



ČAZMATRANS - NOVA d.o.o.

# POLITIKA ADMINISTRIRANJA

ORGANIZACIJSKE MJERE ZAŠTITE OSOBNIH PODATAKA



ČAZMATRANS - NOVA društvo s ograničenom odgovornošću za prijevoze i usluge iz Čazme, M.Novačića 10, OIB:04767584912, skupno zastupano po članovima uprave Damiru Pavloviću, Robertu Šimleši i Berislavu Saraji (u daljnjem tekstu: Poslodavac/ Voditelj obrade) u skladu s člankom 5. i člankom 32. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu: Opća uredba o zaštiti podataka)

donosi sljedeću

## **POLITIKU ADMINISTRIRANJA**

### **1. ČIST STOL**

#### **1.1 Organizacija radne površine:**

Pravilna organizacija radne površine ključna je kako bi se osigurala sigurnost i privatnost osobnih podataka. Zaposlenici su dužni redovito provoditi organizaciju svojih radnih prostora kako bi se smanjila mogućnost nenamjernog otkrivanja osjetljivih informacija. To uključuje osiguravanje da svi dokumenti i materijali koji sadrže osobne podatke budu pravilno pohranjeni u ormarićima ili pretincima.

#### **1.2 Pohrana dokumenata i nosača podataka:**

Osobni dokumenti, papirnate kopije i drugi nosači podataka moraju se sigurno pohranjivati kako bi se izbjeglo neovlašteno otkrivanje ili zloupotreba informacija. Kada takvi dokumenti više nisu potrebni, zaposlenici su dužni koristiti sigurne metode uništenja kako bi se osigurala potpuna zaštita privatnih informacija. To uključuje korištenje usluga profesionalnih uništavača dokumenata ili drugih sigurnih metoda uništenja.

#### **1.3 Zaštita od neovlaštenog pogleda:**

Zaposlenici bi trebali osigurati da osjetljivi dokumenti nisu vidljivi drugima, bilo da su na radnoj površini ili u slobodnom pristupu. Preporučuje se korištenje zaštitnih sredstava poput zaslona za privatnost ili fizičkih pregrada kako bi se spriječilo nenamjerno ili namjerno izlaganje osjetljivih informacija.



#### **1.4 Zaključavanje radne površine:**

Kada zaposlenici privremeno napuste svoj radni prostor, posebno tijekom pauza ili nakon radnog dana, trebaju zaključati svoje računalne sučelje. Ovo je ključno kako bi se spriječio neovlašteni pristup informacijama koje su trenutno dostupne na radnoj površini.

#### **1.5 Pravilno zbrinjavanje dokumenata:**

Osim pohrane, pravilno zbrinjavanje dokumenata također igra ključnu ulogu u zaštiti osobnih podataka. Kada dokumenti više nisu potrebni, zaposlenici bi trebali koristiti sigurne spremnike za papir ili spremnike za reciklažu s osiguranim uništavanjem kako bi se osiguralo da osjetljivi podaci ne dospiju u krive ruke.

Ovaj segment politike naglašava važnost čistog stola kao osnovne sigurnosne mjere u upravljanju osobnim podacima. Pravilna organizacija radne površine, pohrana dokumenata, zaštita od neovlaštenog pogleda, zaključavanje radne površine i pravilno zbrinjavanje dokumenata čine neophodne korake kako bi se zaštitila povjerljivost i integritet osobnih podataka.

### **2. ČIST EKRAN**

#### **2.1 Zaključavanje računalnog sustava:**

Zaštita osobnih podataka na računalu jednako je važna kao i zaštita fizičkih dokumenata. Kada zaposlenici privremeno napuste svoje radno mjesto ili računalni sustav, dužni su aktivirati zaslon za zaključavanje ili se odjaviti kako bi se spriječio neovlašteni pristup podacima. Ova praksa osigurava da nitko drugi ne može pristupiti informacijama koje su trenutno otvorene na ekranu.

#### **2.2 Isključivanje monitora:**

Kada zaposlenici napuste radno mjesto na dulje vrijeme, preporučuje se isključivanje monitora kako bi se smanjila mogućnost neovlaštenog pregledavanja informacija sa strane. Ovo je posebno važno u prostorima s većim protokom ljudi ili otvorenom uredu gdje su ekrani vidljivi drugima.

#### **2.3 Čišćenje privatnih podataka s ekrana:**

Nakon svakog korištenja računalnog sustava, zaposlenici bi trebali osigurati da su svi privatni podaci obrisani s ekrana. Ovo uključuje zatvaranje svih prozora, izlazak iz aplikacija koje



sadrže osobne podatke i brisanje privremenih datoteka. Osim toga, trebaju obratiti posebnu pozornost na unos osjetljivih informacija poput lozinki ili financijskih podataka kako bi se spriječilo neovlašteno prisjećanje.

## **2.4 Upotreba zaslona:**

Kako bi se spriječilo nenamjerno otkrivanje podataka s ekrana, preporučuje se korištenje zaslona za privatnost. Ovi zasloni smanjuju kut gledanja ekrana tako da je sadržaj jasan samo osobama koje sjede ispred računala. Ovo je posebno korisno u situacijama gdje se radi u javnim prostorima ili na mjestima gdje je prisutnost drugih ljudi česta.

## **2.5 Osvježavanje ekrana:**

Zaposlenici bi trebali osigurati da se ekrani redovito osvježavaju kako bi se spriječilo zadržavanje osjetljivih podataka na ekranu nakon što su aplikacije zatvorene. Ova praksa smanjuje rizik od slučajnog otkrivanja informacija drugim osobama koje bi mogle koristiti računalni sustav nakon zaposlenika.

Uključujući ove smjernice u našu politiku administriranja čistog ekrana, mi osiguravamo da se privatni podaci na ekranu obrađuju s visokim standardima sigurnosti. Često zaključavanje, isključivanje ekrana, čišćenje podataka i upotreba zaštitnih zaslona osiguravaju da se informacije ne otkrivaju neovlaštenim osobama, čime se čuva povjerljivost i zaštita osobnih podataka u skladu sa zahtjevima Opće uredbe o zaštiti podataka (GDPR).

# **3. PRAĆENJE AKTIVNOSTI I AUDIT**

## **3.1 Praćenje aktivnosti:**

Kako bismo osigurali dosljednu primjenu politike čistog ekrana, voditelj obrade će redovito provoditi praćenje aktivnosti na računalnim sustavima. Ovo uključuje praćenje vremena kada su zaposlenici aktivni na računalima te kako upravljaju svojim ekranima i privatnim podacima. Praćenje aktivnosti pomaže u identifikaciji potencijalnih propusta ili nepravilnosti u primjeni ove politike te omogućava brzu intervenciju kako bi se očuvala sigurnost podataka.

## **3.2 Redoviti audit:**

Voditelj obrade će provoditi redovite audite kako bi provjerio usklađenost sa standardima i smjernicama o čistom ekranu. Ti auditni postupci uključuju detaljno pregledavanje radnih mjesta i računalnih sustava kako bi se osiguralo da zaposlenici dosljedno primjenjuju



postavljene smjernice. Auditi također pomažu u identifikaciji potreba za dodatnom obukom ili informiranjem zaposlenika o pravilnom postupanju s osobnim podacima.

### **3.3 Praćenje i izvještavanje:**

Rezultati praćenja aktivnosti i audita bit će sustavno praćeni i dokumentirani. U slučaju otkrivanja kršenja ili nepravilnosti u primjeni politike čistog ekrana, voditelj obrade će poduzeti odgovarajuće korake kako bi se rizici minimizirali. O svakom identificiranom slučaju kršenja ili nepravilnosti bit će izvještavano nadležnoj strukturi unutar organizacije.

### **3.4 Kontinuirano usavršavanje:**

Na temelju rezultata praćenja i audita, voditelj obrade će kontinuirano analizirati učinkovitost politike čistog ekrana i provoditi korektivne mjere tamo gdje je to potrebno. Ovo uključuje prilagodbu smjernica, poboljšanje obuka zaposlenika te primjenu najboljih praksi koje se tiču sigurnog upravljanja informacijskim sustavima i zaštitom osobnih podataka.

Uključujući strogo praćenje aktivnosti, redovite audite te kontinuirano usavršavanje, voditelj obrade postavlja temelj za dosljedno poštivanje politike čistog ekrana u skladu s zahtjevima Opće uredbe o zaštiti podataka (GDPR). Ovaj pristup osigurava da se sigurnost podataka održava na najvišoj razini, čime se štite povjerljivost i integritet osobnih podataka na našim računalnim sustavima.

## **4. EDUKACIJA I OSVJEŽAVANJE**

### **4.1 Obuka o politici čistog ekrana:**

Kako bismo osigurali dosljedno razumijevanje i primjenu politike čistog ekrana, svi zaposlenici će biti podvrgnuti obuci pri ulasku u organizaciju te će redovito sudjelovati u osvježavanju znanja. Obuka će pokriti osnovne principe zaštite podataka, rizike povezane s nepoštivanjem politike čistog ekrana, tehnike za osiguranje privatnosti tijekom rada na računalima te postupke za zaštitu podataka u svakodnevnim situacijama.

### **4.2 Tehničke smjernice i praktični savjeti:**

Uz obuku, zaposlenici će biti opskrbljeni tehničkim smjernicama i praktičnim savjetima kako pravilno primijeniti politiku čistog ekrana. Ovo uključuje informacije o postavljanju automatskih zaključavanja zaslona, upotrebi "privatnog načina" preglednika, te načinima minimaliziranja prikaza osjetljivih informacija na zaslonu. Tehničke smjernice omogućuju zaposlenicima konkretno razumijevanje kako primijeniti smjernice politike u svakodnevnom radu.



#### 4.3 Osvježavanje znanja:

Svaki zaposlenik će redovito sudjelovati u programima osvježavanja znanja kako bi se uvjerali da su up-to-date s najnovijim standardima i smjernicama vezanim uz politiku čistog ekrana. Ovi programi osvježavanja mogu uključivati online tečajeve, seminare ili radionice o informacijskoj sigurnosti i upravljanju podacima. Redovitim osvježavanjem znanja, zaposlenici će biti u mogućnosti adekvatno reagirati na nove izazove i prijetnje.

#### 4.4 Praćenje i evaluacija:

Uz obuku i osvježavanje, voditelj obrade će provoditi praćenje i evaluaciju kako bi utvrdio učinkovitost obrazovnih programa. Na temelju povratnih informacija i rezultata praćenja, prilagodit će se obuka i osvježavanje kako bi bolje odgovarali potrebama zaposlenika i organizacije.

Pristup edukaciji i osvježavanju ključan je za uspješnu primjenu politike čistog ekrana. Ulažući u znanje zaposlenika, voditelj obrade doprinosi smanjenju rizika od kršenja sigurnosti podataka te osigurava da svi zaposlenici budu osviješteni o važnosti zaštite podataka i privatnosti tijekom rada s računalima

Ova sveobuhvatna politika administriranja čistog stola i čistog ekrana promovira najviše standarde zaštite podataka u skladu s GDPR-om. Njezin cilj je postići maksimalnu zaštitu osobnih podataka i osigurati integritet i povjerljivost tijekom svih administrativnih aktivnosti. Implementacijom ovih smjernica, osiguravamo dosljedno poštivanje zakonskih zahtjeva i zaštitu privatnosti svih osobnih podataka koje rukujemo.

Ova politika redovito se pregledava, nadopunjuje i usklađuje s primjenom novih mjera i rezultatima internih revizija, pri čemu se provodi najmanje jednom godišnje.

Politika stupa na snagu danom donošenja.

Datum donošenja: 19. prosinca 2024

za ČAZMATRANS - NOVA d.o.o.

\_\_\_\_\_  
Damir Pavlović, član uprave

\_\_\_\_\_  
Robert Šimleša, član uprave

\_\_\_\_\_  
Berislav Saraja, član uprave

## SLUŽBENIK ZA ZAŠTITU PODATAKA

|                                |                                                                                                                                                  |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Datum pripreme prijedloga:     | prosinac 2024. godine                                                                                                                            |
| Službenik za zaštitu podataka: | Ines Krečak Data Protection Professional, CIPP/E<br>E-mail: <a href="mailto:feralis@feralis.hr">feralis@feralis.hr</a><br>Mob.: +385(0)995639746 |



**EUROPEAN FEDERATION  
OF DATA PROTECTION OFFICERS**

