SHARE FONDACIJA

BIRN BALKAN INVESTIGATIVE REPORTING NETWORK SERBIA

Politike i protokoli za medije

Zaštita podataka o ličnosti i digitalna bezbednost

April 2022.

Zaštita podataka o ličnosti

Instrukcije

Politika privatnosti je dokument koji je potrebno izraditi sa ciljem da se publici kojoj je namenjena daju informacije o tome zbog čega i na koji način rukovalac koristi i obrađuje podatke o ličnosti tih lica.

Dužnost obaveštavanja proizilazi iz zakonske obaveze rukovalaca da unapred pruže zakonom propisane informacije licima čiji se podaci prikupljaju. Kako bi tražene informacije bile unapred dostupne zainteresovanim licima, standardna praksa je da politika privatnosti bude javno objavljena na sajtu rukovaoca.

Donji tekst je primer obrasca kako rukovalac može opisati obrade podataka o ličnosti koje prikuplja putem svog sajta u okviru svoje politike privatnosti. Naslovi ovog primera prate obavezne informacije koje je rukovalac dužan da pruži prema pravilima iz GDPR i srpskog Zakona o zaštiti podataka o ličnosti.

U fusnotama se nalaze objašnjenja kako da se ovaj primer prilagodi za potrebe konkretnog rukovaoca. U tom smislu, potrebno je da se u okviru svake tačke (naslova) unesu informacije koje su relevantne za konkretnog rukovaoca, uključujući i informaciju o tome da se neke obrade ne vrše. Nakon finaliziranja teksta sa potrebnim informacijama fusnote treba izbrisati.

Ukoliko rukovalac ne prikuplja nikakve podatke o ličnosti, preporuka je sa svakako na sajtu objavi obaveštenje u kojem to i konstatuje.

Primeri konkretnih politika privatnosti koji su izrađeni u skladu sa ovim preporukama se nalaze ovde ili ovde.

Preuzmite templejt politike privatnosti kao Word dokument

Politika privatnosti

U daljem tekstu se možete informisati o tome u kojim situacijama, za koje svrhe i na koji način dole navedeni rukovalac obrađuje podatke o ličnosti, a uzimajući u obzir informacije koje su rukovaoci dužni da predoče prema članovima 13. i 14. EU Opšte Uredbe o zaštiti podataka o ličnosti (General Data Protection Regulation - „GDPR“) tj. članovima 23. i 24. srpskog Zakona o zaštiti podataka o ličnosti.

1) Identitet i kontakt podaci rukovaoca

<Naziv>
<Adresa>
<Grad, Država>

2) Kontakt podaci rukovaoca u vezi sa zaštitom podataka o ličnosti

<navesti kontakt podatke>

3) Svrha obrade, izvor podataka i pravni osnov za obradu[1]

Svrha[2]	*Vrsta*[3] *i izvor podataka*[4]	*Pravni osnov*[5]
<navesti svrhu obrade podatka>	<navesti načine prikupljanja i izvore podataka za ovu svrhu>	<navesti pravni osnov za obradu podatka za ovu svrhu>
<navesti svrhu obrade podatka>	<navesti načine prikupljanja i izvore podataka za ovu svrhu>	<navesti pravni osnov za obradu podatka za ovu svrhu>

ili

<u formi narativnog teksta navesti / opisati posebno svaku svrhu, informaciju o tome na koji način su prikupljeni podaci za ispunjenje te svrhe i po potrebi o kojim podacima se radi, kao i koji je pravni osnov za svaku posebnu svrhu>

1 Informacije u okviru ovog naslova mogu biti date tekstualno ili u obliku tabele. U finalnom dokumentu je potrebno obrisati tabelu, odnosno narativni tekst, u zavisnosti od toga o kojoj se od te dve forme daju informacije u okviru ovog naslova.

2 Svrha može biti na primer: davanje komentara na sajtu; popunjavanje kontakt forme na sajtu; učestvovanje u anketama; prijava na newsletter; registracija na sajt; doniranje rukovaocu, itd.

3 Vrste podataka mogu biti na primer: ime; email adresa; telefon; IP adresa; sadržaj komentara ili poruke; broj bankovnog računa, itd.

4 Podaci se mogu prikupljati direktno od lica koje ih daje rukovaocu – na primer tako što ih lice samo upisuje na sajtu, ili indirektno – na primer iz javno dostupnih izvora.

5 Pravni osnov za obradu može biti pristanak lica, legitimni interes rukovaoca, ugovor koji rukovalac ima sa licem ili ispunjenje zakonskih obaveza rukovaoca. Ukoliko niste sigurni, potrebno je da po pitanju odgovarajućeg pravnog osnova konsultujete pravnika.

4) Primaoci podataka o ličnosti[6]

Podatke o ličnosti rukovalac deli sa <navesti primaoce podataka tj. organizacije sa kojima se podaci dele>.

5) Iznošenje podataka o ličnosti u drugu državu[7]

Podaci o ličnosti se obrađuju u <navesti zemlje u kojima se podaci čuvaju / hostuju>.

6) Rok čuvanja podataka o ličnosti tj. kriterijumi za njegovo određivanje[8]

<navesti rok čuvanja podataka, tj. trenutak nakon kog se podaci brišu, pri čemu ukoliko ima više svrha, potrebno je navesti različite rokove za svaku od svrha obrade>.

7) Prava lica na koje se podaci odnose

Bilo koje lice na koje se podaci koje obrađujemo odnose ima pravo da zahteva od rukovaoca:

- da ga istinito i potpuno obavesti o obradi njegovih podataka;
- pravo na uvid i/ili kopiju podataka koji se na njega odnose;
- pravo na ispravku i dopunu pogrešnih ili nepotpunih podataka, u bilo koje vreme;
- pravo na brisanje, kome se može udovoljiti u skladu sa zakonskim uslovima, odnosno kada: podaci o ličnosti više nisu neophodni za ostvarivanje svrhe zbog koje su prikupljeni ili na drugi način obrađivani; lice na koje se podaci odnose je podnelo prigovor na obradu po osnovu legitimnog interesa rukovaoca, a nema drugog pravnog osnova za obradu; podaci o ličnosti su nezakonito obrađivani; podaci o ličnosti moraju biti izbrisani u cilju izvršenja zakonskih obaveza rukovaoca;
- pravo na ograničenje obrade, kome se može udovoljiti ukoliko su ispunjeni propisani uslovi: ako je lice na koje se podaci odnose osporilo tačnost podataka o ličnosti, a rukovaocu je potrebno vreme koje mu omogućava da proveri tačnosti; ako je obrada je nezakonita, a lice

6 Uneti primaoce podataka, sa kojima rukovalac deli podatke (radi razumevanja, preporuka je da se navede i razlog zbog kojih se podaci dele). To mogu biti poslovni saradnici, povezana privredna društva ili organizacije, kurirske službe, pravni i finansijski konsultanti, nadležni državni organi, itd. Ukoliko nema primalaca sa kojima se podaci o ličnosti dele, tako u okviru ovog naslova treba i napisati.

7 Uneti informacije o tome u kojim se sve zemljama obrađuju podaci. Po potrebi proveriti gde je vebsajt hostovan. Ukoliko se podaci obrađuju u zemljama koje se ne smatraju adekvatnim prema merodavnim propisima, navesti pravni osnov za prenos podataka u neadekvatne zemlje.

Na primer: Podaci o ličnosti se obrađuju u Srbiji i u Indiji. Prenos podataka u Indiju, koja se ne smatra zemljom koja obezbeđuje adekvatan nivo zaštite podataka, regulisan je i obezbeđen Standardnim ugovornim klauzulama.

8 Primeri za rok čuvanja mogu biti: podaci o ličnosti koje dajete prilikom ostavljanja komentara se čuvaju trajno tj. ne brišu se kao ni sami komentari; email koji ste dali u cilju slanja newletter-a se briše kada se odjavite; podaci koje dajete u kontakt formi na sajtu se čuvaju najviše godinu dana od slanja poruke.

se protivi brisanju i umesto brisanja zahteva ograničenje upotrebe podataka; rukovaocu više nisu potrebni podaci o ličnosti za ostvarivanje svrhe obrade, ali ih je lice zatražilo u cilju podnošenja, ostvarivanja ili odbrane pravnog zahteva; ili je lice već podnelo prigovor na obradu, a u toku je procenjivanje da li pravni osnov za obradu od strane rukovaoca preteže nad interesima lica;

- prenos podataka u mašinski čitljivoj formi, koje postoji u slučajima kada je to primenljivo, tj. ako je to tehnički moguće jer su podaci mašinski čitljivi i kada je pravni osnov za obradu pristanak lica ili ugovorni odnos sa licem na koje se podaci odnose.
- pravo da u bilo kom trenutku povuče svoj pristanak na obradu određenih podataka, ukoliko je pristanak pravni osnov za obradu.

Lice takođe ima pravo na prigovor, ukoliko lice na koje se podaci odnose smatra da legitimni interes rukovaoca na osnovu kog se podaci obrađuju nije opravdan, odnosno da ugrožava prava, slobode i interese tog lica.

U slučaju da se vrši automatizovana obrada podataka o ličnosti i donošenje odluka, lice ima pravo na ljudsku intervenciju, kao i pravo na izražavanje stava o odluci ili osporavanje odluke.

8) Pravo da se podnese pritužba Povereniku

Lice ima pravo da na postupanje rukovaoca podnese pritužbu nadležnom organu čiji su kontakt podaci dati u nastavku:

Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti
Bulevar kralja Aleksandra 15
Beograd 11120, Srbija
E-mail: office@poverenik.rs

9) Postojanje automatizovanog donošenja odluke, uključujući profilisanje[9]

Rukovalac ne vrši automatizovano donošenje odluka, niti profilisanje, na osnovu podataka o ličnosti.

9 Mediji najčešće ne vrše profilisanje (pravljenje jedinstvenih profila) i automatizovano donošenje odluka o pravima i interesima posetilaca svojih sajtova (donošenje odluka bez ljudske intervencije, već samo putem „algoritama“). Ukoliko rukovalac to ipak radi, ovde je potrebno jasno i razumljivo objasniti svrhe i načine na koje se takva obrada vrši.

10) Politika kolačića[10]

<U ovom naslovu je dat samo primer kako rukovalac može opisati korišćenje kolačića na svom sajtu. Ukoliko želite da koristite donji tekst, potrebno ga je prilagati konkretnom sajtu>.

"Kolačić" je mali podatak koji veb stranica može poslati vašem pretraživaču, a koji se onda može čuvati na tvrdom disku. Ako ste zabrinuti zbog vaše privatnosti i korišćenja tehnologije "kolačići", možete podesiti pregledač da vas obavesti kada primite "kolačić". Kolačići vam mogu pomoći da budete efikasniji i da imate koristi od funkcija «memorije», na primer kada sajt pamti vaš jezik na kome se pregledali naš sajt iz prethodne posete. Kolačići vam omogućavaju da sačuvate svoje preferencije, da sačuvate proizvode i usluge i da prilagodite stranice.

Rukovalac koristi kolačiće na svom sajtu u cilju pružanja usluga i funkcionalnosti svojim korisnicima. Možete ograničiti ili onemogućiti upotrebu kolačića preko svog internet pretraživača, ali bez kolačića nećete moći da koristite sve funkcionalnosti sajta.

Postoje različite vrste kolačića, a prema kriterijumu ko postavlja kolačiće na sajt razlikujemo:

- kolačiće prve strane (first party cookies) – kolačići koje postavlja rukovalac kada koristite naš sajt, i
- kolačići trećih strana (third party cookies) – kolačići koje postavlja neka druga organizacija kada koristite naš sajt (neke veb stranice na našem sajtu mogu takođe sadržati sadržaje sa drugih sajtova koji mogu postaviti sopstvene kolačiće).

Što se tiče namene, koristimo sledeće vrste kolačića na sajtu:

- Strogo neophodni kolačići – ovi kolačići koji su neophodni za upravljanje statusom vaše veze.
- Funkcionalni kolačići - ovi kolačići omogućavaju internet sajtu da zapamti vaše prethodne radnje kako bi vam pružio napredne

10 Ukoliko koristite kolačiće koji mogu da dovedu do direktne ili posredne identifikacije određenih korisnika vašeg sajta (putem bilo kog jedinstvenog identifikatora), korišćenje takvih kolačića se takođe smatra obradom podataka o ličnosti. U tom slučaju, potrebno je prvo da odredite da li postoje neki kolačići za koje imate legitimni interes da ih koristite (poput strogo neophodnih kolačića), što je u to slučaju pravni osnov za obradu podataka.

Sve ostale kolačiće je moguće koristiti samo na osnovu pristanka posetioca sajta.

Stoga je tada potrebno i preporučljivo da omogućite pop-up opciju u kojoj bi posetioci sajta imali mogućnost da odbiju sve kolačiće koji se ne mogu pravdati legitimnim interesom, poput analitičkih, marketinških i kolačića trećih strana.

Nisu u skladu sa GDPR standardima prakse u kojima se posetilac sajta samo obaveštava da korišćenjem sajta prihvata sve kolačiće, bez obzira na njihovu vrstu i namenu.

funkcionalnosti.

- Analitički kolačići - ovi kolačići nam omogućavaju da prikupljamo podatke o vašem korišćenju internet stranice u cilju poboljšanja njenog učinka i dizajna. Da biste onemogućili kolačiće Google analitike, preuzmite i instalirajte ovaj dodatak.
- Marketinški kolačići - ovi kolačići koji se koriste za prikupljanje različitih informacija o vašoj poseti našem sajtu, kao što su informacije o sadržaju koji ste pregledali, vezama koje ste pratili, vašem pretraživaču, uređaju ili IP adresi.

Digitalna bezbednost

Interne bezbednosne politike

Digitalna bezbednost je od ključnog značaja za medijske organizacije i ljude koji ih čine, odnosno novinare i druge zaposlene, kao i izvore sa kojima novinari dolaze u kontakt prilikom istraživanja. Kako bi korišćenje tehnologije tokom obavljanja njihovog posla bilo što bezbednije, mediji bi trebalo da usvoje odgovarajuće politike i procedure koje će im u tome pomoći. U slučaju tehničkih incidenata, kao što su recimo napad na sajt medija ili preuzimanje naloga, ove politike mogu biti od pomoći da se šteta po resurse organizacije spreči ili makar svede na minimum.

U zavisnosti od kapaciteta i resursa organizacije, u kreiranju internih bezbednosnih politika se podrazumeva učešće menadžmenta, uredništva, članova tima zaduženih za IT, kao i novinara i drugih zaposlenih koji poseduju naprednije tehničke veštine koje mogu preneti drugima. Obuka i edukacija zaposlenih su značajne kako bi se procedure i politike primenjivale a da se pritom redovni procesi rada ne remete.

Svaki interni dokument u oblasti digitalne bezbednosti treba prilagoditi realnim potrebama i mogućnostima organizacije, na način da bude preobiman, već precizan i napisan razumljivim jezikom. Interne politike moraju biti dostupne u elektronskoj formi samo članovima tima, dakle ne javno. U te svrhe se mogu koristiti recimo platforme za internu komunikaciju (npr. Mattermost, Rocket.Chat, Element) kako bi zaposleni u slučaju nedoumica ili rada van prostorija organizacije imali pristup dokumentaciji i mogli da se konsultuju sa kolegama ili osobama koje su nadležne za nadzor primene politika (npr. urednici).

Primeri internih dokumenata su **politika lozinki, politika korišćenja službenih mejl i pratećih naloga**, kao i **bezbednosni plan**.

Politika lozinki

Instrukcije

Cilj ovog dokumenta je da pomogne organizacijama da kreiraju jedinstvenu politiku za korišćenje i upravljanje lozinkama, kako bi se obezbedili predvidljivost i jasne procedure. Politika lozinki omogućava organizaciji i njenim članovima bezbedno kreiranje, korišćenje, skladištenje i modifikaciju lozinki, koje predstavljaju osnovni mehanizam autentifikacije, odnosno zaštite organizacionih resursa od neovlašćenog pristupa.

Preuzmite templejt politike lozinki kao Word dokument

_____ (Naziv organizacije)

Politika lozinki

1. Ova politika se primenjuje na lozinke (passwords) u upotrebi za zaštitu naloga, uređaja, dokumenata, baza podataka i drugih resursa kojima upravlja _____ (Naziv organizacije).
2. Jedna lozinka se ne sme koristiti za zaštitu više različitih resursa. Lozinke se ne smeju javno prikazivati i deliti sa neautorizovanim osobama.
3. Ukoliko postoji tehnička mogućnost, neophodno je uvesti dvostruku verifikaciju prijave (2-step verification) na svaki resurs kojim upravlja _____ (Naziv organizacije).
4. Promena svih lozinki za resurse kojima upravlja _____ (Naziv organizacije) vrši se na period od _____ meseci.
5. Lozinke moraju biti duge najmanje 15 karaktera, moraju sadržati posebne karaktere (npr. znaci interpunkcije), velika slova, mala slova i cifre. Lozinke ne smeju sadržati podatke o ličnosti zaposlenih (npr. imena, prezimena, datume rođenja, brojeve telefona, adrese stanovanja) niti njima bliskih lica (npr. članova uže porodice).
6. Za naročito osetljive resurse (npr. baze koje sadrže podatke naročito osetljive prirode: žrtve nasilja, zdravstveno stanje, seksualno opredeljenje itd) neophodno je uvesti zaštitne fraze (passphrases) koje čine nizovi nasumično odabranih reči u kombinaciji sa drugim obaveznim elementima za lozinke iz tačke 5. ove politike. Zaštitne fraze moraju da budu dužine najmanje 20 karaktera.
7. Lice u organizaciji zaduženo za administriranje lozinkama je _____ (ime i prezime, radno mesto).
8. Po dodeli lozinke za naloge koji se koriste za poslove i aktivnosti _____ (Naziv organizacije), kao što su recimo službeni mejl nalozi, zaposleni su dužni da datu lozinku promene u skladu sa ovom politikom odmah pošto je dobiju od nadležnog lica koje je kreiralo nalog (npr. tehnički administrator) i dodelilo ga zaposlenom. Nove lozinke moraju biti generisane i skladištene u menadžeru lozinki.
9. Lozinke i zaštitne fraze se čuvaju u posebnim aplikacijama namenjenim isključivo za upravljanje lozinkama (npr. KeePass, KeePassXC) koje čuvaju bazu lozinki na lokalnoj memoriji uređaja. Čuvanje lozinki u internet pregledačima (internet

browsers) i na sajtovima za onlajn čuvanje lozinki nije dozvoljeno.

10. Pravljenje rezervne kopije baze lozinki koja se čuva na eksternoj memoriji (npr. eksterni hard disk, USB fleš memorija) se vrši prilikom svake izmene lozinki i zaštitnih fraza (dodavanje novih ili menjanje starih) i obavezno se u nazivu fajla označava datum kada je napravljena.
11. U slučaju da zaposleni primeti ili posumnja da je bilo koji resurs kojim upravlja _____ (Naziv organizacije) kompromitovan, odmah će o tome obavestiti nadređenog i promeniti lozinku ili zaštitnu frazu za taj resurs, a ukoliko je reč o resursu koji se zajednički koristi obavestiće lice u organizaciji zaduženo za administriranje lozinkama.
12. Ova politika stupa na snagu ____ dana od dana donošenja.

Datum:_____ Ovlašćeno lice organizacije:_____

Mesto:_____

Politika korišćenja email i pratećih naloga

Instrukcije

Pomoću ovog dokumenta organizacije mogu da kreiraju jedinstvenu politiku za korišćenje i upravljanje službenim mejl nalozima i sa njima povezanim nalozima (tj. kompletnih paketa usluga za produktivnost koje nude provajderi kao što su Google ili Microsoft) kako bi bilo jasno u koje svrhe mogu da se koriste, kome se dodeljuju, kako se postupa prilikom odlaska članova tima iz organizacije i tome slično. Politika naloga omogućava organizacijama i njenim članovima da nalozima u vlasništvu organizacije upravljaju na načine koji smanjuju moguće rizike u pogledu digitalne bezbednosti i koriste ih u skladu sa propisanim svrhama.

Preuzmite templejt politike korišćenja email i pratećih naloga kao Word dokument

Naziv i adresa organizacije

Politika korišćenja email i pratećih naloga _____ (naziv organizacije)

U ovoj politici su sadržani uslovi korišćenja email i pratećih naloga na internet domenima u vlasništvu _____, i to: _____ (upisati domene, npr. organizacija.rs) (u daljem tekstu: domeni _____).

1. Email i prateći nalozi kreirani za potrebe rada, obavljanja prakse i volontiranja u _____ su u vlasništvu _____.
2. _____ upravlja nalozima i izdaje ih na korišćenje licima koja su u radnom odnosu u _____, licima koja su na praksi i licima koja volontiraju.
3. Lice kome je izdat email nalog koristi nalog i _____ nema uvid u sadržaj tog naloga niti u njegove prateće delove (cloud storage, kolaborativni dokumenti i sl).
4. Nalozi na domenima _____ se koriste isključivo u svrhe koje odredi _____.
5. U slučaju prestanka odnosa između _____ i lica kome je izdat nalog, vlasništvo naloga ostaje kod _____.
6. _____ će ostaviti rok od 30 dana od dana prestanka odnosa da lice kome je izdat nalog prikupi iz naloga sav sadržaj koji smatra da će mu biti potreban.
7. Posle isteka roka od 30 dana od prestanka odnosa nalog će biti izbrisan, a kopija sadržaja arhivirana za potrebe _____.
8. Politika stupa na snagu danom donošenja.
9. Lica kojima su dodeljeni nalozi će biti obaveštena o svakoj budućoj izmeni ove politike.

Mesto i datum,

Odgovorno lice

_____

Bezbednosni plan

Instrukcije

Bezbednosni plan ima za cilj da pomogne organizacijama da kreiraju preventivne i reaktivne mere u pogledu tehničkih incidenata, razmotre moguće rizike i pretnje po tehničku infrastrukturu organizacije, propišu procedure i korake u slučaju suočavanja sa različitim vrstama tehničkih incidenata, itd. Iako nije moguće predvideti scenario svakog pojedinačnog tehničkog napada, posedovanje bezbednosnog plana može sprečiti ili umanjiti štetu i pomoći da se izvrši sanacija.

Prilikom izrade bezbednosnog plana, obratite pažnju na sledeće:

Ciljevi: postavite realističan primarni cilj ili više sekundarnih ciljeva, kako bi propisane mere zaista bile primenjene zarad postizanja datih ciljeva.

Pretnje i rizici: razmislite o mogućim scenarijima ugrožavanja digitalne bezbednosti vaše organizacije i njenih članova, to će vam pomoći da preciznije identifikujete moguće pretnje i rizike po digitalnu bezbednost i bolje se pripremite za suočavanje sa njima.

Preventivni koraci: navedite realistične korake koje možete da preduzmete u vezi sa zaštitom digitalne bezbednosti, uzimajući u obzir pretnje, rizike i kapacitete same organizacije (tehničke, organizacione i kadrovske).

Koraci u slučaju incidenta: razmotrite moguće scenarije incidenta (npr. neovlašćeno preuzimanje naloga na društvenim mrežama) i definišite neophodne korake u datim situacijama. Iako nije realistično predvideti sve scenarije, odaberite nekoliko za koje smatrate da su najrealističniji da se ostvare ili koji su se već dogodili vašoj organizaciji.

Preporučeni uređaji i oprema: napravite listu hardverskih i softverskih rešenja koja imaju dobru reputaciju i recenzije i preporučena su od strane ekspertske zajednice. Imajte na umu kapacitete organizacije, a ukoliko niste sigurni šta bi vašim potrebama najviše odgovaralo, potražite eksterni savet.

Primena internih procedura: opišite konkretno primenu vaših bezbednosnih procedura na više primera incidenata za koje smatrate da su najrealističniji da se ostvare ili sa kojima ste ranije imali iskustva u organizaciji.

Preuzmite templejt bezbednosnog plana kao Word dokument

Bezbednosni plan

CILJ	**Unaprediti digitalnu bezbednost organizacije kao celine i njenih pojedinačnih članova**
PRETNJE I RIZICI	• Kompromitacija podataka o ličnosti i poverljivih informacija (dokumenti, prepiske...) • Kompromitacija tehničke infrastrukture i resursa organizacije • Gubitak kontrole nad infrastrukturom i podacima kao rezultat
PREVENTIVNI KORACI	• Pristup infrastrukturi i resursima organizacije (serveri, mrežna oprema, nalozi na društvenim mrežama, admin paneli sajtova...) omogućen samo određenim licima i zaštićen jakim lozinkama koje se čuvaju u posebnim aplikacijama za tu namenu (password managers, npr. KeePass) • Usvojena politika lozinki organizacije • Dvostruka autentifikacija (2-step authentication) uključena na svim korisničkim nalozima koji je podržavaju. • Naročito osetljive podatke (npr. informacije o žrtvama seksualnog nasilja) čuvati enkriptovane, na posebnim uređajima koji se ne koriste za svakodnevni rad. • Uređaji zaposlenih zaštićeni lozinkama/pin kodovima • Redovno pravljenje rezervnih kopija podataka (backup) na lokalnim uređajima (npr. eksterni hard diskovi) i/ili onlajn (na serveru organizacije ili na cloud uslugama, npr. Dropbox, Google Drive, OneDrive...). **Međutim, naročito osetljive podatke o ličnosti i druge poverljive informacije ne treba čuvati na cloud servisima**. • Za razmenu poverljivih informacija koristiti enkriptovane mejlove (PGP) i čet aplikacije (Signal).

KORACI U SLUČAJU INCIDENTA	• Što pre obavestiti nadležne kolege (administratore zadužene za tehničku infrastrukturu u organizaciji) i tehničku podršku (npr. hosting kompaniju) i pratiti njihove instrukcije • Prikupiti sve dostupne informacije o incidentu (vreme, mesto, aktivnosti u toku incidenta, IP adrese, logovi, skrinšotovi, poslednje ispravne konfiguracije...) kako bi se utvrdila šteta i posledice • Obavestiti posebne/sektorske timove za reakciju u slučajevima sajber incidenata: **SHARE CERT**, čiji je osnivač SHARE Fondacije, prvi je poseban centar za zaštitu informacionih sistema onlajn i građanskih medija i prevenciju od rizika u sajber okruženju: Adresa: Kapetan Mišina 6a, kancelarija 31, Beograd Email: info@sharecert.rs, emergency@sharecert.rs Sajt: sharecert.rs Telefon: 064 089 7067 • Prijaviti incident nadležnim državnim organima: **MUP Republike Srbije, Odeljenje za borbu protiv visokotehnološkog kriminala** (pri Službi za borbu protiv organizovanog kriminala Uprave kriminalističke policije): Adresa: Bulevar Mihaila Pupina 2, Beograd Email: ukp@mup.gov.rs Sajt: mup.gov.rs **Posebno tužilaštvo za borbu protiv visoko-tehnološkog kriminala:** Adresa: Savska 17a, Beograd Email: vtk@beograd.vtk.jt.rs Sajt: beograd.vtk.jt.rs **Ako su kompromitovani podaci o ličnosti, neophodno je obavestiti Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti:**

	Adresa: Bulevar kralja Aleksandra 15, Beograd Email: office@poverenik.rs Sajt: poverenik.rs Telefon: 011 3408 900 • Proveriti poslednju dostupnu verziju podataka/konfiguracije sistema radi pokušaja vraćanja u pređašnje stanje i rekonstrukcije napada
PREPORUČENI UREĐAJI I OPREMA	• Mobilni telefoni sa instaliranim enkriptovanim čet aplikacijama (Signal) • Računari: instaliran i redovno ažurirani anti-virus softver, kao i svi ostali softveri koji se koriste • Računari: instaliran menadžer lozinki (npr. KeePass, KeePassXC) • Računari: instaliran softver za enkripciju hard diska (VeraCrypt) • Kreirani PGP ključevi za mejlove zaposlenih i instaliran odgovarajući softver (npr. Thunderbird, Gpg4Win, Mailvelope) • Browsers: Mozilla Firefox, instalirani dodaci (HTTPS Everywhere, Privacy Badger, uBlock Origin, minerBlock, Facebook Container) ili Brave na kome se mogu instalirati verzije dodataka za Google Chrome • Na uređajima instaliran pouzdan VPN (npr. Mullvad, ProtonVPN) i Tor Browser

PRIMENA INTERNIH PROCEDURA (PRIMER)	Među zaposlenima je primećeno je da je sajt organizacije nedostupan ili da se stranica teško učitava 1. Proveriti dostupnost stranice na servisu "Down For Everyone Or Just Me" (https://downforeveryoneorjustme.com/) i internet konekciju 2. Izvršiti skeniranje svih računara i uređaja anti-virus softverom 3. Ukoliko se utvrdi da nije reč o tehničkom problemu, zaposleni obaveštava tehničkog administratora organizacije lično ili putem sigurnog kanala komunikacije (Signal čet, enkriptovana mejl poruka) 4. Administrator, u saradnji sa tehničkom podrškom, izvršava proveru infrastrukture i ukoliko se utvrdi da je došlo do neuobičajenog saobraćaja, neovlašćenog pristupa ili druge povrede integriteta informacionog sistema, vrši prikupljanje digitalnih dokaza 5. Sledi pokušaj povraćaja podataka/povraćaj funkcionalnosti pomoću rezervnih kopija i/ili poslednjih dobrih konfiguracija 6. Sledi utvrđivanje vrste napada i pravne kvalifikacije, obaveštavanje nadležnih organa i pripremanje podnesaka (npr. krivične prijave) u saradnji sa posebnim/sektorskim timovima (npr. SHARE CERT)

April 2022.