanje osobnih podataka** - uništavanje osobnih podataka ili njihova izmjena koja neće omogućiti utvrđivanje identiteta nositelja podataka (anonimizacija). Uklanjanje osobnih podataka je trajni i nepovratni proces.

## § 4 Ciljevi i načela obrade osobnih podataka

1. WAGAS obrađuje Podatke u svrhe vezane uz predmet svojih poslovnih aktivnosti, osobito osobne podatke zaposlenika i suradnika, kandidata za posao i sudionika natjecanja koje organizira WAGAS, kao i za obavljanje dužnosti koje proizlaze iz opće primjenjivih zakona i podataka koje povjeravaju druge subjekti koji su njihovi upravitelji, posebice podaci o klijentima koje povjeri osiguravatelji (sindikati), a WAGAS je zastupnik koji djeluje na temelju ugovora sklopljenih s tim osiguravateljima.
2. Načela navedena u ovoj Politici primjenjuju se na sve zaposlenike i suradnike WAGAS S.A. ako je za provedbu svojih zadaća potrebno obraditi osobne podatke, čiji je administrator WAGAS ili povjeren WAGAS-u na temelju sporazuma sklopljenog s drugim subjektom koji je njihov administrator.
3. Politika se odnosi na sve Podatke obrađene u WAGAS-u putem IT sustava, u papirnatom obliku, na drugim informacijskim medijima i usmeno.
4. Svi podaci obrađeni za potrebe WAGAS-a pripadaju važnim poslovnim sredstvima i stoga se njihovo otkrivanje izvan WAGAS-a može dogoditi samo u vezi s obavljanjem službenih zadataka za WAGAS.
5. WAGAS obrađuje osobne podatke u skladu sa sljedećim načelima koja proizlaze iz opće primjenjivih zakona i internih dokumenata WAGAS-a (uključujući ovu Politiku):
  - a. poštivanje zakona, pravičnost i transparentnost (Obrada podataka mora imati pravnu osnovu, poštivanje interesa i prava osoba čiji se podaci obrađuju, biti transparentna prema osobama na koje se odnose podaci koji se obrađuju);
  - b. ograničenje svrhe (svrha obrade podataka mora biti specifična, eksplicitna i pravno opravdana, a podaci se ne smiju obrađivati protivno ovoj svrsi);
  - c. minimiziranje podataka (podaci trebaju biti prikladni i potrebni za svrhu obrade);
  - d. ispravnost podataka (podaci moraju biti istiniti, potpuni i aktualni);
  - e. Ograničenja pohrane (Podaci moraju biti obrađeni samo u razdoblju u kojem je potrebno za postizanje legitimne svrhe Obrade);
  - f. integritet, povjerljivost i dostupnost (podaci moraju biti obrađeni na način koji osigurava njihovu sigurnost, uključujući zaštitu od neovlaštene ili nezakonite obrade, slučajnog gubitka, uništenja ili oštećenja);
  - g. odgovornost (tijekom obrade podataka potrebno je pridržavati se načela navedenih u točkama 1) - 6) i sposobnost dokazivanja njihove usklađenosti).

## § 5 Obveze osoba koje imaju pristup osobnim podacima

1. Svi zaposlenici i suradnici koji imaju u obavljanju svojih službenih dužnosti pristup osobnim podacima obrađenim u WAGAS-u, dužni su:
  - a. da se upoznaju i strogo se pridržavaju zakonskih propisa i internih postupaka koji reguliraju načela zaštite osobnih podataka usvojena u WAGAS-u;
  - b. sudjelovati najmanje jednom godišnje na obuci koju organizira WAGAS;
  - c. uključiti se u sve planirane i provedene procese, tehnička i organizacijska rješenja ili alatevezane uz obradu podataka:
    - I. pravila Privacy by design (Zaštita podataka u fazi projektiranja) i Privacy by default (zadana zaštita podataka), i također
    - II. (rezultate procjene PIA-a provedene u skladu s Načelima za provođenje procjene učinka zaštite podataka (procjena PIA) u WAGAS-u,
  - d. poštivanje načela zaštite osobnih podataka
  - e. neodređeno očuvanje povjerljivosti obrađenih osobnih podataka i načina njihove zaštite,
  - f. podnijeti izvješće Odboru i razjasniti svaku sumnju u vezi s ispravnnošću obrade osobnih podataka,
  - g. suradnju s Upravom u slučaju revizija koje se provode na WAGAS-u (interno i eksterno), kao i kontrolu koju provodi PUODO;
  - h. na zahtjev Upravnog odbora odmah pripremiti i poslati podatke o obradi osobnih podataka (u skladu s opsegom zahtjeva);
  - i. vođenje i praćenje evidencije osoba ovlaštenih za obradu osobnih podataka u okviru zadataka koji se obavljaju u organiziranoj jedinici koju nadziru, pod uvjetom da osobne podatke obrađuju zaposlenici/suradnici ove jedinice samo u papirnatom obliku ili na vanjskim medijima, u skladu s modelom iz Priloga Politike br. 7,
  - j. nadzirati podređene zaposlenike i suradnike u ispunjavanju dužnosti opisanih u ovoj Politici,
  - k. izvještavanje o svakoj aktivnosti, čiji je element obrada osobnih podataka (osim obrade vizitki za komunikacijske svrhe) u registar.
  - l. cjelovitost, povjerljivost i dostupnost (podaci se moraju obrađivati na način koji osigurava njihovu sigurnost, uključujući zaštitu od neovlaštene ili nezakonite obrade, slučajnog gubitka, uništenja ili oštećenja);
  - m. Odgovornost (obrada podataka zahtijeva poštivanje načela iz točaka 1) - 6) gore i sposobnost.
2. Nadalje, zaposlenici / suradnici primjenjuju **sigurnosne zahtjeve IT sustava usvojene u WAGAS-u**, u skladu s IT sigurnosnom politikom u Wagas S.A., koja predstavlja dodatak ovoj Politici.

## § 6 Provedba prava osoba čije se podaci obrađuju

1. WAGAS provodi prava osoba na koje se podaci odnose:
  - a. pravo na informacije i dobivanje potvrde o obradi podataka od strane administratora i pristup podacima,
  - b. pravo na povlačenje pristanka,
  - c. pravo ispravljanja / dopune podataka,
  - d. pravo na brisanje podataka ("pravo na zaborav"),
  - e. pravo na ograničavanje Obrade,
  - f. pravo na prijenos podataka,
  - g. pravo na prigovor na obradu osobnih podataka,
  - h. pravo da ne bude predmet odluka donesenih u automatiziranoj obradi podataka, uključujući profiliranje.
2. Provedba postupanja sa zahtjevima osoba čije se informacije odnose na njih osigurava Upravni odbor WAGAS-a u skladu s **Uputama za postupanje na zahtjevu subjekata podataka**, što predstavlja privitak ovoj Politici.

## § 7 Registar

1. Upravni odbor vodi Registar. U tu svrhu može imenovati osobu odgovornu za njegovu provedbu.
2. Svi zaposleni i suradnici odgovorni su za ažuriranje informacija u Registru, uključujući prestanak obrade osobnih podataka, a posebno:
  - a. odmah prijavljuju stvaranje novog skupa podataka,
  - b. odmah izvješćuju i ažuriraju informacije o obradi osobnih podataka, uključujući prestanak obrade osobnih podataka.
3. Priprema i podnošenje Upravnom odboru ispravne prijave u Registar ili njegovo ažuriranje u okviru ugovora o povjeravanju ili dijeljenju podataka odgovornost je zaposlenika ili suradnika odgovornog za sklapanje ugovora, u skladu s § 8 i § 9 u nastavku.

## § 8 Dijeljenje podataka

1. Odluku o davanju podataka, uključujući pružanje podataka na zahtjev nadležnih državnih tijela, donosi Upravni odbor WAGAS-a.
2. Osiguranje osobnih podataka, čiji je administrator WAGAS, upisuju se u registar nakon obavijesti osobe odgovorne za provedbu pristupa.
3. Pristup podacima trećoj zemlji moguć je samo pod uvjetima utvrđenim važećim zakonom (članak 44. i dalje RODO).

## § 9 Povjeravanje podataka

1. WAGAS kao administrator može povjeriti drugoj osobi (subjekt za obradu) obradu osobnih podataka u ime WAGAS-a samo na temelju pisanog sporazuma sklopljenog s tim subjektom, međutim to može biti samo subjekt koji jamči pravilnu i sigurnu obradu osobnih podataka.
2. WAGAS kao procesor Podataka može povjeriti podatke drugom subjektu samo u svrhe i prema uvjetima sporazuma između kontrolora podataka i WAGAS-a kao procesora.
3. Ugovor o povjeravanju obrade osobnih podataka, u kojem WAGAS djeluje kao administrator podataka ili kao procesor, mora udovoljavati zahtjevima čl. 28 RODO uz prethodnu suglasnost Odbora.
4. Povjeravanje obrade osobnih podataka, čiji je administrator WAGAS, upisuje se u registar nakon obavijesti osobe odgovorne za sklapanje ugovora.
5. U slučaju pristupa vanjskih subjekata IT sustavu u svrhu provedbe, popravka, pregleda ili održavanja ovog sustava, kada vanjski subjekt pristupa osobnim podacima koji se obrađuju u ovom sustavu, potrebno je sklopiti sporazum o obradi osobnih podataka u skladu s odredbama stavaka 1 - 3 gore.
6. U slučaju pristupa zaposlenika / suradnika vanjskih subjekata sustavu Korporativne Pošte ili Intranetu (u slučaju i kada se provodi), odredbe koje uređuju taj pristup moraju biti uključene u sporazum.
7. U slučaju namjere sklapanja Ugovora o povjeravanju, u kojem WAGAS djeluje kao obrađivač, osoba odgovorna za njegovo sklapanje dužna je to prijaviti Registru.
8. WAGAS kao administrator može povjeriti podatke trećoj državi pod uvjetima koji su u skladu s važećim zakonom, ali odluku o tom pitanju donosi Odbor nakon što ga je dostavila osoba odgovorna za povjeravanje podataka.
9. Povjeravanje Podataka, čiji je administrator WAGAS, trećoj zemlji upisuje se u registar nakon što ga obavijesti osoba odgovorna za sklapanje ugovora.
10. Ako WAGAS, zajedno s drugim subjektima, definira svrhe i metode obrade osobnih podataka (podaci o zajedničkom administriranju), treba sklopiti ugovor koji će regulirati opseg odgovornosti svakog od zajedničkih kontrolora i odnose između kontrolora i subjekata na koje se podaci odnose.
11. Sklapanje ugovora o su-upravljanju Podacima se upisuje u Registar nakon što ga obavijesti osoba odgovorna za njegovo sklapanje.

## § 10 Upravljanje pristupom osobnim podacima u WAGAS-u

1. Podatke mogu obraditi samo osobe koje su za to ovlaštene. Administrator odobrava Obradu podataka svim osobama koje obrađuju osobne podatke u vezi s obavljanjem njihovih dužnosti administratoru, sukladno odredbama iz podstavka 3 ispod.
2. Ovlaštenje za obradu osobnih podataka uključeno je u ugovor o radu, ugovor o upravljanju, ugovor o mandatu, drugi tip sporazuma o suradnji sklopljen izravno između WAGAS-a i zaposlenika / suradnika.
3. Uvjeti i odredbe Pristupa osobnim podacima, čiji je administrator WAGAS, od strane zaposlenika i suradnika subjekta za obradu, mogu biti navedeni u ugovoru za obradu osobnih podataka koje je sklopio WAGAS s procesorom.
4. Zaposlenici / suradnici tvrtke WAGAS ovlašteni za obradu osobnih podataka moraju:
  - a. proći obuku o načelima zaštite osobnih podataka i znakova koji čine element ugovora o radu, izjavu o upoznavanju sa zakonom za područje zaštite osobnih podataka i pravilima o zaštiti osobnih podataka koja se primjenjuju u WAGAS-u,
  - b. podnijeti, kao dio radnog odnosa, obvezu neograničenog čuvanja povjerljivosti obrađenih osobnih podataka i načina njihove zaštite,
  - c. u slučaju promjene opsega zadataka ili radnog mjesta u WAGAS-u, što rezultira nedostatkom potrebe za obradom osobnih podataka ili otkazom ugovora o radu s zaposlenikom, on je dužan vratiti poslodavcu dokumentaciju ili druge medije koji sadrže osobne podatke.
5. Pristup informacijskom sustavu u kojem se obrađuju osobni podaci, osim ispunjavanja zahtjeva iz st. 4 odobravanje pristupa IT sustavu u skladu s Politikom sigurnosti informacijske tehnologije u WAGAS-u, što predstavlja privitak ovoj politici.
6. Evidenciju osoba ovlaštenih za obradu osobnih podataka u IT sustavu vodi osoba koju odredi Upravni odbor, pod nadzorom Upravnog odbora.
7. Pristup osobnim podacima obrađenim izvan ICT sustava provodi se pod nadzorom Upravnog odbora.

## § 11 Mjesta obrade osobnih podataka

1. Prostor za obradu osobnih podataka, tj. Zgrada, soba ili dijelovi prostorija koji čine područje u kojem se obrađuju osobni podaci, zaštićeni su korištenjem mjera fizičke zaštite i usvajanjem odgovarajućih organizacijskih rješenja za sprječavanje neovlaštenog pristupa podacima.
2. Treće osobe koje ulaze u prostorije prihvaćaju se od ovlaštenog recepcijskog osoblja koje osigurava povjerljivost osobnih podataka.
3. Osim toga, osoblje recepcije dužno je pridržavati se povjerljivosti podataka u obavljanju svojih dužnosti na mjestu prijema u području:
  - a. rukovanje dolaznom i odlaznom korespondencijom
  - b. upravljanje telefonskim centrom
  - c. organizaciju poslovnih putovanja (rezervacija, poslovna putovanja)
  - d. prijevod tekstova
  - e. uređivanje pisama i dokumenata
  - f. arhiviranje dokumenata
4. Uz iznimku mjesta posvećenih sastancima s trećim stranama, prisutnost neovlaštenih osoba u mjestima navedenim u st. 1, dopušteno je samo u prisutnosti osobe ovlaštene za obradu osobnih podataka.
5. Mjesta iz st. 1, moraju biti zaštićena tijekom odsutnosti osoba ovlaštenih za obradu osobnih podataka na način koji sprječava neovlašteni fizički pristup njima.
6. Osim mjesta namijenjenih sastancima s trećim osobama, zabranjeno je na mjestima iz st. 1 ovoga članka, snimanje slike ili zvuka, kao i prijenos slika ili zvuka izvan tih mjesta, osim kada se te aktivnosti poduzimaju u okviru mjera fizičke zaštite.
7. Osobe ovlaštene za obradu osobnih podataka dužne su provjeriti da li na mjestima navedenim u st. 1. ovog članka, nema nezaštićenih dokumenata ili materijala koji sadrže osobne podatke (tj. Usklađenost s načelom "čistog stola").
8. Održavanje, popravak i hitna služba uređaja i IT sustava u mjestima navedenim u st. 1, mora se obaviti nakon savjetovanja s Upravnim odborom i u nazočnosti osoba ovlaštenih za obradu osobnih podataka.

## § 12 Obrada podataka u IT sustavu

Obradena zaštita sigurnosti osobnih podataka:

- a. u IT sustavu,
- b. na mobilnim uređajima

- također je regulirano 'Politikom sigurnosti informacijske tehnologije u WAGAS-u', koja je vezana uz ovu Politiku.

## § 13 Obrada osobnih podataka izvan IT sustava

1. Papirni dokumenti koji sadrže osobne podatke zaštićeni su od oštećenja, uništenja ili otkrivanja neovlaštenim osobama.
2. Dokumenti trebaju biti fizički zaštićeni od gubitka i pristupa neovlaštenih osoba. Načelo "čistog stola" znači da svi dokumenti koji sadrže osobne podatke trebaju biti pohranjeni nakon završetka radnog dana na mjestu koje ne jamči pristup neovlaštenim osobama (npr. Uredski namještaj koji se može zaključati).
3. Svaki papirnati dokument koji sadrži osobne podatke, nakon što je potreba za uporabom prestala postojati, bit će uništen na siguran način koji sprječava čitanje sadržaja tih dokumenata. Do trenutka uništenja treba ga čuvati na sigurnom mjestu koje onemogućava pristup neovlaštenih osoba (npr. Uredski namještaj koji se može zaključati).
4. Zabranjeno je kopiranje osobnih podataka sadržanih u papirnim dokumentima bez pristanka neposrednog nadređenog.
5. Princip "čistog printera" znači da ispise i kopije koji sadrže osobne podatke donosi samo zaposlenik koji ih je dužan odmah odnijeti s printera.
6. Dokumenti koji sadrže osobne podatke šalju se u jakoj, neprozirnoj omotnici, kao registrirani paketi s potvrdom o primitku, putem tvrtki koje pružaju poštanske i kurirske usluge.
7. Elektronički nositelji informacija s osobnim podacima trebaju biti zaštićeni od fizičkog oštećenja ili uništenja, što bi onemogućilo čitanje ili vraćanje informacija sadržanih u njima.
8. Elektronički nositelji informacija s osobnim podacima koje koriste korisnici trebaju biti fizički zaštićeni od gubitka i pristupa neovlaštenih osoba.
9. Napuštanjem radnog mjesta, Informacijski mediji trebaju biti osigurani na način koji sprječava pristup neovlaštenim osobama (npr. Spremanje u zaključani uredski namještaj).
10. Zabranjeno je obraditi osobne podatke na osobnim računalima.
11. Zabranjeno je kopiranje osobnih podataka u medije informacija, u druge osim poslovne svrhe. Broj elektroničkih kopija osobnih podataka koji sadrže dokumente treba ograničiti na minimum.
12. Upotreba medija s informacijama tipa pendrive, vanjskog diska itd. Koji omogućavaju snimanje podataka, treba biti ograničena i dopuštena samo u potrebnim slučajevima uz pristanak neposrednog nadređenog. Pristup podacima na ovim medijima treba biti šifriran.

## § 14 Suočavanje s povredama zaštite osobnih podataka

1. Svatko tko je primio obavijest o sumnjivim kršenjima zaštite osobnih podataka obrađenih u informacijskom sustavu i izvan sustava, kao i o kršenju ili pokušajima prevladavanja primijenjenih mjera fizičke zaštite i usvojenog sustava zaštite mjesta na kojem se obrađuju osobni podaci, dužan je odmah nakon primitka takvih informacija, prijaviti kršenja Odboru WAGAS-a.
2. Prijavljene povrede analiziraju se u skladu s odredbama internih procedura i dostavljaju se Odboru.
3. U skladu s važećim zakonom, nakon potvrđivanja kršenja:
  - a. Uprava izvješćuje o kršenju PUODO-a;
  - b. osoba čiji se podaci odnose na povredu, o tome je obaviještena - u skladu s internim postupcima WAGAS-a,

podložno odredbama 'Uputa u slučaju kršenja zaštite osobnih podataka', koji predstavlja prilog ovoj Politici.

## § 15 Revizije

1. Provjera usklađenosti obrade osobnih podataka u WAGAS-u s odredbama o zaštiti osobnih podataka obuhvaća sve organizacijske jedinice WAGAS-a u kojima se obrađuju osobni podaci, kao i procesore kojim je WAGAS povjerio osobne podatke za obradu.
2. Revizija usklađenosti obrade osobnih podataka s odredbama o zaštiti osobnih podataka odvija se na način:
  - a. Planirana revizija - u skladu s planom revizije odobrenom od strane Upravnog odbora WAGAS-a,
  - b. Ad hoc revizija - provodi se u slučajevima zaštite osobnih podataka ili opravdane sumnje u takve povrede.
3. Planiranu reviziju provode zaposlenici koje je Upravni odbor naveo, jednom kalendarskom godinom, počevši od 2019. godine. U opravdanim slučajevima Upravni odbor može izvršiti reviziju trećoj strani.
4. Ad hoc reviziju provode zaposlenici / suradnici koje je Upravni odbor naveo u vremenu koje svaki put odredi Upravni odbor, ovisno o potrebi i razlogu revizije.
5. Osobe koje provode Ad hoc reviziju ili sudjeluju u njoj kao stručnjaci, dužne su Upravnom odboru dostaviti izvješće o reviziji odmah nakon njenog završetka, prema obrascu koji je priložen ovoj Politici.

## § 16 Kontrola PUODO

1. Prema pravilima predviđenim važećim zakonskim odredbama, PUODO može provoditi provjere usklađenosti obrade podataka s odredbama o zaštiti osobnih podataka u WAGAS-u.
2. Svatko tko je dobio informacije o kontroli PUODO-a, dužan je odmah obavijestiti Upravni odbor WAGAS-a ili neposredno nadređenog. Zaposlenik WAGAS-a ovlašten od strane Uprave, odgovoran za područje pod kontrolom PUODO-a, sudjeluje u kontrolnim aktivnostima koje PUODO poduzima osobno ili putem određenih zaposlenika.
3. Ovlašteno osoblje obavještava Upravni odbor o rezultatima inspekcije koju je proveo PUODO.

## § 17 Završne odredbe

1. U pitanjima koja nisu obuhvaćena odredbama Politike, primjenjuju se općenito primjenjivi zakoni.
2. Ako se zaposlenici WAGAS-a ne pridržavaju odredbi Politike, to će rezultirati poduzimanjem disciplinskih mjera koje proizlaze iz Pravilnika o radu i odredbi Zakona o radu.

## § 18 Povezani dokumenti

Sastavni dio ove politike su:

1. Načela provođenja procjene utjecaja na zaštitu podataka (procjena PIA-a);
2. Upute o postupanju u slučaju kršenja zaštite osobnih podataka;
3. Upute za postupanje po zahtjevima subjekata podataka;
4. Uputa za obavljanje obveze informiranja;
5. Politika sigurnosti IT-a u WAGAS-u;
6. Model izvješća o reviziji usklađenosti obrade osobnih podataka u WAGAS-u s odredbama o zaštiti osobnih podataka.
7. Zapis osoba ovlaštenih za obradu osobnih podataka - model