TZO Ston – Mjere sigurnosti pri obradi osobnih podataka

Izvršitelj obrade poduzima sljedeće mjere sigurnosti kako bi jamčio primjerenu razinu zaštite osobnih podataka i usklađenosti s važećim propisima o zaštiti osobnih podataka:

- prostorije u kojima se nalaze oprema i sustavi koji se koriste za obradu osobnih podataka kao i dokumentacija koja sadrži osobne podatke moraju na odgovarajući način biti zaštićeni kako bi bili dostupni samo osobama ovlaštenima za obradu kao i administratoru sustava,
- pristup prostorijama, opremi, sustavima i dokumentaciji koja sadrži osobne podatke mora biti odmah nakon prestanka ugovornog odnosa ili prestanka ovlaštenja za obradu osobnih podataka onemogućen osobama koje su bile ovlaštene za obradu,
- pristup sustavnom i aplikacijskom softveru mora biti zaštićen sustavom zaporki za autorizaciju i identifikaciju korisnika koji omogućava jednoznačno određivanje aktivnosti svakog korisnika (korisničko ime i zaporka, odnosno pin za mobilne telefone);
- uporaba korisničkih imena i zaporki mora biti na razini pojedinačne osobe, ne smije biti omogućena upotreba jedinstvenih korisničkih imena i zaporki za više osoba;
- prilikom korištenja zaporki upotrebljavati snažne zaporke, izbjegavati riječi iz rječnika, slijed brojki ili slova, imena, nadimke itd.;
- sva računala, uključujući prijenosne i mobilne uređaje, potrebno je redovito ažurirati pomoću sigurnosnih programskih ispravaka koje izdaje proizvođač operativnog i aplikacijskog sustava;
- koristiti samo ovlašteni i uredno licencirani softver na svim radnim stanicama, prijenosnim i mobilnim uređajima na kojima se obrađuju osobni podaci;
- aktivirati antivirusni sustav na svim radnim stanicama, prijenosnim i mobilnim uređajima na kojina se obrađuju osobni podaci;
- antivirusni sustav mora trajno raditi i potrebno ga je konstantno ažurirati s najnovijim nadogradnjama prema preporuci proizvođača;
- kod spremanja podataka na vanjske medije (usb, cd, vanjski disk itd.) potrebno ih je dodatno zaštititi zaporkom pomoću nekog od alata za kriptiranje (npr. 7zip, bitlocker itd.) kako ne bi bili čitljivi u slučaju neovlaštenog pristupa uslijed gubitka ili krađe vanjskog medija;
- spriječiti svako neovlašteno iznošenje podataka izvan službenih prostorija, kao i svako neovlašteno dijeljenje bilo putem fizičkih medija ili slanjem putem mreže;
- ako je za potrebe odvijanja poslovnog procesa dokumentaciju i opremu koja sadrži osobne podatke potrebno iznositi izvan službenih prostorija, istu se ne smije ostavljati bez nadzora;
- zabranjena je izrada nepotrebnih kopija dokumenata/datoteka koji sadrže osobne podatke;
- prilikom otpisa i ekološkog zbrinjavanja (uključujući i prodaju, zamjenu, darovanje i dr.) računala i računalne opreme potrebno je prethodno osigurati da su svi podaci trajno i nepovratno izbrisani korištenjem nekog od alata za sigurno brisanje ili fizičkim uništenjem;
- vodit će evidenciju pristupa podacima;
- osigurati primjenu politike čistog stola/čistog ekrana

Politika čistog stola / čistog ekrana

- za vrijeme odsutnosti s radnog mjesta korisnik računala mora zaključati računalo („lock“) ili se mora odjaviti s računala („log off)
- na kraju radnog dana korisnik mora isključiti računalo,
- svi tiskani dokumenti koji sadrže osobne podatke moraju biti uklonjeni s radnog stola i zaključani u ormar/ladicu kada se ne koriste ili nisu pod nadzorom (za vrijeme odsutnosti s radnog mjesta i na kraju radnog dana); to uključuje i vanjske medije (npr. cd, dvd, vanjski disk, usb) kao i prijenosna računala, tablete i ostale uređaje na kojima su pohranjeni osobni podaci;
- ključevi ormarića/ladice u kojima se nalaze tiskani dokumenti i uređaji koji sadrže osobne podatke ne smiju biti ostavljeni bez nadzora na vidljivim i lako dostupnim mjestima (npr. na radnom stolu);
- korisnička imena i/ili zaporke ne smiju biti ostavljeni na vidljivim i lako dostupnim mjestima (ispod tipkovnice, na monitoru, u nezaključanim ladicama i dr.);
- tiskani dokumenti koji sadrže osobne podatke moraju odmah biti uklonjeni s printera ili telefaksa;
- tiskani dokumenti koji sadrže osobne podatke ne smiju biti odloženi u javne (plave) spremnike za papir, u plastične ili kartonske kutije za prikupljanje papira i dr. ako prethodno nisu uništeni u uništavaču papira ili na drugi odgovarajući način.