PRAVILNIK O ZAŠTITI OSOBNIH PODATAKA

I. OPĆE ODREDBE

Članak 1.

Ovim Pravilnikom društvo LAUS INTERNATIONAL d.o.o., Dr. Franje Tuđmana 16 B, 10431 Sveta Nedjelja, propisuje organizacijske, tehničke i kadrovske mjere za zaštitu osobnih podataka, sve sa svrhom izbjegavanja neovlaštenog uništavanja podataka, njihove izmjene ili gubitka, kao i neovlaštenog pristupa, obrade, korištenja ili prijenosa osobnih podataka.

Zaposlenici i vanjski suradnici koji u svom poslu obrađuju i koriste osobne podatke moraju biti upoznati sa važećim propisima o zaštiti osobnih podataka, Općom uredbom (EU) o zaštiti osobnih podataka (u daljem tekstu: Opća uredba), iz oblasti zakonodavstva koje uređuje pojedinačno područje njihovog posla, sadržajem krovne politike zaštite informacija, politikom zaštite i sigurnosti podataka pojedinih područja poslovanja, te politikom zaštite osobnih podataka iz sadržaja ovog Pravilnika.

Izrazi koji se koriste u ovom Pravilniku, a koji imaju rodno značenje, bez obzira koriste li se u muškom ili ženskom rodu, obuhvaćaju na jednak način muški i ženski rod.

Članak 2.

Pojmovi korišteni u ovom Pravilniku imaju sljedeće značenje:

- Uredba - Uredba (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 (Opća uredba o zaštiti podataka);
- Ispitanik **-** pojedinac čiji je identitet utvrđen ili se može utvrditi;
- Pojedinac čiji se identitet može utvrditi - osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca;
- Osobni podaci - svi podaci koji se odnose na ispitanika ;
- Obrada - svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, automatiziranim i/ili neautomatiziranim sredstvima, kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje;
- Voditelj obrade - fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka, osim u slučajevima kada se svrhe i sredstva obrade utvrđuju pravom Europske Unije ili pravom države članice;
- Primatelj - fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana;
- Treća strana - sve osobe koje nisu zaposlenici i/ili zastupnici voditelja obrade;

- Posebna kategorija osobnih podataka - podaci koji se odnose na rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca;
- Trajni nosač podataka - svako sredstvo koje omogućuje pohranu podataka i kojem se može naknadno pristupiti tijekom određenog vremena u svrhe za koje su te informacije namijenjene i koje omogućuje nepromijenjenu reprodukciju pohranjenih informacija;
- Informacijski sustav - svaki materijalni i nematerijalni dio koji služi za prikupljanje, obradu, pohranu ili distribuciju informacija značajnih u poslovnom procesu;
- Poslovna tajna su podaci koji su označeni sa naznakom tajnosti, sukladno propisima o trgovačkim društvima.
- Koordinator za informacijsku sigurnost - osoba nadležna za definiranje i provedbu programa informacijske sigurnosti unutar informacijskog sustava;
- Administrator sustava - ovlaštena pravna ili fizička osoba koju voditelj obrade ovlasti za obavljanje poslova vezanih uz održavanje sustava hardvera, softvera te drugih sustava vezanih uz poslovanje voditelja obrade, a koji se odnose na postupak informatizacije istog. Administrator sustava može ujedno biti i koordinator za sve navedene poslove.

II. VODITELJ OBRADE

Članak 3.

Društvo LAUS INTERNATIONAL d.o.o. kao voditelj obrade izvršava organizacijske, tehničke i kadrovske mjere iz članka 1. ovog Pravilnika na sljedeći način:

- raspolaže prostorijama, opremom i sistemskom računalnom opremom, uključujući i ulazno- izlazne uređaje,
- osigurava primjenu programske opreme za obradu osobnih podataka,
- sprječava neovlašteni pristup osobnim podacima pri njihovom prijenosu, uključujući i putem telekomunikacijskih sredstava i putem mreže,
- osigurava učinkovit način blokiranja, uništenja ili brisanja osobnih podataka te
- osigurava organizacijsku, kadrovsku i tehničku zaštitu osobnih podataka u poslovanju voditelja obrade.

Poslove iz stavka 1. voditelj obrade provodi u skladu s mjerama koje su definirane i usvojene ovim Pravilnikom.

Voditelj obrade dužan je sklopiti ugovor s izvršiteljem obrade kojim se određuju predmet i trajanje obrade, prirode i svrhe obrade, vrste osobnih podataka i kategorije ispitanika te obveze i prava voditelja obrade.

III. SIGURNOSNE MJERE, ZAŠTITA PROSTORIJA I RAČUNALNE OPREME

Članak 4.

Sigurnosne mjere obuhvaćaju osobna računala, mrežne poslužitelje, mrežne uređaje i mrežnu infrastrukturu informacijskog sustava putem kojih se pristupa informacijskom sustavu te sistemski i korisnički softver, koji se koristi u pojedinim dijelovima informacijskog sustava.

Prostorije u kojima se nalaze trajni nosači podataka, strojna (hardver) i programska (softver) oprema, moraju biti osigurani raznim organizacijskim i fizičkim i/ili tehničkim sredstvima koje sprječavaju neovlašteni pristup podacima (dalje: zaštićeni prostori).

Zaštićeni prostori su zaštićeni sustavom kontrole pristupa, videonadzorom, alarmnim sustavom koji se nalaze u prostorijama voditelja obrade, kao i protupožarnim sustavima (u nastavku teksta: sustavi tehničke zaštite).

Prostorije su zaštićene sustavom kontrole pristupa na način da pravo ulaska imaju samo ovlaštene osoba.
Voditelj obrade vodi evidencije osoba koje imaju ključeve i/ili lozinke za ulazak u zaštićene prostore.

Zaštićeni prostori ne smiju se ostavljati bez nadzora ili u slučaju odsutnosti radnika koji ih nadziru, moraju biti zaključani i osigurani od neovlaštenog pristupa.

Izvan radnog vremena i tijekom odsutnosti radnika voditelja obrade ili koje druge ovlaštene osobe, uredi, ormari i radni stolovi u kojima se nalaze osobni podaci moraju se obavezno zaključavati, a računala i druga računalna oprema moraju biti ugašeni i zaključani fizički ili putem programa.

Radnik koji privremeno napušta radno mjesto, dužan je programski zaključati računalo (engl. „Lock“) radi sprječavanja neovlaštenog pristupa.

Na računalima gdje to nije moguće, potrebno je završiti rad u svim aktivnim programima i odjaviti se s računala.

Sva računala moraju biti sustavno podešena na način da se automatski nakon isteka pet (5) minuta neaktivnosti korisnika zaključavaju.

Osoba iz stavka 6. ovog članka ne smije davati ključeve ili lozinke trećim osobama, ne smije ostavljati ključeve i lozinke na mjestima kojima mogu pristupiti drugi zaposlenici te ne smiju ostavljati ključ u ključanici s vanjske strane.

Posebne kategorije osobnih podataka (dalje: osjetljivi podaci) ne smiju se iznositi izvan zaštićenih prostora.

Članak 5.

Trajni nosači podataka ne smiju se ostavljati na vidljivim i lako dostupnim mjestima.

Trajni nosači podataka koji se nalaze u hodniku ili zajedničkim prostorijama moraju se uvijek zaključavati ili biti pod nadzorom ovlaštenih osoba.

Trajni nosači podataka i monitori na kojima se nalaze osobni podaci, a koji se nalaze u prostorijama u kojima su prisutne treće strane, moraju se čuvati na način da im treće strane nemaju pristup ili uvid.

Članak 6.

Održavanje i popravak strojne i računalne opreme dozvoljen je pod uvjetom da se obavijesti ovlaštena osoba te se može obavljati isključivo u za to ovlaštenim servisima.

Osoblje za održavanje opreme iz stavka 1. ovog članka mora imati potpisan odgovarajući ugovor sa voditeljem obrade.

Članak 7.

Osobe ovlaštene za održavanje prostorija, strojne i programske opreme, posjetitelji i poslovni partneri mogu biti u zaštićenim prostorima samo uz prisutnost ovlaštene osobe voditelja obrade.

Čistačice, zaštitari i druge osobe ne mogu izvan radnog vremena boraviti ili se zadržavati u zaštićenim prostorima.

IV. ZAŠTITA SISTEMSKE I KORISNIČKE RAČUNALNE OPREME TE PODATAKA KOJI SE OBRAĐUJU PUTEM RAČUNALNE OPREME

Članak 8.

Logički pristup svim mrežnim uređajima, koji ima mogućnost upravljanja i konfiguracije, zaštićen je zaporkom.

Pristup informacijskom sustavu mora biti zaštićen na način da se pristup dopusti samo unaprijed određenim radnicima ili fizičkim ili pravnim osobama koje na temelju sklopljenih ugovora pružaju određene usluge voditelju obrade (dalje: izvršitelji obrade).

Radnici i druge ovlaštene osobe moraju svoje ovlasti za pristup informacijskom sustavu koristiti isključivo kroz vlastiti rad te ne smiju drugome omogućiti njihovo korištenje.

Radnici i druge ovlaštene osobe ne smiju pokušati pristupiti nijednom podatku ili programu za koji nemaju dozvolu pristupa ili eksplicitnu suglasnost voditelja obrade.

Ostali radnici i treće strane ne smiju pristupati računalnom sustavu koristeći lozinku i korisničke ovlasti druge osobe.

Pristup informacijskom sustavu imaju i tijela koja provode nadzor nad poslovanjem voditelja obrade.

Radnici ne smiju instalirati programsku opremu bez znanja osoba zaduženih za rad računalnog informacijskog sustava.

Radnici bez odobrenja ovlaštene osobe i znanja osoba zaduženih za rad računalnog informacijskog sustava, ne smiju iznositi računalnu opremu izvan prostorija voditelja obrade.

Članak 9.

Ispravljanje, izmjena i ažuriranje sistemske i korisničke računalne opreme dopuštena je jedino uz odobrenje ovlaštene osobe i može se provoditi samo u ovlaštenim servisima i organizacijama te s osobljem koji na temelju sklopljenih ugovora pružaju određene usluge voditelju obrade.

Ispravljanje, izmjena i ažuriranje sistemske i korisničke računalne opreme mora biti ispravno dokumentirane od strane pružatelja usluge.

Članak 10.

Za pohranu i zaštitu programske opreme na adekvatan način primjenjuju se članci ovog pravilnika koji uređuju postupak čuvanje podataka.

Članak 11.

Voditelj obrade dužan je redovito provjeravati sadržaj mrežnog diska i lokalnih direktorija, u kojima su pohranjeni osobni podaci, zaštićeni od računalnih virusa.

U slučaju pojave računalnog virusa isti se mora ukloniti što je prije moguće od strane ugovorene vanjske stručne službe voditelja obrade i/ili izvršitelja obrade te se mora identificirati uzrok pojave virusa u informacijskom sustavu voditelja obrade.

Svi primljeni trajni nosači podataka i sadržaji preuzeti s Interneta ili drugih računala koji ne pripadaju voditelju obrade moraju biti provjereni kako bi se detektirali i uništili virusi ili drugi potencijalno maliciozni programi.

Stavci 1.,2. i 3. ovog članka primjenjuju se i u slučaju prijenosa datoteke s računala koja nisu u vlasništvu voditelja obrade.

Članak 12.

Radnici ne smiju namještati programsku opremu bez znanja i dopuštenja osobe odgovorne za djelovanje računalnog informacijskog sustava.

Nije dopušteno iznošenje programske opreme i trajnih nosača na kojima se osobni podaci čuvaju izvan prostorija voditelja obrade, bez znanja i odobrenja izravno nadređene odgovorne osobe ili koordinatora za informacijsku sigurnost ili osobe koju je voditelj obrade ovlastio da obavlja te poslove.

Radnici ne smiju kopirati, instalirati ili izvoditi programe kojima je svrha otkrivati sigurnosne slabosti na sustavu te ne smiju neovlašteno izvoditi programe za prikupljanje podataka o informacijskom sustavu.

U slučaju pojave potrebe za enkripcijom podataka, radnik može upotrijebiti softver za enkripciju podataka koji je propisan od strane voditelja obrade.

Radnici ne smiju raditi kopije konfiguracijskih i sistemskih datoteka, ne smiju takve datoteke neovlašteno koristiti, ne smiju ih koristiti za namjenu koja je različita od osnovne namjene te ih ne smiju neovlašteno davati na uvid drugim osobama.

Članak 13.

Pristup podacima korisničkog softvera zaštićen je korisničkim imenom i lozinkom za autorizaciju i identifikaciju programa i korisničkih podataka.

Sistem lozinke mora pružiti mogućnost naknadne procjene sljedećeg:

- kada su određeni osobni podaci upisani u bazu podataka, kada se koriste ili na drugi način obrađuju i
- tko je izvršio neku od prethodno navedenih radnji.

Administrator sustava, temeljem pisanog zahtjeva odgovorne osobe, dodjeljuje ovlaštenim radnicima korisničko ime i lozinku, kako bi mogli pristupiti dijelovima informacijskog sustava.

Za pristup različitim dijelovima informacijskog sustava korisnicima mogu biti dodijeljeni različiti korisnički računi i lozinke.

Korisnici su dužni lozinke redovito mijenjati i držati tajnima.

Svaki je radnik odgovoran za zaštitu svih informacija korištenih ili spremljenih posredstvom vlastitih korisničkih ovlasti.

Radnici su odgovorni za sve transakcije i aktivnosti koje se obave s dodijeljenim korisničkim računom te ne smiju otkriti ili dijeliti korisničke račune i lozinke s drugim osobama.

Članak 14.

Postupak određivanja lozinki odnosno način dodjeljivanja, pohrana i mijenjanje lozinki, predlaže voditelj obrade ili osoba koju on za to ovlasti.

Pri izboru i primjeni lozinki, administrator sustava dužan je poštovati sljedeće smjernice:

- lozinke moraju biti kombinacija alfanumeričkih znakova i specijalnih znakova,
- lozinke ne mogu biti u obliku imena osoba, zemljopisnih pojmova, karakterističnih datuma povezanih sa zaposlenikom ili drugih riječi koje se ne mogu lako pogoditi,
- lozinka se mora sastojati od najmanje 6 znakova, od kojih je najmanje jedan specijalni znak (različit od alfanumeričkih znakova),
- lozinka koja dolazi kod početne instalacije programskih paketa ili uređaja mora biti zamijenjena.

Članak 15.

Sve lozinke i postupci koji se koriste za pristup i upravljanje mrežama, upravljanje e-mailovima i programima moraju se čuvati na sigurnim mjestima i moraju biti zaštićeni od neovlaštenog pristupa. Smiju se koristiti jedino u iznimnim ili hitnim situacijama.

Članak 16.

Za potrebe obnavljanja računalnog sustava prilikom kvara ili u slučaju bilo koje druge izvanredne situacije najmanje jednom dnevno radi se kopija sadržaja mrežnog diska i lokalnih direktorija, kao i podataka iz svih ključnih poslovnih aplikacija.

Kopije iz stavka 1. pohranjuju se u zaštićenim prostorijama, a sve sukladno odredbama ovog Pravilnika.

Pristup arhiviranim kopijama potrebno je ograničiti isključivo na osobe koje za to imaju poslovnu potrebu.

V. ODVAJANJE U MREŽI (SEGMENTIRANJE)

Članak 17.

Mreža je segmentirana u posebne logičke mrežne segmente kako bi se omogućilo definiranje posebnih prava pristupa pojedinim mrežnim resursima, informacijskim sustavima i uslugama, u skladu s poslovnim potrebama.

Segmentiranje mreže provedeno je uzevši u obzir:

- organizacijsku strukturu voditelja obrade,
- vrstu informacijskih resursa i informatičkih usluga kojima se treba pristupati,
- vrijednost i klasifikacija podataka kojima se pristupa preko tih resursa,
- procjenu rizika za povjerljivost, integritet i dostupnost informacija koje se prenose ili se nalaze u određenom mrežnom segmentu.

Članak 18.

Određene mreže mogu se smatrati nesigurnima.

Nesigurne mreže su, ali ne ograničavaju se na:

- Internet,
- bežične lokalne mreže
- mreže vanjskih partnera.

Kontrola pristupa radnika ili izvršitelja obrade iz nesigurnih mreža na mrežnu infrastrukturu provodi se korištenjem vatrozida (engl. firewall).

Pravila pristupa na vatrozidu dozvoljavaju pristup samo određenim mrežnim segmentima i samo ograničenom broju komunikacijskih protokola.

Članak 19.

Segmentiranje mreže uz kontrolu pristupa logičkim mrežnim segmentima vrši se putem listi za kontrolu pristupa na središnjem vatrozidu.

Tehnike za segmentiranje mreže uz kontrolu pristupa logičkim mrežnim segmentima mogu biti ostvarene korištenjem, vatrozida, kontrola mrežnog usmjeravanja uz istodobnu uporabu listi za kontrolu pristupa (engl. Access Control List) itd.

Osnovni princip od kojeg se polazi kod uspostave kontrole pristupa jest da se omogućuje pristup isključivo do onih mrežno dostupnih resursa koji su potrebni za obavljanje redovitih radnih aktivnosti.

Članak 20.

Davatelj informatičkih usluga odgovoran je za provođenje aktivnosti vezanih za segmentiranje mrežne infrastrukture i održavanje pristupnih lista mrežnih uređaja i vatrozida temeljem zahtjeva odgovornih osoba voditelja obrade.

Sve promjene na pristupnim listama mrežnih uređaja i vatrozida moraju biti evidentirane i provedene u skladu s procedurama za upravljanje promjenama na mrežnoj infrastrukturi.

O svim promjenama na pristupnim listama mrežnih uređaja i vatrozida, davatelj informatičkih usluga (izvršitelj obrade) dužan je obavijestiti koordinatora za informacijsku sigurnost voditelja obrade.

VI. PRISTUP INTERNETU I SADRŽAJU ELEKTRONIČKE POŠTE

Članak 21.

Pristup preko bežične lokalne mreže (eng. WLAN) je pristup definiran IEEE 802.11 skupinom standarda.

Bežični pristup korporativnoj mreži voditelja obrade mora biti poslovno opravdan pri čemu se jasno trebaju odrediti segmenti mreže kojima se može bežično pristupiti te komunikacijski protokoli koji se mogu pri tome koristiti.

Članak 22.

Nije dozvoljeno postavljanje pristupnih točaka za bežični pristup bez dozvole odgovorne osobe davatelja informatičkih usluga.

Potrebno je provoditi periodičke provjere kako bi se spriječilo neautorizirano ili nekontrolirano postavljanje pristupnih točaka za bežični pristup.

Članak 23.

Pod udaljenim pristupanjem i upravljanjem računalima i računalnim sustavima podrazumijeva pristup jednom dijelu ili dijelovima IT sustava putem različitih komunikacijskih tehnologija, aplikacija i protokola koji ne zahtjeva fizičku prisutnost tom dijelu sustava.

Za udaljeni pristup zaposlenika internoj mreži voditelj obrade mora osigurati provjeru vjerodostojnosti.

Korisnici mogu pristupiti IT sustavu putem udaljene veze samo ako su ispunjeni ovi uvjeti:

- Pristup mora biti odobren od strane uprave ili druge odgovorne osobe
- Pristup mora biti omogućen i odobren od strane IT odjela
- Pristup mora biti kontroliran od strane IT odjela
- Aplikacije i protokoli za pristup moraju biti osigurani od strane IT odjela
- Korisnici mogu koristiti samo aplikacije i protokole koje im je dodijelio IT odjel.
- Korisnici mogu imati pristup samo onim dijelovima sustava koji im je odobrila Uprava i dodijelio IT odjel.
- Pristupni podatci su zaštićeni od krađe. (kriptirani)

Korisnici ne smiju dijeliti svoje pristupne podatke s bilo kojom trećom stranom.

Korisnici ne smiju dijeliti informacije s IT sustava s neovlaštenom trećom stranom.

Svaki udaljeni pristup informatičkom sustavu voditelja obrade poslovno je opravdan i dokumentiran, te zabilježen u sustavu.

Članak 24.

Radnik i druga ovlaštena osoba mogu pristupati sustavu elektroničke pošte i koristiti se njime isključivo temeljem dodijeljenih korisničkih prava, svojeg korisničkog imena i pripadajuće lozinke.

Radnik i druga ovlaštena osoba dužna je birati i čuvati lozinke u skladu s odredbama ovog Pravilnika.

Članak 25.

Radnici i druge ovlaštene osobe mogu se koristiti zajedničkom adresom elektroničke pošte kada je to svrsishodno za obavljanje uobičajenih poslovnih aktivnosti.

Radnici i druge ovlaštene osobe dužne su koristiti se, određivati i čuvati lozinke zajedničke adrese elektroničke pošte u skladu s odredbama ovog Pravilnika.

Administrator IT sustava odgovoran je za dodjeljivanje i promjenu lozinke, kao i za povlačenje ovlaštenja pristupa u slučaju prestanka radnog odnosa ili u slučaju nastupa drugih okolnosti uslijed kojih bi radnik izgubio ovlast pristupa iz stavka 1. ovog članka.

VII. ZAŠTITA OSOBNIH PODATAKA KOD UPORABE MOBILNE RAČUNALNE OPREME I RADA NA DALJINU

Članak 26.

Pod mobilnom računalnom opremom podrazumijeva se:

- prijenosno računalo
- tablet računalo
- mobilni telefon
- pametni telefoni

Rad izvan mjesta je obavljanje poslovnih aktivnosti s bilo koje druge lokacije koja nije glavna lokacija radnika pri obavljanju poslovnih zadataka, a koji predstavlja dogovor između voditelja obrade i radnika.

Članak 27.

Razina informacijske sigurnosti koju zahtijeva voditelj obrade pri korištenju informacijskog sustava mora biti zadržana prilikom korištenja mobilne računalne opreme i pri radu na daljinu.

Ovlaštene osobe unutar voditelja obrade odgovorne su za zaduživanje, podešavanje, održavanje i razduživanje mobilne računalne opreme na kojoj se nalaze osobni podaci, a nakon čega postaju odgovornost radnika.

Pristup i korištenje mobilne računalne opreme radnika nije dozvoljeno članovima obitelji, prijateljima te bilo kojim drugim fizičkim i pravnim osobama.

Članak 28.

Radnik je odgovoran za zaštitu mobilne računalne opreme od krađe i neovlaštenog pristupa u svako vrijeme i na svakom mjestu.

U slučajevima kada se mobilna računalna oprema ne koristi, ona mora biti adekvatno zaštićena od krađe ili neovlaštenog pristupa.

Korisnik je dužan odmah prijaviti bilo kakav sigurnosni incident povezan s mobilnom računalnom opremom davatelju informatičkih usluga ili koordinatoru za informacijsku sigurnost.

Članak 29.

Pristup mobilnoj računalnoj opremi mora biti zaštićen sigurnosnim mehanizmima za identifikaciju i autorizaciju korisnika.

Prilikom rada na javnim mjestima i na mjestima na kojima postoji povećana prijetnja od nadgledanja rada od strane neovlaštene osobe, radnik treba voditi računa da spriječi promatranje svog rada, osobito ako se na trajnom nosaču podataka ili monitoru nalaze osobni podaci.

Na mjestima iz stavka 2. ovog članka, obvezno je zaključavanje računala opcijom Lock computer ili odjava rada iz sustava opcijom Log off za vrijeme za koje se prijenosno računalo ne koristi.

Na mobilnoj računalnoj opremi zabranjeno je korištenje dijeljenih direktorija odnosno dijeljenje lokalnih direktorija na mobilnoj računalnoj opremi s drugima.

Članak 30.

Kod mobilne računalne opreme cijeli tvrdi disk ili drugi oblik perzistentne memorije potrebno je kriptirati (šifrirati) korištenjem odgovarajućih tehnologija. Davatelj informatičkih usluga je odgovoran za odabir odgovarajuće tehnologije i procesa podrške za ispunjavanje ovog zahtjeva

Iznimno, kod uređaja gdje ne postoje tehničke mogućnosti kriptiranje cijele perzistentne memorije, moraju biti kriptirani barem osobni podaci.

Davatelj informatičkih usluga osigurava proces izrade kopija podataka, a radnici se moraju pridržavati odgovarajućih uputa od davatelja informatičkih usluga.

Članak 31.

Rad na daljinu zahtijeva odgovarajuću razinu zaštite od krađe opreme i podataka, neovlaštenog otkrivanja podataka, neovlaštenog udaljenog pristupa informacijskom sustavu voditelja obrade te neovlaštenog korištenja informacijskog sustava voditelja obrade.

Članak 32.

Zahtjev za udaljeni pristup računalnoj mreži voditelja obrade može podnijeti radnik za to odgovornoj osobi ili ga može dati odgovorna osoba isključivo zbog poslovnih razloga.

Izvan radnog mjesta dopušteno je koristiti sustave i servise koje definira i za njih pismeno odobrava odgovorna osoba kroz odobrenje zahtjeva.

Radniku kojem se odobrava pristup iz stavka 1. i 2. ovog članka, ne smije biti izrečena opomena zbog neprimjerenog korištenja informacijskog sustava.

Prilikom rada na daljinu radniku se ne mijenjaju poslovne odgovornosti kao ni obveze i prava koja proizlaze iz opisa njegova radnog mjesta.

Članak 33.

Korištenje bežične lokalne mreže (engl. Wireless LAN ili WLAN) u javnim prostorima (npr. zračne luke, hoteli itd.) treba biti svedeno na minimum.

U slučaju korištenja bežične lokalne mreže zaposlenici moraju biti svjesni rizika nezaštićene komunikacije na mreži.

Pristup dijelovima informacijskog sustava voditelja obrade dozvoljen je isključivo uz upotrebu SSL VPN pristupa koji osigurava zaštićenu komunikacijsku liniju između mobilnog uređaja i informacijskog sustava voditelja obrade.

Radnici ne smiju izmjenjivati osobne podatke u nezaštićenom obliku (nekriptiranom) korištenjem bežične lokalne mreže u javnim prostorima.

Članak 34.

Prilikom obavljanja rada na daljinu zaposlenicima nije dozvoljeno korištenje privatne mobilne računalne opreme (npr. privatno prijenosno računalo).

Iznimno, u slučaju izvanrednih okolnosti korištenje privatne mobilne računalne opreme za rad na daljinu moguć je isključivo uz prethodnu konzultaciju s nadležnom osobom zaduženom za informacijsku sigurnost.

Članak 35.

Na osnovu odobrenog zahtjeva za udaljeni pristup, zaposlenik ili nadređena odgovorna osoba prosljeđuju taj zahtjev davatelju informatičkih usluga.

Udaljeni pristup informacijskom sustavu treba se implementirati korištenjem sigurnih mehanizama autentikacije i autorizacije.

Davatelj informatičkih usluga treba osigurati udaljeni pristup samo onim dijelovima informacijskog sustava koji se nalaze u zahtjevu za udaljeni pristup.

Komunikacijski kanali kojima se prilikom pristupa informacijskom sustavu prenose podaci moraju biti kriptirani koristeći sigurne mehanizme kao što je korištenje IPSec Ili SSL tehnologija.

Članak 36.

Autentikacija kod udaljenog pristupa dijelovima informacijskog sustava uvijek se odnosi na individualni pristup.

Nije dozvoljeno korištenje tuđih ili grupnih korisničkih imena i lozinki za udaljeni pristup informacijskog sustava.

Članak 37.

Prava udaljenog pristupa informacijskom sustavu voditelja obrade, odobrena na temelju zahtjeva za udaljeni pristup, mogu trajati najviše deset godina odnosno do povlačenja ovlaštenja od strane odgovorne osobe voditelja obrade..

Istekom roka iz stavka 1. ukidaju se dodijeljena prava.

Radnik može ponovno dobiti pravo udaljenog pristupa informacijskom sustavu na temelju novog zahtjeva za udaljeni pristup.

Članak 38.

Dodijeljena prava za udaljeni pristup traju do isteka roka na koji je radniku odobren rad na daljinu..

VIII. USLUGE KOJE PRUŽAJU VANJSKE FIZIČKE ILI PRAVNE OSOBE

Članak 39.

Svaka vanjska fizička ili pravna osoba koja obavlja poslove obrade osobnih podataka, kao što je prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, uporaba, otkrivanje, ograničavanje, brisanje ili uništavanje i koja je registrirana za obavljanje takve djelatnosti (izvršitelj obrade), mora sklopiti pisani ugovor s voditeljem obrade.

Ugovor iz stavka 1. definira uvjete i mjere kojima se osigurava zaštita osobnih podataka, a odnosi se i na vanjske suradnike koji održavaju, proizvode i uvode računalnu i strojnu opremu.

Izvršitelji obrade obavljaju usluge obrade osobnih podataka u kontekstu i opsegu dozvole klijenata te podatke kojima ima pristup na osnovi ugovora s voditeljem obrade ne smiju obrađivati niti na bilo koji drugi način koristiti.

Izvršitelj obrade koji pruža svoje usluge izvan prostorija voditelja obrade mora imati razinu zaštite osobnih podataka prilagođenu Općoj uredbi o zaštiti podataka i zakonskim propisima koji reguliraju obradu osobnih podataka.

IX. PRIJAM I PRIJENOS OSOBNIH PODATAKA

Članak 40.

Radnik, koji je odgovoran za prijam i evidentiranje pošte, dužan je:

- predati pošiljku s osobnim podacima direktno pojedincima ili odjelima na koje se odnose,
- otvarati i pregledavati pošiljke koje na bilo koji način pristignu u prostorije voditelja obrade, osim pošiljaka koje su naslovljene na neko drugo tijelo ili organizaciju, a dostavljeni su zabunom.

Članak 41.

Dozvoljen je prijenos osobnih podataka putem informacijskih, telekomunikacijskih i drugih sredstava, samo kad se koriste postupci i mjere zaštite od neovlaštenog prisvajanja ili uništavanja podataka te neopravdano upoznavanje s njihovim sadržajem.

Radnici koji su ovlašteni za prijem i evidentiranje pošte, ne otvaraju one pošiljke koje su naslovljene na drugo društvo i koje su greškom dostavljene, kao i pošiljke koje su označene kao osobni podaci, ili za koje iz označavanja na omotu proizlazi da se odnose na natječaj i/ili javnu nabavu.

Radnici koji su ovlašteni za prijem i evidentiranje pošte, ne smiju otvarati pošiljke naslovljene na drugog radnika, kada je na omotu navedeno da se uručuju osobno (oznaka N/R).

Stavak 3. ovog članka primjenjuje se i u slučaju pošiljaka na kojima je prvo navedeno osobno ime radnika, bez naznake njegovog službenog položaja i tek nakon navedenoga adresa društva.

Osjetljivi podaci šalju se na određene adrese u zapečaćenoj omotnici uz potpis u knjizi pošiljaka ili isporuku uz potvrdu primitka.

Osobni podaci šalju se preporučenom poštom s povratnicom. Te je nužno osigurati da se ne može izvršiti otvaranje i uvid u sadržaj omotnice bez ostavljanja traga od otvaranja iste.

Omotnica u kojoj se šalju osobni podaci mora biti izrađena na način da je nemoguće vidjeti sadržaj omotnice u normalnom ili posebnom osvjetljenju.

Članak 42.

Obrada osjetljivih podataka mora biti posebno naznačena i zaštićena.

Zabranjuje se obrada osobnih podataka koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca.

Stavak 2. ne primjenjuje se ako je ispunjeno jedno od sljedećeg:

(a) ispitanik je dao izričitu privolu za obradu tih osobnih podataka za jednu ili više određenih svrha, osim ako se pravom Unije ili pravom države članice propisuje da ispitanik ne može ukinuti zabranu iz stavka 2.;

(b) obrada je nužna za potrebe izvršavanja obveza i ostvarivanja posebnih prava voditelja obrade ili ispitanika u području radnog prava i prava o socijalnoj sigurnosti te socijalnoj zaštiti u mjeri u kojoj je to odobreno u okviru prava Unije ili prava države članice ili kolektivnog ugovora u skladu s pravom države članice koje propisuje odgovarajuće zaštitne mjere za temeljna prava i interese ispitanika;

(c) obrada je nužna za zaštitu životno važnih interesa ispitanika ili drugog pojedinca ako ispitanik fizički ili pravno nije u mogućnosti dati privolu;

(d) obrada se provodi u sklopu legitimnih aktivnosti s odgovarajućim zaštitnim mjerama zaklade, udruženja ili drugog neprofitnog tijela s političkim, filozofskim, vjerskim ili sindikalnim ciljem te pod uvjetom da se obrada odnosi samo na članove ili bivše članove tijela ili na osobe koje imaju redovan kontakt s njom u vezi s

njezinim svrhama i da osobni podaci nisu priopćeni nikome izvan tog tijela bez privole ispitanika;

(e) obrada se odnosi na osobne podatke za koje je očito da ih je objavio ispitanik;

(f) obrada je nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva ili kada sudovi djeluju u sudbenom svojstvu;

(g) obrada je nužna za potrebe značajnog javnog interesa na temelju prava Unije ili prava države članice koje je razmjerno željenom cilju te kojim se poštuje bit prava na zaštitu podataka i osiguravaju prikladne i posebne mjere za zaštitu temeljnih prava i interesa ispitanika;

(h) obrada je nužna u svrhu preventivne medicine ili medicine rada radi procjene radne sposobnosti zaposlenika, medicinske dijagnoze, pružanja zdravstvene ili socijalne skrbi ili tretmana ili upravljanja zdravstvenim ili socijalnim sustavima i uslugama na temelju prava Unije ili prava države članice ili u skladu s ugovorom sa zdravstvenim radnikom te u skladu s uvjetima i zaštitnim mjerama iz stavka 4.;

(i) obrada je nužna u svrhu javnog interesa u području javnog zdravlja kao što je zaštita od ozbiljnih prekograničnih prijetnji zdravlju ili osiguravanje visokih standarda kvalitete i sigurnosti zdravstvene skrbi te lijekova i medicinskih proizvoda, na temelju prava Unije ili prava države članice kojim se propisuju odgovarajuće i posebne mjere za zaštitu prava i sloboda ispitanika, posebno čuvanje profesionalne tajne;

(j) obrada je nužna u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe na temelju prava Unije ili prava države članice koje je razmjerno cilju koji se nastoji postići te kojim se poštuje bit prava na zaštitu podataka i osiguravaju prikladne i posebne mjere za zaštitu temeljnih prava i interesa ispitanika.

Iznimno, osobni podaci iz stavka 2. mogu se obrađivati u svrhe navedene u stavku 3. točki (h) kada te podatke obrađuje stručno tijelo ili se podaci obrađuju pod odgovornošću stručnog tijela koje podliježe obvezi čuvanja poslovne tajne sukladno pravu Unije ili pravu države članice ili pravilima koja su odredila nadležna nacionalna tijela ili druga osoba koja podliježe obvezi čuvanja tajne sukladno pravu Unije ili pravu države članice ili pravilima koja su utvrdila nadležna nacionalna tijela.

Osjetljivi podaci mogu biti poslani elektroničkom poštom samo ako se koristi neki od oblika enkripcije poruka elektroničke pošte, a koji su odobreni i podržani od strane voditelja obrade. Prilog 1. ovog Pravilnika propisuje jedan od načina zaštite podataka prilikom slanja.

Članak 43.

Osobni podaci daju se na uvid primateljima koji za to imaju odgovarajuću pravnu osnovu.

Originalni i izvorni dokumenti ne smiju se prenositi osim u slučaju pisane sudske odluke.

U slučaju iz stavka 2.dokumente tijekom odsustva moraju zamijeniti kopije.

X. BRISANJE PODATAKA

Članak 44.

Osobni podaci čuvaju se dok traje zakonska osnova za njihovo prikupljanje i obradu.

Po proteku roka iz stavka 1.osobni podaci se moraju obrisati, uništiti ili anonimizirati, osim ako zakonom ili drugim aktom nije previđeno drugačije.

Revizija dokumentacija, provjera isteka rokova te pohranjivanje i uništavanje dokumentacije vrši se minimalno jednom godišnje.

Članak 45.

Ispitanik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose bez nepotrebnog odgađanja, a voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako je ispunjen jedan od sljedećih uvjeta:

a) osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili na drugi način obrađeni;

b) ispitanik povuče privolu na kojoj se obrada temelji

c) ispitanik uloži prigovor na obradu osobnih podataka koji se odnose na njega, u slučajevima:

-kada je obrada nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade,

-kada je obrada nužna za potrebe legitimnih interesa voditelja obrade ili treće strane te

-kada ne postoje jači legitimni razlozi za obradu ili ispitanik uloži prigovor na obradu ako se osobni podaci koji se odnose na njega obrađuju za potrebe izravnog marketinga, što uključuje izradu profila u mjeri koja je povezana s takvim izravnim marketingom;

d) osobni podaci nezakonito su obrađeni;

e) osobni podaci moraju se brisati radi poštovanja pravne obveze iz prava Unije ili prava države članice kojem podliježe voditelj obrade;

f) osobni podaci koji su prikupljeni u vezi s ponudom usluga informacijskog društva izravno djetetu, ako dijete ima najmanje 16 godina ili je privolu dao ili odobrio nositelj roditeljske odgovornosti nad djetetom.

Ako je voditelj obrade javno objavio osobne podatke, a ispitanik zatraži brisanje svojih osobnih podataka, voditelj obrade dužan je obrisati te podatke, poduzimajući razumne mjere, uključujući tehničke mjere, kako bi informirao voditelje obrade koji obrađuju osobne podatke da je ispitanik zatražio od tih voditelja obrade da izbrišu sve poveznice do njih ili kopiju ili rekonstrukciju tih osobnih podataka.

Članak 46.

Pravo na brisanje ne primjenjuje se u mjeri u kojoj je obrada nužna:

a) radi ostvarivanja prava na slobodu izražavanja i informiranja;

b) radi poštovanja pravne obveze kojom se zahtijeva obrada u pravu Unije ili pravu države članice kojem podliježe voditelj obrade ili za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;

c) zbog javnog interesa u području javnog zdravlja;

d) u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u mjeri u kojoj je vjerojatno da se pravom na brisanje može onemogućiti ili ozbiljno ugroziti postizanje ciljeva te obrade te

e) radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva.

Članak 47.

Za brisanje podataka iz računalnih medija koristi se takva metoda brisanja da je nemoguće vratiti sve ili dio obrisanih podataka.

U slučaju ponovne upotrebe ili prenamjene medija s pohranjenim osobnim podacima, potrebno je provesti trajno brisanje sadržaja medija s ciljem potpunog onemogućavanja mogućnosti rekonstrukcije izvornih podataka.

U slučaju prestanka korištenja medija, medije je potrebno fizički uništiti.

Članak 48.

Podaci na klasičnim medijima, kao što su dokumenti, registratori, popisi, moraju se uništiti na način da je nemoguće pročitati sve ili dio uništenih podataka, i to korištenjem prikladnih uništavača dokumenata (npr. rezač papira).

Na način iz stavka 1. potrebno je uništiti sve dodatne materijale kao što su tablice i skice odnosno nacrti pojedinih dokumenata.

Zabranjeno je bacati nosače podataka u koševe za smeće.

Nosače podataka potrebno je zbrinuti na adekvatan način kako bi se osiguralo da pristup podacima koji su bili na njemu pohranjeni nije moguć.

XI. POSTUPANJE PRILIKOM SUMNJE NA NEOVLAŠTENI PRISTUP

Članak 49.

Radnici su obvezni odmah obavijestiti voditelja obrade ili osobu koju je on za to ovlastio kao koordinatora informacijske sigurnosti o aktivnostima koje se odnose na otkrivanje neovlaštenog pristupa zaštićenim podacima, kao i o zlonamjernim ili neovlaštenim korištenjima, prisvojenjima, izmjenama ili oštećenjima takvih podataka.

Radnici su obvezni spriječiti bilo koju od aktivnosti koje se mogu smatrati neovlaštenim pristupom..

Voditelj obrade ili osoba koju je ovlastio za obavljanje poslova informacijske sigurnosti dužan je odmah po saznanju, o aktivnostima iz stavka 1., obavijestiti službenika za zaštitu osobnih podataka.

Voditelj obrade posebnim internim aktima propisati će metodologiju i postupanje u slučaju neovlaštenog pristupa i/ili u slučaju incidenta kao što je sigurnosni incident i/ili incident koji je vezan uz zaštitu osobnih podataka.

Članak 50.

Radnici i druge ovlaštene osobe dužni su u najkraćem mogućem roku obavijestiti voditelja obrade ili osobu koju je voditelj obrade ovlastio za obavljanje poslova informacijske sigurnosti ili druge ovlaštene osobe o svakom događaju koji upućuje na povredu sigurnosnih mjera koje proizlaze iz ovog Pravilnika.

Radnici i druge ovlaštene osobe moraju izvijestiti osobu ovlaštenu za obavljanje poslova informacijske sigurnosti o svakom uočenom nedostatku u sustavu sigurnosti informacijskog sustava.

Osoba ovlaštena za obavljanje poslova informacijske sigurnosti dužna je o okolnostima iz stavka 1. i 2. obavijestiti ovlaštenu osobu voditelja obrade.

Članak 51.

U slučaju da radnici ili druge ovlaštene osobe iz vanjskih izvora doznaju o pojavi virusa ili sigurnosnoj prijetnji, dužni su o tome obavijestiti osobe iz članka 53. ovog Pravilnika.

Radnici i druge ovlaštene osobe ne smiju samostalno poduzimati aktivnosti u slučaju iz stavka 1. ovog članka te ne smiju takve obavijesti slati drugim zaposlenicima ili ovlaštenim osobama u obliku masovne ili lančane elektroničke pošte.

Osoba ovlaštena za obavljanje poslova informacijske sigurnosti dužna je o okolnostima iz stavka 1. i 2. obavijestiti službenika za zaštitu osobnih podataka.

XII. ODGOVORNOST ZA PRIMJENU MJERA I POSTUPAKA

Članak 52.

Zakonski zastupnici voditelja obrade i ovlaštene osobe imenovane od strane voditelja obrade, odgovorni su za primjenu postupaka i mjera za zaštitu osobnih podataka kako je to uređeno ovim Pravilnikom.

Voditelj obrade kao poslodavac može radniku otkazati ugovor o radu, u slučaju grubog kršenja ovog Pravilnika ili teške povrede odredaba ovog Pravilnika.

Članak 53.

Svatko tko obrađuje osobne podatke dužan je postupati sukladno propisanim postupcima i mjerama radi sigurnosti i zaštite podataka, a koje mu moraju biti dostupne tijekom procesa obrade.

Obveza postupanja u skladu sa zaštitom podataka ne prestaje sa završetkom radnog odnosa ili koje druge pravne osnove.

Prije zaposlenja na radnom mjestu na kojem se obrađuju osobni podaci, radnik mora potpisati posebnu izjavu koja ga obvezuje da poštuje pravila o zaštiti osobnih podataka.

Kadrovska služba čuva izjavu iz stavka 3. ovog članka u dokumentu ″Evidencija radnika″.

Članak 54.

Nakon prestanka radnog odnosa kod voditelja ili izvršitelja obrade, radnik je dužan vratiti ovlaštenoj osobi svu računalnu i komunikacijsku opremu i sve podatke (i njihove kopije) kojima je bio u posjedu tijekom rada u kompaniji.

Nije dozvoljeno zadržavanje računalne i komunikacijske opreme te podataka bez pisane dozvole ovlaštene osobe voditelja obrade ili izvršitelja obrade.

Radnik ne smije koristiti službenu opremu suprotno od načina na koji mu je odredio voditelj obrade.

Članak 55.

Pravilnik stupa na snagu u roku jednog dana od dana donošenja.

Danom stupanja na snagu ovog Pravilnika prestaju važiti svi pravilnici o zaštiti osobnih podataka u Laus International d.o.o.

Pravilnik će se objaviti na Oglasnoj ploči poslodavca i poslati svim radnicima na mail.

U Zagrebu, 13. travnja 2021. godine

Laus International d.o.o.

Mislav Kurtela, Direktor

PRILOG 1. Pravilnika

UPUTE O ZAŠTITI DOKUMENTA ŠIFROM

Kako zaštititi dokument (Word, Excel, PowerPoint) šifrom prije slanja drugim fizičkim ili pravnim osobama koje nisu dio _____ ili osobama unutar _____ ukoliko se radi o posebnim kategorijama osobnih podataka, prijenosu u treće zemlje ili drugim dokumentima unutar kojih se obrađuju kategorije podataka i ispitanika koje su posebno zaštićene te su kao takve određene ovim Pravilnikom.

1. Otvorite document (Word, Excel, PowerPoint)

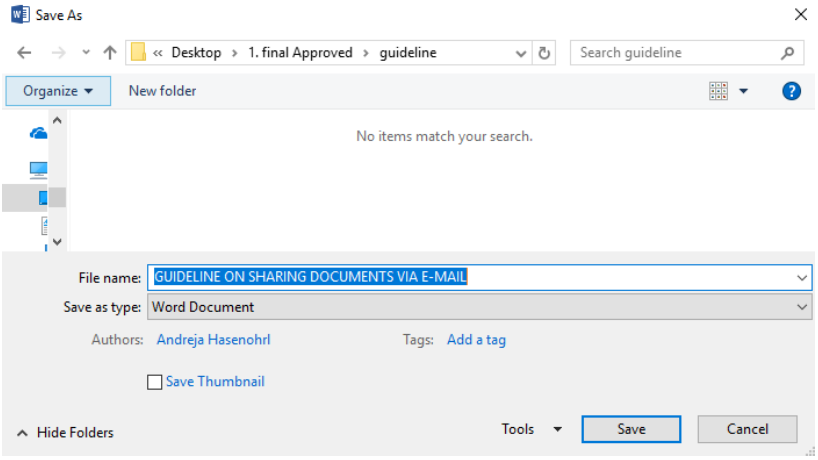
2. Kliknite na **File,** zatim odaberite **Save As,** napišite ili odaberite naziv datoteke i odredite lokaciju za spremanje dokumenta

Commented [NĐ1]: Koje su posebne kategorije osobnih podataka? Da li je ova Uputa obvezni dio Pravilnika tj u kojim slučajevima je obvezno/preporuča se slanje šifriranih dokumenata?

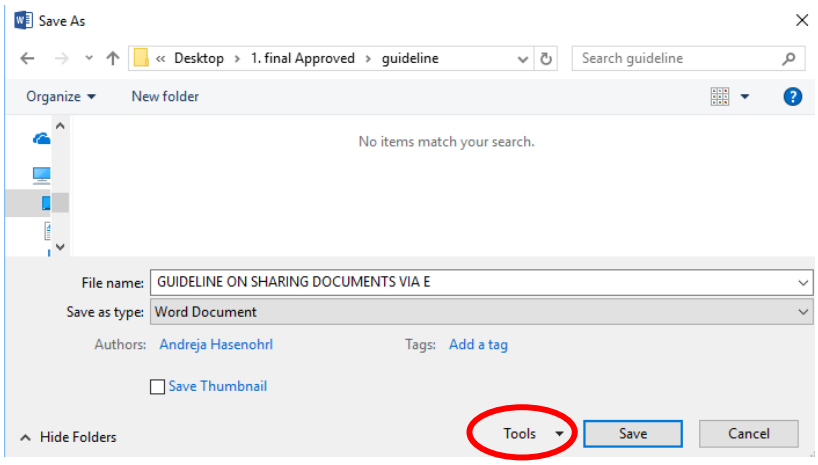
Commented [ab2R1]: Posebne kategorije podataka su primjerice podaci o zdravlju, podaci vezani uz sindikate i sl. Uređeno člankom 9. Opće uredbe o zaštiti podataka.

Uputa ne mora biti dio Pravilnika ali se preporuča jer je bitan dio politika sigurnosti svih društava.

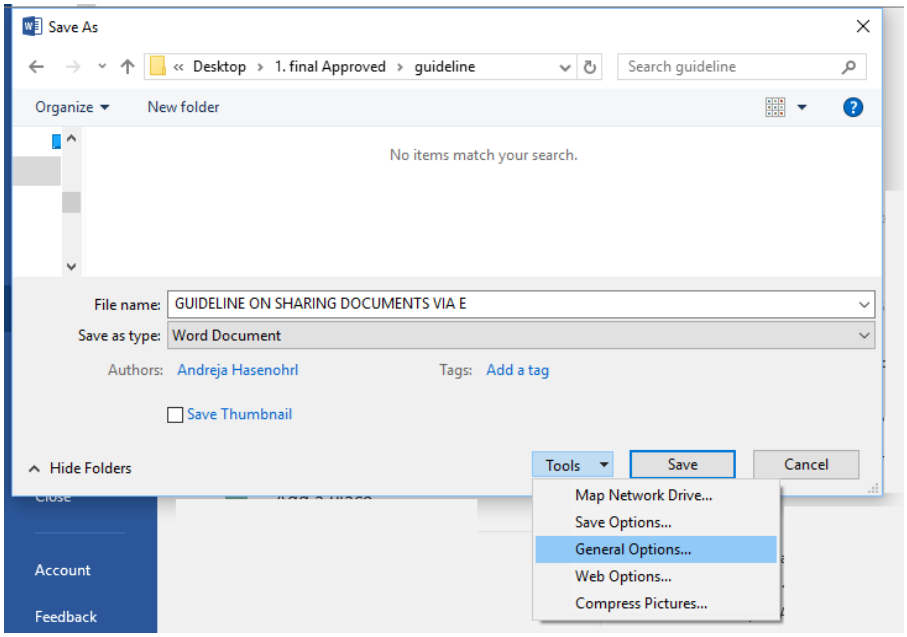
Morate šifrirati i zaštiti podatke koji se šalju izvan Lausa a sadržavaju veliki obim ili podataka zaposlenika (primjerice plaće radnika. KPI-evi, bonusi, raspored go i sl.) ili kada se šalju posebne kategorije podataka.


Save As
Desktop › 1. final Approved › guideline
Search guideline
Organize
New folder
No items match your search.
File name: GUIDELINE ON SHARING DOCUMENTS VIA E-MAIL
Save as type: Word Document
Authors: Andreja Hasenohrl
Tags: Add a tag
Save Thumbnail
Hide Folders
Tools
Save
Cancel

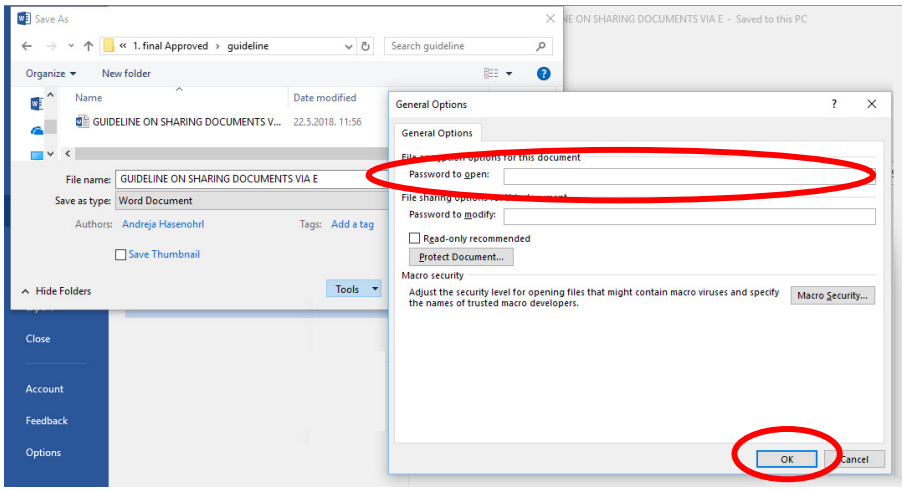
3. Kliknite na **Tools** u desnom donjem kutu



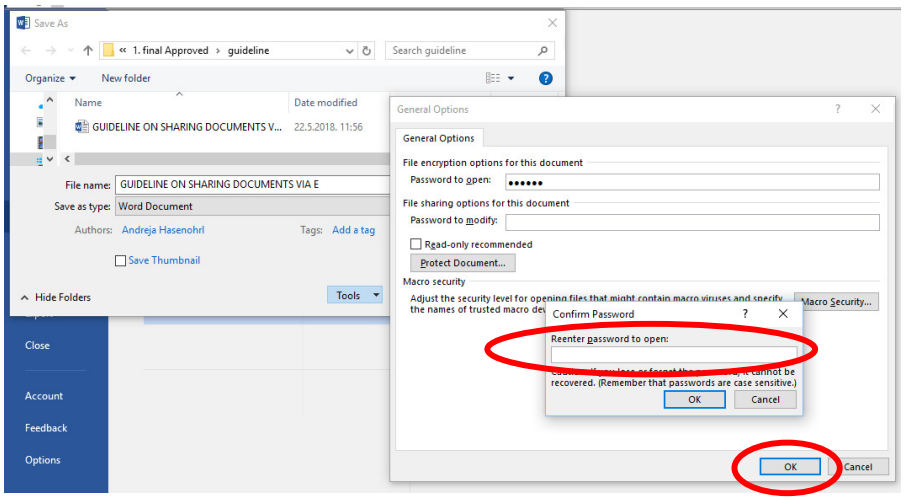
4. Unutar odabira **Tools** , označite **General Options**



5. Kada kliknete **General Options**, dodajte šifru pod „**Password to open**“ i kliknite **OK**



6. Kako biste potvrdili šifru, kliknite na “**Reenter password to open**“ i kliknite **OK**



7. Kliknite **Save**