

VODIČ ZA POSTUPANJE U SLUČAJU INCIDENATA SA TAJNIM PODACIMA



web: www.nsa.gov.rs

Prof.dr Goran D. Matić

Beograd, 2025. godina

Podizanje bezbednosne svesti i kulture sa primarnim i težišnim zadatkom zaštite interesa Republike Srbije koji se odnose na nacionalnu i javnu bezbednost, unutrašnje i spoljne poslove Republike Srbije, odbranu, zaštitu ustavnog poretka, kao i ljudskih i manjinskih prava!

SADRŽAJ

UVODNA RAZMATRANJA	3
1. Bezbednosni incident u radu sa tajnim podacima	5
2. Ko ima obavezu obaveštavanja o incidentu u radu sa tajnim podacima?	7
3. Klasifikacija incidenata u sistemu zaštite tajnih podataka.....	8
4. Procena okolnosti nastanka incidenta u radu sa tajnim i njegova pravna kvalifikacija.....	10
5. Postupanje u slučaju incidenta sa tajnim podacima.....	12
6. Preporučene mere — postupanje po preporuci Kancelarije SNBiZTP.....	14
7. Doprinos organizacije nastanku štetnog događaja u radu sa tajnim podacima	16
8. LISTA ZA PROVERU U SLUČAJU INCIDENTA SA TAJNIM PODACIMA.....	23
9. PREPORUČENE MERE – USKLAĐENE SA EU PRAKSOM.....	25
10. Zaključna razmatranja.....	26

UVODNA RAZMATRANJA

Vodič za postupanje u slučaju incidenta sa tajnim podacima predstavlja ključni instrument za adekvatno upravljanje situacijama koje ugrožavaju bezbednost i integritet zaštićenih podataka u okviru organa javne vlasti i pravnih lica. Ovaj vodič je zasnovan na odredbama **Zakona o tajnosti podataka** i **Zakona o informacionoj bezbednosti**, kao i na najboljim praksama iz oblasti zaštite informacija i tajnih podataka, sa ciljem da pruži jasne smernice za otkrivanje, upravljanje i izveštavanje o incidentima koji uključuju tajne podatke. Osnovna svrha ovog vodiča je da omogući svim relevantnim učesnicima u procesu upravljanja incidentima brzo, precizno i pravovremeno reagovanje u slučaju da dođe do narušavanja bezbednosti tajnih podataka. Vodič definiše konkretne korake koji treba da se preduzmu u svakom od etapa: od ranog otkrivanja incidenta i obaveštavanja nadležnih organa, do postupanja sa ugroženim tajnim podacima i izveštavanja o posledicama.

Zakon o tajnosti podataka postavlja osnovne principe koji regulišu način određivanja i označavanja tajnosti podataka, njihovu zaštitu i postupanje u slučaju njihovog ugrožavanja i neovlašćenog korišćenja. **Zakon o informacionoj bezbednosti**, s druge strane, definiše tehničke i organizacione mere koje treba da budu primenjene u cilju zaštite informacionih sistema i tajnih podataka od neovlašćenog pristupa, uništenja ili zloupotrebe. U skladu sa ovim propisima, vodič obuhvata sve ključne aspekte procesa upravljanja incidentima i obezbeđuje usaglašenost sa zakonskim zahtevima i međunarodnim standardima bezbednosti informacija i tajnih podataka. Postupanje prema ovim smernicama omogućiće organizacijama da ubrzano identifikuju i spreče dalju štetu u slučaju incidenta, kao i da osiguraju poštovanje prava lica čiji su podaci ugroženi, u skladu sa propisima o tajnim podacima, ali i drugim propisima. Osim toga, ovaj vodič služi kao osnova za stalno unapređenje procesa zaštite tajnih podataka i povećanje svesti zaposlenih o važnosti bezbednosti informacija i tajnih podataka.

U ovom kontekstu, vodič nije samo pravni ili tehnički dokument, već i alat koji pomaže organizacijama da razviju bezbednosnu kulturu i svest i daju konkretne smernice za svakog pojedinca koji je odgovoran za bezbednost tajnih podataka. Razmatranje trenutnih mera bezbednosti, identifikovanje slabih tačaka i usmeravanje pažnje na postojeće mehanizme zaštite. Ovaj korak je ključan u kontekstu reagovanja na incidente, jer dozvolava organizacijama da procene svoje trenutne kapacitete i operativnu spremnost za brzu i efikasnu reakciju. Procena takođe podrazumeva reviziju postojećih normativa i procedura u skladu sa zakonom i najboljim bezbednosnim praksama.

Opis preventivnih mera koje organizacije treba da preduzmu kako bi minimizirale rizik od incidenata sa tajnim podacima. Ove mere obuhvataju uvođenje jasno definisanih procedura i pravila za upravljanje tajnim podacima, kao i redovne bezbednosne provere

i revizije. Takođe, važno je osigurati da su svi zaposleni svesni važnosti zaštite tajnih podataka.

Naglasak na važnosti obuke i treninga u kontekstu bezbednosti tajnih podataka i odgovornosti svih zaposlenih u organizaciji. Stalna edukacija zaposlenih o procedurama postupanja u slučaju incidenta, kao i upoznavanje sa novim pretnjama i tehničkim merama bezbednosti, ključni su za prevenciju i brzu reakciju. Sveobuhvatna obuka takođe pomaže u stvaranju bezbednosne kulture i svesti i poštovanju propisa.

Razmatranje novih tipova incidenata, kao što su sajber napadi i neovlašćeni pristup, te kako se oni mogu prepoznati. Ovde je ključno i usmeravanje sistema zaštite na prepoznavanje potencijalnih pretnji u ranim fazama. Takođe, ovaj segment obuhvata usvajanje tehnika i tehnologija za brzo otkrivanje incidenata koji mogu ugroziti tajne podatke. Opis uloge kontrole i nadzora u osiguranju primene svih bezbednosnih mera, kao i procesa revizije. Odgovornosti su jasno definisane na svim nivoima organizacije, od menadžmenta do operativaca, kako bi se osigurala pravovremena i adekvatna reakcija na incidente. Kontrole uključuju i redovne interne i eksterne revizije sistema bezbednosti i skladu sa propisima.

Procedura za postupanje u slučaju incidenta, koja uključuje pravovremenu komunikaciju sa javnosti i medijima, ali i sa nadležnim organima. Komunikacija mora biti precizna i u skladu sa zakonskim zahtevima, kako bi se smanjila šteta i očuvala reputacija organizacije. Ovaj segment takođe obuhvata aktivnosti koje se preduzimaju kako bi se osigurala tajnost podataka i pravovremenost u izveštavanju.

Postupanje prema smernicama iz ovog vodiča, kao i usaglašavanje sa propisima o tajnosti podataka i standardima nacionalne bezbednosti, omogućiće organima javne vlasti i pravnim licima da adekvatno upravljaju incidentima i spreče potencijalne štete. Stalna edukacija, nadzor i usavršavanje sistema zaštite tajnih podataka igraju ključnu ulogu u minimizaciji rizika i održavanju visokih standarda njihove zaštite.

1. Bezbednosni incident u radu sa tajnim podacima

Bezbednosni incident je svaki događaj, radnja ili propust koji je doveo ili može dovesti do neovlašćenog pristupa, otkrivanja, izmene, uništenja ili gubitka tajnih podataka. Takođe, incidentom se smatra i svako odstupanje od propisanih mera zaštite podataka, utvrđenih zakonom, podzakonskim aktima, bezbednosnim politikama i internim procedurama. U slučaju postojanja **sumnje ili saznanja** o sledećim događajima u vezi sa tajnim podacima ili stranim tajnim podacima:

- **gubitak** (npr. fizičko odsustvo dokumenta ili uređaja sa podacima),
- **krađa** (npr. neovlašćeno preuzimanje od strane trećeg lica),
- **oštećenje** (npr. fizičko ili logičko oštećenje nosača podataka),
- **uništenje** (bez sprovođenja propisane procedure za uništavanje),
- **neovlašćeno otkrivanje** (npr. pristup ili uvid lica bez odgovarajućeg stepena ovlašćenja),

svako lice (zaposleni, saradnik, angažovano lice), koje dođe do takvog saznanja, **dužno je da bez odlaganja** obavesti starešinu organa javne vlasti, rukovaoca tajnih podataka ili **ovlašćeno lice za zaštitu tajnih podataka u okviru svog organa**.

Ova obaveza proizilazi iz principa **odgovornosti (accountability)** i **obaveze prijavljivanja bezbednosnog incidenta**, u skladu sa članom 35. i 36. Zakona o tajnosti podataka.

Karakteristike bezbednosnog incidenta:

- Može biti **namernog** (zlomamerne radnje) ili **nenamernog** karaktera (nehat, nemar).
- Uvek predstavlja **odstupanje od propisanih pravila** zaštite tajnih podataka.
- Može imati **pravne posledice** kao prekršaj ili krivično delo, u zavisnosti od težine i posledica.

Primeri bezbednosnih incidenata:

- Uvid neovlašćenih lica u dokumente sa tajnim podacima.
- Razgovor o tajnim podacima u neobezbeđenom prostoru ili preko nesigurne komunikacije.
- Gubitak ili krađa uređaja (npr. USB, laptop) sa tajnim sadržajem.
- Slanje tajnih podataka bez kriptografske zaštite.
- Neovlašćeno kopiranje, umnožavanje ili uništavanje tajnog podatka.

Kompromitacija štićenih podataka u najširem smislu (tajnih podataka, ličnih podataka, bankarske tajne, poreske tajne, poslovne i profesionalne tajne) nastaje kada dođe do neovlašćenog otkrivanja, pristupa, izmene, uništenja ili gubitka podataka, čime se ugrožava njihova poverljivost, integritet ili dostupnost. Takvi događaji mogu prouzrokovati ozbiljnu štetu po organ javne vlasti, pravno lice, organizaciju ili pojedinca.

Oblici kompromitacije

-  Otključan i nadgledan sef sa poverljivim podacima
-  Uvid u podatke od strane neovlašćenih lica
-  Nebezbedan prenos poverljivih informacija
-  Iznošenje van zaštićenog prostora
-  Uništavanje bez propisane procedure

Uobičajeni uzroci kompromitacije:

- Ljudska greška, nepažnja ili nemar.
- Nedovoljna stručnost i obuka.
- Gubitak nosača podataka.
- Sajber napadi, špijunaža, haktivizam.
- Zloupotreba pristupa ili baza podataka.

Kompromitacija podataka (Data Breach): Incident u kom štićeni ili osetljivi podaci postaju dostupni, kopirani, ukradeni ili iskorišćeni od strane neovlašćenih lica.

Najčešće ugroženi štićeni podaci, pored tajnih podataka:

- Identifikacioni i lični podaci
- Finansijske informacije
- Medicinska dokumentacija
- Poslovne tajne i intelektualna svojina

Ključni uzroci:

1. Propusti u ponašanju i obuci osoblja
2. Zlonamerni softver (npr. ransomver)
3. Nedostatak fizičke i druge zaštite
4. Nepoštovanje bezbednosnih procedura

Kompromitacija tajnih podataka – konkretni rizici:

1. Nenamerni incidenti:

- Greške u kontroli pristupa
- Prekoračenje principa need to know
- Tehnički propusti u konfiguraciji sistema

2. Namerne zloupotrebe:

- Špijunaža, diverzije, korupcija
- Sajber napadi, krađa identiteta
- Haktivizam i ideološki motivisane akcije

3. Tehničke nepravilnosti:

- Nema u rukovanju opremom ili podacima
- Gubitak ili krađa uređaja sa osetljivim sadržajem

2. Ko ima obavezu obaveštavanja o incidentu u radu sa tajnim podacima?

U skladu sa članom 35. stav 3. Zakona o tajnosti podataka i važećim internim aktima, **obavezu obaveštavanja u slučaju incidenta ima svako lice koje je na bilo koji način došlo u kontakt sa tajnim podacima**, odnosno koje je uočilo ili prouzrokovalo povredu mera njihove zaštite.

Obavezu obaveštavanja imaju:

- ✓ **Sva zaposlena lica, angažovana lica i funkcioneri** u organu javne vlasti koji rukuje tajnim podacima;
- ✓ **Lica koja su vršila prenos, obradu ili čuvanje tajnih podataka**, uključujući i slučajeve kada se podatak nalazio van službenih prostorija ili informacionog sistema organa;
- ✓ **Lice zaduženo za fizičko, logičko ili organizaciono obezbeđenje tajnih podataka**, ako je uočilo povredu mera;
- ✓ **Rukovalac tajnih podataka ili ovlašćeno lice za zaštitu tajnih podataka u pravnom licu**, ukoliko mu je incident prijavljen ili ga je samo otkrilo.

Posebno:

- Ukoliko je tajni podatak **prenošen van prostorija organa**, lice koje ga je prenosilo ima **obavezu da odmah obavesti ovlašćeno lice ili starešinu organa**, kao i organ javne vlasti od kojeg je podatak potekao (izvorni organ), bez obzira na stepen štete ili prividnu beznačajnost incidenta.

Napomena: Ova obaveza obaveštavanja je **neodložna i neposredna**. Odlaganje ili prikrivanje incidenta može se smatrati težom povredom radne obaveze, a u određenim slučajevima i osnovom za pokretanje prekršajnog ili krivičnog postupka.

Principi odgovornosti: - Odgovornost za postupanje je raspoređena na svim nivoima upravljanja, uz obavezno poštovanje sledećih principa:

- **Need to know** („*potreba za znanjem*“) – pristup tajnim podacima dozvoljen je isključivo licima kojima su ti podaci neophodni za obavljanje konkretnih poslova, odnosno zadataka u okviru ovlašćenih nadležnosti.

Accountability („*odgovornost i praćenje postupanja*“) – svako lice koje rukuje tajnim podacima mora biti u potpunosti odgovorno za svoje postupke u vezi sa tim podacima, a organ je u obavezi da obezbedi sistem nadzora, praćenja i evidentiranja aktivnosti.

3. Klasifikacija incidenata u sistemu zaštite tajnih podataka

Saglasno odredbama Zakona o tajnosti podataka („Sl. glasnik RS“, br. 72/2009), incidenti u sistemu zaštite tajnih podataka klasifikuju se prema stepenu rizika po zaštićene interese i vrsti povrede zakona:

1. Povreda radne discipline (Disciplinska odgovornost): Incident koji **ne dovodi do kompromitacije tajnih podataka**, ali predstavlja **nezakonito ili nesavesno postupanje u vršenju službene dužnosti**, kao što su:

- nepoštovanje propisanih procedura za rukovanje tajnim podacima,
- nemar u primeni mera fizičke, tehničke ili organizacione zaštite,
- neprijavlivanje gubitka dokumenta ili uređaja sa tajnim podacima,
- pristup tajnim podacima bez potrebe zasnovane na službenoj funkciji („*potreba da se zna*“).

→ Pravni osnov:

- **Zakon o državnim službenicima**, čl. 107–109: teže povrede službene dužnosti.
- **Zakon o radu**, čl. 179: razlozi za otkaz ugovora o radu.

- **Zakon o Vojski Srbije**, čl. 145-170.: disciplinski greške i prestupi profesionalnih pripadnika Vojske Srbije.
- **PZakon o policiji**, čl. 202–217: lake i teške povrede službene dužnosti.

→ **Sankcije**: disciplinski postupak, mera upozorenja, smanjenje plate, premeštaj, razrešenje ili otkaz.

2. Prekršaj (Prekršajna odgovornost): Incident koji **nije doveo do kompromitacije tajnih podataka**, ali ukazuje na **propuste u primeni propisanih mera zaštite**, kao što su:

- nepravilno označavanje stepena tajnosti podataka (član 11, stav 2),
- izostanak obrazloženja o određivanju tajnosti (član 11, stav 4),
- nepreduzimanje propisanih mera zaštite od strane rukovaoca tajnih podataka (član 34),
- odsustvo unutrašnje kontrole i procene rizika (članovi 22, 84),
- dostavljanje podataka neovlašćenim subjektima bez kompromitacije samog sadržaja (član 46).

→ **Prekršajna odgovornost** snosi se u skladu sa članovima **99. i 100. Zakona**, i novčana kazna iznosi **od 5.000 do 50.000 dinara**.

3. Krivično delo (Krivična odgovornost): Incident koji je **doveo ili mogao dovesti do kompromitacije tajnih podataka**, uključujući:

- neovlašćeno saopštavanje, predaja ili omogućavanje pristupa tajnim podacima,
- gubitak, uništenje ili otkrivanje dokumenata koji sadrže tajne podatke,
- pribavljanje tajnih podataka bez odobrenja.

→ U skladu sa članom **98. Zakona**, krivično delo se kvalifikuje prema oznaci tajnosti podataka:

- Za „INTERNO“ ili „POVERLjIVO“ → **zatvor od 3 meseca do 3 godine**
- Za „STROGO POVERLjIVO“ → **zatvor od 6 meseci do 5 godina**
- Za „DRŽAVNA TAJNA“ → **zatvor od 1 do 10 godina**

U težim oblicima (iz koristoljublja, u inostranstvu, u ratnom stanju), kazne se kreću do **15 godina zatvora**.

Za **dela iz nehata**, zakonom su propisane blaže sankcije — u rasponu od **novčanih kazni do pet godina zatvora**, u zavisnosti od stepena tajnosti podataka.

4. Procena okolnosti nastanka incidenta u radu sa tajnim i njegova pravna kvalifikacija

Procena okolnosti nastanka bezbednosnog incidenta u radu sa tajnim podacima, kao i njegova pravna kvalifikacija, jedan je od najvažnijih koraka u obradi i određivanju daljeg postupanja u skladu sa propisima. U zavisnosti od vrste incidenta, različito će se reagovati nadležni organi i primeniti odgovarajući pravni mehanizmi. Ova procena ima velike pravne i bezbednosne implikacije, jer pogrešna kvalifikacija može dovesti do propusta u postupanju, što može imati ozbiljne posledice po bezbednost i pravni sistem.

1. **Tip incidenta:** Prva stvar koju treba razmotriti je sam tip incidenta. U pitanju mogu biti:
 - **Povreda radne discipline** – kada je incident izazvan nehatom ili nestručnim radom, ali bez namere ili ozbiljnih posledica po bezbednost podataka.
 - **Prekršaj** – ako su prekršeni propisani pravni ili tehnički okviri u radu sa tajnim podacima, ali ne postoji direktna namera da se ugrozi nacionalna bezbednost ili sigurnost.
 - **Krivično delo** – ako postoji namera ili svesno kršenje zakona koje rezultira ozbiljnim posledicama, kao što je otkrivanje, zloupotreba ili neovlašćeno otkrivanje tajnih podataka.
2. **Faktori koji utiču na kvalifikaciju:** Da bi se pravilno kvalifikovao incident, neophodno je uzeti u obzir nekoliko važnih faktora:
 - **Težina incidenta** – kolika je šteta nastala i koja je vrsta podataka ugrožena? Ako je ugrožen podatak visokog stepena tajnosti (na primer, državna tajna), incident će verovatno biti kvalifikovan kao ozbiljan, moguće i kao krivično delo.
 - **Namera počinioca** – da li je incident nastao zbog nenamerne greške ili zbog svesnog delovanja koje je imalo za cilj da se kompromituju tajni podaci? Namera će imati presudnu ulogu u kvalifikaciji incidenta.
 - **Šteta i efekti incidenta** – koja je stvarna šteta? Da li je incident imao ozbiljne posledice po bezbednost, integritet ili dostupnost podataka? Ako je nastala ozbiljna šteta, kao što je otkrivanje državne tajne ili kompromitacija bezbednosti, to može ukazivati na krivično delo.
3. **Postupci koji slede u zavisnosti od pravne kvalifikacije:**
 - **Povreda radne discipline:** Ako incident ne rezultira značajnom štetom i ako nije bilo svesne zloupotrebe podataka, može se smatrati povredom radne discipline. U tom slučaju, formira se posebna disciplinska komisija koja razmatra odgovornost pojedinca, a postupak se vodi u skladu sa propisima o radnoj disciplini.
 - **Prekršaj:** Ako su prekršeni propisani zakoni i procedure, ali nije došlo do ozbiljne štete, incident može biti kvalifikovan kao prekršaj.

U tom slučaju, prijava se upućuje nadležnom sudiji za prekršaje, koji donosi odluku o daljem postupku.

- **Krivično delo:** Ako postoji osnov sumnje da je izvršeno krivično delo (npr. svesno otkrivanje tajnih podataka ili njihova zloupotreba), nadležni tužilac će pokrenuti istragu u skladu sa Zakonikom o krivičnom postupku. U ovom slučaju, postupak će obuhvatiti sve radnje koje su potrebne za dokazivanje krivičnog dela, uključujući forenzičke analize i prikupljanje dokaza.

Procena uticaja i rizika od incidenta u radu sa tajnim podacima važan je korak u razumevanju stepena ugrožavanja koji je nastupio. To podrazumeva ne samo procenu nastanka materijalne štete, već i potencijalne posledice po nacionalnu bezbednost, prava lica ili organizaciju. Kada se procenjuje da li je incident mogao imati međunarodne implikacije, važno je uzeti u obzir stepen osetljivosti podataka, kao i mogućnost da se povreda izazove preko granica.

Mere koje treba preduzeti u slučaju incidenta - U zavisnosti od kvalifikacije incidenta, primenjuju se različite mere:

- **Blokada pristupa:** Za sprečavanje daljih oštećenja, neophodno je ograničiti pristup ugroženim podacima i preduzeti tehničke mere kao što su lock-out i povlačenje dokumenata.
- **Aktiviranje containment mera:** Ove mere podrazumevaju brzu reakciju kako bi se incident izolovao i sprečilo dalje širenje oštećenja.
- **Obaveštavanje nadležnih organa:** Bez odlaganja treba obavestiti Kancelariju SNBiZTP, BIA, kao i organe koji su odgovorni za informacionu bezbednost, u skladu sa propisima (npr. GDPR, NIS2).

Pravilna procena okolnosti nastanka incidenta i njegova pravna kvalifikacija od suštinske su važnosti za uspešnu obradu incidenta u radu sa tajnim podacima. Na osnovu precizne procene, nadležni organi mogu doneti odgovarajuće odluke i primeniti adekvatne pravne postupke. Pogrešna kvalifikacija može dovesti do propusta u zaštiti bezbednosti podataka i narušavanja pravnih procedura, što može imati ozbiljne posledice po organizaciju i društvo.

Jasno prepoznavanje prirode incidenta je od presudnog značaja za određivanje postupka koji će se primeniti. U zavisnosti od toga da li se radi o povredi radne discipline, prekršaju ili krivičnom delu, postupak i odgovornost nadležnih organa se razlikuju. Važno je da svaki incident bude adekvatno procenjen kako bi se odredio pravi pravni okvir u kojem će se nastaviti postupak.

5. Postupanje u slučaju incidenta sa tajnim podacima

Svaki incident koji se odnosi na zaštitu tajnih podataka smatra se **bezbednosnim incidentom visokog rizika** i zahteva **hitnu, koordinisanu i dokumentovanu reakciju**, u skladu sa Zakonom o tajnosti podataka („Sl. glasnik RS“, br. 72/2009).

Osnovne mere i obaveze postupanja:

- **Hitna prijava i dokumentacija incidenta** rukovodiocu organa javne vlasti i nadležnom rukovaocu tajnih podataka ili ovlašćenom licu u organu.
- **Sastavljanje pisanog izveštaja o incidentu**, u skladu sa članom 36. i 84. Zakona o tajnosti podataka.
- **Sprovođenje unutrašnje kontrole**, sa procenom uzroka, stepena rizika i eventualne kompromitacije podataka.
- **Primena mera sanacije i zaštite**, uključujući tehničke, organizacione i kadrovske korektivne mere.
- **Revizija postojećih mera zaštite** kako bi se sprečilo ponavljanje incidenta.
- U zavisnosti od karaktera povrede, **pokretanje disciplinskog, prekršajnog ili krivičnog postupka**, u skladu sa važećim propisima.

Napomena: Sprovođenje unutrašnje kontrole i izrada izveštaja su **obavezni** u svim slučajevima – **bez obzira na težinu posledica** incidenta. Izveštaj mora da sadrži:

- opis incidenta,
- analizu uzroka i posledica,
- procenu rizika po bezbednost podataka,
- predložene preduzete mere zaštite i prevencije, kao i pokrenutih disciplinskih, prekršajnih ili krivičnih postupaka.

Ovim se osigurava da svaki incident bude tretiran na ozbiljan, zakonit i sistemski način, uz dokumentovano praćenje i izveštavanje, što je osnova za efikasnu zaštitu tajnih podataka i jačanje bezbednosne kulture u organizaciji.

Uloga ovlašćenog lica ili starešine organa - Nadležno ovlašćeno lice ili starešina organa ima ključnu ulogu u upravljanju bezbednosnim incidentima koji uključuju tajne podatke. Njihova odgovornost nije samo da se odmah reaguje na incident, već i da se osigura da se preduzmu sve mere koje će sprečiti ponovno dešavanje sličnih incidenata u budućnosti. U skladu sa Zakonom o tajnosti podataka, kao i Zakonom o informacionoj bezbednosti, uloga ovih lica uključuje nekoliko osnovnih koraka koji su neophodni da se adekvatno postupi u slučaju bezbednosnog incidenta.

1. Utvrđivanje svih relevantnih činjenica - Nadležno ovlašćeno lice ili starešina organa ima obavezu da u saradnji sa relevantnim stručnim timovima, kao što su stručnjaci za bezbednost informacija i pravnici, utvrdi sve okolnosti koje su dovele do incidenta. Ovo podrazumeva detaljno istraživanje koji su faktori izazvali incident i koji su bili njegovi glavni uzroci. Postupak utvrđivanja činjenica treba biti sistematičan i uključivati sve aspekte incidenta, od tehničkih do ljudskih faktora.

Primer: Ako je došlo do neovlašćenog pristupa tajnim podacima, ovlašćeno lice mora utvrditi kako je do toga došlo — da li je u pitanju ljudska greška, tehnička manipulacija, ili namerna zloupotreba.

2. Procena stepena i vrste štete - Posle utvrđivanja činjenica, ovlašćeno lice je dužno da proceni stepen i vrstu štete koju je incident prouzrokovao. Ova procena mora obuhvatiti ne samo neposrednu materijalnu štetu (npr. uništene ili kompromitovane podatke), već i dugoročne posledice po nacionalnu bezbednost, integritet sistema, i moguće međunarodne implikacije. Stepen štete može varirati od lokalizovane štete koja ne ugrožava bezbednost zemlje, do većih bezbednosnih pretnji koje zahtevaju hitne mere.

Primer: Ako je incident podrazumevao izlaganje državnih tajni koje bi mogle biti iskorišćene od strane stranih vlada ili agencija, procena štete uključuje rizike od eskalacije međunarodnih sukoba ili diplomatskih posledica.

3. Preduzimanje hitnih mera radi ublažavanja posledica - Nadležno ovlašćeno lice ili starešina organa mora odmah preduzeti sve hitne mere koje su neophodne da se ublaže posledice incidenta. Ovo uključuje tehničke i operativne korake, kao što su blokiranje pristupa ugroženim podacima, ponovno obezbeđivanje pristupa podacima koji nisu ugroženi, kao i obustavljanje aktivnosti koje su doprinele incidentu. Ovakve mere su od presudne važnosti da bi se smanjila moguća šteta i da se spreči dalje širenje incidenta.

Primer: Ako je došlo do napada na informacioni sistem, hitne mere mogu uključivati onemogućavanje daljeg pristupa sistemu, izolaciju ugroženih delova mreže, kao i oporavak sa rezervnih kopija.

4. Iniciranje mera za sprečavanje ponavljanja incidenta - Jedan od najvažnijih zadataka ovlašćenog lica je da inicira mere koje će sprečiti ponavljanje sličnih incidenata u budućnosti. Ove mere mogu obuhvatati reviziju i unapređenje bezbednosnih politika, tehničkih mera i procedura koje su bile na snazi pre incidenta. Takođe, treba preduzeti korake za edukaciju i obuku zaposlenih u vezi sa najnovijim bezbednosnim rizicima i kako da ih izbegnu. Mere mogu uključivati i promene u procesima, kao i poboljšanje fizičke i logičke bezbednosti.

Primer: Ukoliko je incident rezultat ljudske greške, treba organizovati dodatne obuke o upravljanju podacima i bezbednosnim procedurama kako bi se sprečile slične greške u budućnosti.

5. Izveštavanje Kancelariji Saveta za nacionalnu bezbednost i zaštitu tajnih podataka - Kada je incident razjašnjen i mere su preduzete, ovlašćeno lice je dužno da obavesti Kancelariju Saveta za nacionalnu bezbednost i zaštitu tajnih podataka o svim detaljima incidenta, merama koje su preduzete i rezultatima. Ova izveštaja imaju ključnu ulogu u koordinaciji sa drugim državnim organima i međunarodnim partnerima, kao i u sprovođenju daljih mera ako je potrebno.

Primer: Kancelarija SNB treba biti obaveštena o prirodi incidenta, preduzetim merama i bilo kojim mogućim pravnim ili bezbednosnim posledicama koje su nastale kao rezultat incidenta.

Uklanjanje posledica bezbednosnog incidenta sa tajnim podacima i sprečavanje budućih incidenata zahteva pravovremeno, organizovano i koordinisano postupanje od strane ovlašćenog lica ili starešine organa. Njihova odgovornost je ključna za minimiziranje štete, obezbeđivanje daljeg sigurnog rukovanja tajnim podacima i održavanje poverenja u sistem zaštite podataka. U skladu sa Zakonom o tajnosti podataka i drugim relevantnim propisima, ove mere moraju biti strogo primenjene da bi se obezbedila visoka bezbednost podataka i sprečili potencijalni rizici po nacionalnu bezbednost.

6. Preporučene mere — postupanje po preporuci Kancelarije SNBiZTP

U skladu sa članom 35, stav 3. Zakona o tajnosti podataka, kao i sa opštim principima zaštite tajnih podataka, preporučene mere za postupanje u slučaju bezbednosnog incidenta u vezi sa tajnim podacima moraju biti izvedene sa visokim stepenom pažnje i u skladu sa propisanim pravnim i bezbednosnim procedurama. U nastavku su detaljno objašnjene sve relevantne mere koje treba preduzeti, kao i postupak prijema i obrade incidenta:

1. Obaveštavanje organa javne vlasti od kojeg potiče tajni podatak - Kada se utvrdi da je došlo do bezbednosnog incidenta koji uključuje tajne podatke, prvi korak je obaveštavanje organa javne vlasti od kojeg potiče tajni podatak. Ovo obaveštenje ima za cilj da omogući pravovremeno reagovanje i preuzimanje mera od strane nadležnih organa, što uključuje identifikaciju i eliminaciju uzroka incidenta. Takođe, organ koji upravlja podacima mora biti obavešten kako bi mogao da proceni potencijalne posledice po bezbednost podataka i njihovu klasifikaciju, kao i da se pruži pomoć u određivanju stepena ugroženosti.

Primer: Ako incident uključuje tajne podatke vezane za odbranu ili nacionalnu bezbednost, organ koji je zadužen za tajne podatke mora biti obavešten o svim detaljima, kako bi mogao preduzeti korake za dalje postupanje.

2. Pokrenuti postupak unutrašnje (vanredne) kontrole - Pokretanje postupka unutrašnje kontrole predstavlja obavezan korak u svim slučajevima bezbednosnog incidenta. U skladu sa Zakonom o tajnosti podataka, odgovorna lica u organizaciji moraju pokrenuti vanrednu kontrolu koja će ispitati sve okolnosti incidenta. Cilj ove kontrole je da se utvrdi kako je došlo do incidenta, koji su faktori doprineli njegovom nastanku, i da se identifikuju svi nedostaci u sistemu zaštite podataka.

Primer: Ako je incident posledica tehničke greške u sistemu zaštite, istraživanje će obuhvatiti analizu incidenta, forenzičku analizu podataka i reviziju bezbednosnih mera koje su bile na snazi u tom trenutku.

3. Obaveštavanje nadležnog tužilaštva (ako postoji osnovana sumnja na krivično delo) - U slučaju da tokom istrage incidenta postoji osnovana sumnja da je izvršeno krivično delo (npr. neovlašćeno otkrivanje tajnih podataka, zloupotreba ili drugi vidovi namernog kršenja zakona), nadležno tužilaštvo mora biti obavešteno. Zakon o tajnosti podataka i drugi relevantni propisi nalože na nadležne organe obavezu da, ako postoji krivično delo, postupe u skladu sa Zakonom o krivičnom postupku, što podrazumeva pokretanje istrage i, ako je potrebno, podnošenje krivične prijave.

Primer: Ukoliko se utvrdi da je neko svesno otkrio državnu tajnu ili distribuirao osetljive podatke bez dozvole, nadležno tužilaštvo treba biti obavešteno kako bi moglo pokrenuti postupak istrage.

4. Obaveštavanje Kancelarije SNBiZTP - U skladu sa članom 35 Zakona o tajnosti podataka, svaki incident koji uključuje povredu bezbednosti tajnih podataka mora biti odmah prijavljen Kancelariji za bezbednost nacionalnih podataka (SNB). Kancelarija SNB igra ključnu ulogu u koordinaciji i nadzoru postupanja u slučaju incidenta, obezbeđujući da sve mere budu usklađene sa nacionalnim i međunarodnim standardima zaštite podataka. Obaveštavanje Kancelarije SNB je takođe važno za koordinaciju sa drugim relevantnim organima, kao što su BIA i druge službe za bezbednost.

Primer: Kancelarija SNBiZTP treba biti obaveštena kada postoji bilo kakvo pomeranje u statusu tajnih podataka, kao i kada se utvrdi da je bezbednost podataka ugrožena.

5. Po potrebi, obaveštavanje Bezbednosno-informativne agencije (BIA) - U situacijama kada incident uključuje potencijalne pretnje po nacionalnu bezbednost, kao što su zloupotreba tajnih podataka u političkim ili bezbednosnim kontekstima, obaveštavanje Bezbednosno-informativne agencije (BIA) može biti neophodno. BIA ima zadatak da prati i analizira pretnje po bezbednost zemlje, i može biti odgovorna za sprečavanje daljih rizika po bezbednost.

Primer: Ako je incident doveo do izlaganja podataka koji mogu biti iskorišćeni od strane stranih agencija, BIA treba biti obavještena da bi se pokrenule kontramere.

Preporučene mere postupanja po preporuci Kancelarije SNBiZTP predstavljaju ključne korake u osiguranju da se svaki bezbednosni incident u vezi sa tajnim podacima adekvatno obradi. Pravovremeno obavješćavanje relevantnih organa i preduzimanje mera unutrašnje kontrole obezbeđuje da se spreče dalje posledice i da se održi integritet bezbednosnog sistema. Primenom ovih mera, organizacija može ne samo minimizirati rizike od potencijalnih šteta, već i biti u skladu sa zakonskim i bezbednosnim zahtevima koji regulišu rad sa tajnim podacima.

Upravljanje incidentima u vezi sa tajnim podacima mora se zasnivati na pravovremenoj reakciji, pravnoj i tehničkoj usklađenosti, kao i kulturi bezbednosti na svim nivoima. Dokumentovano postupanje nije samo zakonska obaveza, već i preduslov za očuvanje poverenja u institucionalni sistem zaštite tajnih podataka Republike Srbije.

7. Doprinos organizacije nastanku štetnog događaja u radu sa tajnim podacima

U sistemu zaštite tajnih podataka, odgovornost za bezbedno rukovanje podacima, dokumentima i informacijama od značaja za nacionalnu bezbednost, odbranu, spoljne i unutrašnje poslove, kao i vođenje krivičnih postupaka (tajnih podataka) ne leži isključivo na pojedincima, već prevashodno na samoj organizaciji – bilo da je reč o organu javne vlasti ili pravnom licu kome je omogućen pristup tajnim podacima na osnovu prethodnog postupka koji se sprovodi od strane organa javne vlasti. Organizacija kao celina može svojim propustima, neblagovremenim postupanjem ili nepotpunim primenama propisanih mera direktno ili indirektno doprineti nastanku štetnog događaja, odnosno bezbednosnog incidenta koji ugrožava tajne podatke.

1. Neuspostavljanje unutrašnjeg sistema zaštite tajnih podataka

Prvi i najčešći oblik doprinosa organizacije nastanku štetnog događaja jeste potpuno ili delimično **neuspostavljanje sistema zaštite tajnih podataka u skladu sa Zakonom o tajnosti podataka** („Službeni glasnik RS“, br. 104/2009). Ovakav propust ukazuje na institucionalni nedostatak u razumevanju ili primeni osnovnih obaveza u oblasti zaštite podataka od značaja za bezbednost, što ozbiljno ugrožava unutrašnju i spoljnu bezbednosnu poziciju organa ili pravnog lica.

Najčešći oblici ovog propusta uključuju:

- **✗ Nepostojanje internog akta – Plana zaštite tajnih podataka**, koji predstavlja osnovni normativni dokument u kome se definišu unutrašnje mere i odgovornosti zaštite u konkretnoj instituciji;
- **✗ Nepostavljanje rukovaoca tajnih podataka** (odgovornog lica za rukovođenje sistemom zaštite unutar organizacije), kao ni **ovlašćenog lica za zaštitu tajnih podataka**, što dovodi do izostanka kontrole nad pristupom i obradom podataka;
- **✗ Odsustvo internih procedura i uputstava** za prijem, obradu, evidenciju, čuvanje, uništavanje i prenos tajnih podataka, što zaposlene ostavlja bez jasnih smernica u svakodnevnom radu;
- **✗ Neodređivanje i neuspostavljanje fizičkih i tehničkih uslova** za bezbedno skladištenje, pristup i kontrolu tajnih podataka (npr. odgovarajući prostori, signalizacija, ormari, kontrolisan ulaz, sistemi video-nadzora i pristupnih lista).

✦ **Posledice ovih propusta** su sistemske prirode – dovode do ranjivosti cele institucije, omogućavaju neovlašćen pristup podacima, a zaposleni ostaju **nedovoljno informisani i nedovoljno obučeni za pravilno postupanje sa podacima označenim stepenom tajnosti**.

🔍 **Procena o postojanju ili nepostojanju sistema zaštite tajnih podataka** donosi se na osnovu **stručnog nadzora koji, na zahtev organa javne vlasti, periodično sprovodi Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka**, u skladu sa svojim ovlašćenjima propisanim zakonom i podzakonskim aktima.

✓ Uspostavljanje sistema mora biti dokumentovano, proverljivo i usklađeno sa uputstvima Kancelarije, uključujući i obavezu registracije sistema zaštite, redovnog izveštavanja, kao i edukacije zaposlenih o merama i procedurama zaštite.

2. Propusti u preventivnim i kontrolnim merama

Organizacija takođe može doprineti nastanku incidenta **nesprovođenjem preventivnih mera**, kao što su:

- nepostojanje plana upravljanja rizicima;
- neizvršavanje redovne procene bezbednosnih rizika;
- zanemarivanje bezbednosne provere lica koja pristupaju tajnim podacima;
- izostanak unutrašnje kontrole i revizije primene mera zaštite;
- **upotreba neakreditovanih IKT sistema za obradu tajnih podataka, odnosno sistemâ koji nisu prošli propisanu procenu i odobrenje od strane nadležnog organa** – što obuhvata:

- odsustvo tehničke i fizičke izolacije IKT sistema od javnih i internih mreža;
- nepostojanje mehanizama za kontrolu pristupa, registraciju aktivnosti i čuvanje evidencija;
- nepotpunu ili nedovoljnu primenu kriptografskih mera zaštite;
- nepravilnu instalaciju ili konfiguraciju softvera i operativnog sistema koji se koriste za rad sa tajnim podacima;
- zanemarivanje redovnog ažuriranja, tehničkog održavanja i praćenja sistema;
- nepostojanje zvanične odluke o akreditaciji IKT sistema od strane rukovodioca organa, u skladu sa propisima Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka.

Ovakvi propusti u IKT domenu ne samo da predstavljaju kršenje zakonskih obaveza, već direktno izlažu tajne podatke riziku od kompromitovanja, neovlašćenog pristupa i gubitka integriteta podataka.

3. Nedovoljna obučenost zaposlenih

Jedan od značajnih indirektnih doprinosa organizacije nastanku štetnog događaja jeste odsustvo ili neadekvatnost obuke zaposlenih, naročito lica koja imaju pristup tajnim podacima ili učestvuju u njihovoj obradi, čuvanju i prenosu. Nedovoljna edukacija i nesprovođenje redovnih obuka dovodi do smanjene svesti o rizicima, neodgovarajuće procene situacija i neprimene mera zaštite.

Organizacija koja ne sprovodi:

- ✓ **Obaveznu početnu obuku novozaposlenih** – u skladu sa propisima, sva lica koja dobiju sertifikat za pristup tajnim podacima moraju pre početka rada biti upoznata sa zakonskim i podzakonskim aktima koji uređuju postupanje sa tajnim podacima, kao i sa unutrašnjim procedurama u okviru organa;
- ✓ **Periodične obuke i provere znanja** – redovna obuka je obaveza i instrument za podsećanje, nadogradnju i proveru postojećih znanja, uključujući i testiranje razumevanja mera zaštite, tehničkih postupaka i pravnih okvira;
- ✓ **Simulacije bezbednosnih incidenata i praktične vežbe postupanja** – organizovanje scenarija i vežbi koje simuliraju gubitak, otkrivanje ili kompromitaciju tajnih podataka doprinosi sposobnosti zaposlenih da brzo, ispravno i usklađeno reaguju u realnim situacijama;

- ✓ **Specijalizovane edukacije u skladu sa nivoom pristupa i odgovornosti** – Kancelarija SNBiZTP organizuje osnovne, napredne i specijalizovane programe za lica u organima javne vlasti, odgovorna lica, ovlašćena lica za zaštitu tajnih podataka, kao i administratore IKT sistema koji rade u okviru zaštićenih zona;
- ✓ **Evidenciju i verifikaciju pohađanih obuka** – organizacija koja ne vodi evidenciju o obukama zaposlenih, sertifikatima i redovnom usavršavanju, gubi mogućnost kontrole kompetencija i pravovremenog upućivanja na obnovu znanja.

Odsustvo ovih oblika edukacije direktno smanjuje sposobnost zaposlenih da prepoznaju bezbednosni rizik, adekvatno postupe u slučaju sumnje na kompromitaciju, ili primene procedure koje bi sprečile nastanak većeg štetnog događaja. Sa druge strane, organizacije koje sistemski ulažu u **bezbednosnu kulturu**, kroz kontinuiranu edukaciju, smanjuju rizik od incidenata i povećavaju stepen usaglašenosti sa zakonom.

U skladu sa članom 82. Zakona o tajnosti podataka („Službeni glasnik RS“, broj 104/2009), organ javne vlasti dužan je da vodi i čuva evidenciju o licima koja su prošla obuku za rad sa tajnim podacima, kao i o izdatim sertifikatima za pristup podacima određenog stepena tajnosti. Ova evidencija predstavlja sastavni deo kadrovskog dosijea zaposlenih i služi kao dokaz o ispunjenosti uslova za pristup i postupanje sa tajnim podacima. Podaci iz evidencije moraju se čuvati na bezbedan način, uz poštovanje mera zaštite tajnih podataka i ograničen pristup, u skladu sa propisanim nivoom tajnosti. Nedovoljna ili nepostojeća evidencija ukazuje na nedostatke u sistemu zaštite i uskraćuje osnovu za internu i spoljnu kontrolu postupanja sa podacima od značaja za bezbednost.

4. Neadekvatna reakcija na bezbednosni incident

Drugi kritičan oblik organizacionog propusta odnosi se na **nepostojanje jasno definisane procedure reagovanja u slučaju incidenta sa tajnim podacima**. Bez utvrđenih koraka za identifikaciju, prijavu, analizu i otklanjanje posledica incidenta, čak i **naizgled manji propusti mogu eskalirati u ozbiljan bezbednosni rizik**, sa potencijalno dalekosežnim posledicama po interese Republike Srbije.

Tipični elementi neuspostavljenе ili neefikasne procedure obuhvataju:

- ✗ **Nedefinisani pojam bezbednosnog incidenta** – odsustvo preciznih kriterijuma šta se u konkretnoj organizaciji smatra incidentom u vezi sa tajnim podacima;
- ✗ **Nepostojanje unutrašnjeg mehanizma za prijavu incidenta** – ko je odgovoran da incident prijavi, kome se podnosi prijava, u kom roku i kojim kanalom;

- **✗ Neprijavljivanje incidenta nadležnim organima**, pre svega **Kancelariji Saveta za nacionalnu bezbednost i zaštitu tajnih podataka**, a u određenim slučajevima i **Ministarstvu pravde** u skladu sa zakonskim obavezama;
- **✗ Pokušaji prikrivanja, odugovlačenje sa analizom ili nepotpuno dokumentovanje incidenta**, što onemogućava identifikaciju uzroka i sprečavanje sličnih događaja u budućnosti;
- **✗ Izostanak preduzimanja hitnih mera** radi sprečavanja širenja posledica ili kompromitacije dodatnih podataka ili sistema.

✦ **Pravovremeno, transparentno i sistematizovano postupanje u slučaju incidenta** predstavlja jedan od osnovnih stubova sistema zaštite tajnih podataka. Ovakve procedure moraju biti deo Plana zaštite tajnih podataka, uključujući i evidenciju svih prijavljenih incidenata, analiza uzroka i izveštavanje prema nadležnim institucijama.

🔍 U okviru **stručnog nadzora koji sprovodi Kancelarija SNBiZTP**, često se kao pokazatelj niskog stepena zrelosti sistema uočavaju upravo ovakvi propusti u reagovanju, što ukazuje da organizacija nema unapređen mehanizam unutrašnjeg upozoravanja i sanacije rizika.

✓ Uspostavljanje mehanizama reagovanja ne predstavlja samo formalnu obavezu, već i praktičnu zaštitu organizacije od interne odgovornosti, gubitka poverenja i ugrožavanja integriteta celokupnog sistema bezbednosti podataka.

5. Odsustvo odgovornosti i disciplinskog postupanja

Treći značajan oblik doprinosa organizacije nastanku štetnog događaja jeste **nepostojanje utvrđenih mehanizama za pokretanje disciplinske, upravne ili krivične odgovornosti u slučaju propusta u radu sa tajnim podacima**.

Organizacije koje ne predviđaju jasne postupke za:

- **⚠ utvrđivanje lične i funkcionalne odgovornosti** lica koja su izazvala ili omogućila propust;
- **⚠ izricanje disciplinskih mera** u skladu sa internim aktima i važećim propisima;
- **⚠ pokretanje upravnih ili krivičnih postupaka** u slučajevima težih povreda obaveza u radu sa tajnim podacima;
- **⚠ analizu i sistematsko učenje iz prethodnih incidenata**, kroz unapređenje procedura i edukaciju zaposlenih,

ostavljaju pojedince bez osećaja odgovornosti i podstiču ponavljanje istih propusta.

✦ Odsustvo sankcionisanja stvara ambijent u kojem se kršenje procedura ili nemarno postupanje sa tajnim podacima **ne doživljava kao ozbiljan prekršaj**, što direktno ugrožava bezbednost celog sistema.

🔍 Ovakav propust se redovno identifikuje u okviru **stručnog nadzora koji Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka sprovodi na zahtev organa javne vlasti**, kao deo procene efikasnosti unutrašnjeg sistema kontrole i zaštite tajnih podataka.

✓ Uspostavljanje sistema odgovornosti predstavlja ključni element sistema upravljanja zaštitom tajnih podataka, jer obezbeđuje ne samo prevenciju, već i povratnu informaciju za stalno unapređenje zaštitnih mera.

6. Tolerisanje kulture nebezbednog postupanja

Na kraju, ali ne manje važno, **organizacija doprinosi nastanku incidenata ukoliko ne razvija i ne neguje kulturu bezbednosti u radu sa tajnim podacima**. Kultura bezbednosti predstavlja skup vrednosti, stavova i navika zaposlenih koji doprinose doslednoj primeni mera zaštite tajnih podataka u svakodnevnom radu. Ukoliko organizacija zanemari ovaj aspekt, javljaju se sledeći rizični obrasci ponašanja:

- ⚠ **zanemarivanje procedura i internih pravila**, koja se često doživljavaju kao puka formalnost ili birokratska obaveza;
- ⚠ **neovlašćeno postupanje sa podacima**, uključujući nošenje tajnih podataka u ličnim torbama, fotografisanje dokumenata mobilnim telefonima ili slanje poverljivih sadržaja putem nezaštićenih elektronskih komunikacija;
- ⚠ **odsustvo sistema za prijavu propusta**, kao i atmosfere u kojoj se prijavljivanje grešaka ne podstiče već demotiviše;
- ⚠ **tolerisanje neprofesionalnog i nehatnog pristupa u radu sa poverljivim i tajnim podacima**, čime se podrivaju osnovni bezbednosni principi.

✦ Izostanak kulture bezbednosti dovodi do toga da zaposleni ne prepoznaju ozbiljnost rizika, ne osećaju ličnu odgovornost i ne postupaju u skladu sa propisanim obavezama.

✓ Uspostavljanje kulture bezbednosti podrazumeva **liderski primer rukovodstva, kontinuiranu edukaciju, transparentnost u postupanju i podsticanje odgovornog ponašanja na svim nivoima organizacije**.

🔍 Ova dimenzija bezbednosti takođe je predmet **stručne procene u okviru nadzora koji Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka**

sprovodi na zahtev organa javne vlasti, pri čemu se posebno vrednuje koliko se bezbednosne vrednosti primenjuju u praksi, a ne samo u formalnim dokumentima.

Doprinos organizacije nastanku štetnog događaja u radu sa tajnim podacima ogleda se u propustima koji mogu biti prisutni na **sistemskom, operativnom i edukativnom** nivou. Ovaj problem se ne odnosi samo na pojedinačne greške ili namerne propuste pojedinaca, već na **celokupni kontekst i pristup** koji organizacija ima prema bezbednosti podataka.

Bez obzira na karakter konkretnog incidenta, odgovornost organizacije se ogleda u sledećem:

-  **Stvaranju uslova za bezbedan rad sa tajnim podacima** – To podrazumeva uspostavljanje sistema koji obuhvata sve aspekte zaštite tajnih podataka, od pravnih akata do tehničkih mera;
-  **Obezbeđivanju alata za adekvatno reagovanje i sankcionisanje** – Organizacija mora da ima unapred definisane procedure za postupanje u slučaju incidenta, kao i mehanizme za sankcionisanje propusta, čime se stvara sistem odgovornosti i podsticanje na pažljivo postupanje sa tajnim podacima;
-  **Izgrađivanju kulture bezbednosti** – U okviru ove kulture, bezbednost podataka ne predstavlja samo tehničku ili administrativnu obavezu, već je **profesionalna i zakonska odgovornost svih članova organizacije**. Prema tome, izgrađivanje svesti i stavova koji podstiču odgovorno ponašanje i kontinuiranu obuku zaposlenih čini osnovu uspešne zaštite tajnih podataka.

✦ Ova sistemska odgovornost organizacije podrazumeva ne samo sagledavanje incidenata kao individualnih propusta, već i procenu da li organizacija kao celina ima postavljene mehanizme koji sprečavaju nastanak i eskalaciju ovakvih događaja.

🔍 **Procena i nadzor**, koji sprovodi Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka na zahtev organa javne vlasti, takođe uključuje analizu ovih aspekata, te **periodične kontrole i savete za unapređenje sistema zaštite tajnih podataka**.

8. LISTA ZA PROVERU U SLUČAJU INCIDENTA SA TAJNIM PODACIMA

Ova lista za proveru služi kao **praktičan i sistematski alat** koji omogućava pravovremeno i efikasno reagovanje u slučaju incidenta sa tajnim podacima. Ona pomaže u održavanju usklađenosti sa pravnim i operativnim zahtevima, kao i u stvaranju osećaja odgovornosti unutar organizacije.

★ 1. Identifikacija incidenta

Cilj: Brzo i precizno utvrditi osnovne informacije o incidentu i početne mere reagovanja.

- ☐ Jasan i sažet opis događaja
- ☐ Datum i vreme kada je incident uočen
- ☐ Precizna lokacija nastanka incidenta
- ☐ Navođenje ugroženih tajnih podataka (naziv, broj, stepen tajnosti)
- ☐ Lica koja su bila u kontaktu sa tajnim podacima
- ☐ Procena rizika od kontakta neovlašćenih lica
- ☐ Utvrđenje da li je podatak napustio zaštićeni prostor ili sistem (fizički ili elektronski)

★ 2. Obaveštavanje nadležnih

Cilj: Osigurati pravovremeno obaveštavanje svih relevantnih institucija radi preduzimanja daljih mera.

- ☐ Rukovalac tajnim podacima ili ovlašćeno lice za tajne podatke unutar pravnog lica
- ☐ Starešina organa ili odgovorno lice
- ☐ Organ javne vlasti koji je odredio stepen tajnosti
- ☐ Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka
- ☐ Nadležno tužilaštvo (ukoliko postoji osnov za krivičnu odgovornost)
- ☐ Bezbednosno-informativna agencija – BIA (ako je potrebno)
- ☐ Obaveštavanje po preporuci Kancelarije SNBiZTP (ako je već izdata ili se očekuje)

★ 3. Utvrđivanje okolnosti i pravna kvalifikacija

Cilj: Rasvetljavanje uzroka incidenta, identifikacija propusta i odgovornih lica.

- ☐ Pokrenuta unutrašnja (vanredna) kontrola
- ☐ Utvrđeni uzroci incidenta
- ☐ Procenjena šteta i potencijalni domet posledica
- ☐ Procena da li postoje elementi:
- ☐ Povrede radne discipline
- ☐ Prekršaja
- ☐ Krivičnog dela
- ☐ Konsultacija sa pravnim službama ili tužilaštvom radi kvalifikacije
- ☐ Donosena odluka o pokretanju postupka (disciplinski, prekršajni, krivični)

✦ 4. 🛡️ **Zaštita i sanacija**

Cilj: Hitno sprečavanje daljeg ugrožavanja podataka i poboljšanje mera zaštite.

- ☐ Onemogućen dalji pristup ugroženim podacima
- ☐ Aktivirane containment mere (tehničke, administrativne, fizičke)
- ☐ Sprovedene privremene i trajne preventivne mere
- ☐ Održana obuka i izdata uputstva za zaposlene
- ☐ Ažurirana tehnička i organizaciona dokumentacija

✦ 5. 📋 **Izveštavanje i evidencija**

Cilj: Kompletna dokumentacija događaja radi praćenja, kontrole i sistemskog unapređenja.

- ☐ Sačinjen zvaničan izveštaj o incidentu
- ☐ Izveštaj dostavljen svim relevantnim institucijama
- ☐ Incident evidentiran u:
- ☐ Registar incidenata u organu
- ☐ Registar u skladu sa NIS2 direktivom (ako je primenljivo)
- ☐ Sprovedena analiza sa predlozima za unapređenje bezbednosnih mera
- ☐ Posebna evidencija preporuka Kancelarije SNBiZTP

9. PREPORUČENE MERE – USKLAĐENE SA EU PRAKSOM

Mera	Opis
 Obaveštavanje	U skladu sa Zakonom o tajnosti podataka, obaveštavanje nadležnih organa mora biti odmah po utvrđivanju incidenta. Ovo uključuje izvorni organ, Kancelariju SNBiZTP, BIA (ako je potrebno), kao i druge relevantne institucije. Prema GDPR i NIS2, relevantna tela uključuju Vladu Srbije, CERT i druge institucije informacione bezbednosti.
 Utvrdjivanje okolnosti	Forenzička analiza sa detaljnom vremenskom linijom, identifikacijom svih ugroženih podataka i eventualnih bezbednosnih rupa, u skladu sa Zakonom o informacionoj bezbednosti. Forenzička analiza mora obuhvatiti sve aspekte incidenta i utvrditi uzroke, kao i eventualne propuste u sistemu zaštite podataka.
 Procena uticaja i rizika	Procena prirode podataka (npr. odbrambeni, lični, poslovne tajne), rizika po prava lica (GDPR), kao i potencijalnih međunarodnih posledica, posebno u kontekstu EU i NATO obaveza. Ova procena uključuje sve aspekte kao što su mogućnost neovlašćenog pristupa, moguće oštećenje ugleda ili finansijske posledice.
 Ograničenje štete	Tehničke i administrativne mere kao što su blokada pristupa, izmene lozinki, deaktiviranje naloga, uklanjanje informacija sa otvorenih platformi. Sve u skladu sa propisima o informacionoj bezbednosti. Ove mere moraju biti implementirane odmah nakon utvrđivanja incidenta i obuhvatati sve sisteme koji su bili u riziku.
 Izveštaj i dokumentacija	Zvanični izveštaj o incidentu mora biti arhiviran i dostupan nadležnim institucijama. Prati ga analiza uzroka i mera. Čuvanje i evidencija u skladu sa Zakonom o tajnosti podataka. Izveštaj treba da sadrži sve bitne podatke, kao i preporuke za unapređenje mera bezbednosti kako bi se sprečilo ponovno dešavanje sličnih incidenata.
 Obaveštavanje stranih partnera	Ako su ugroženi podaci pod kontrolom EU, NATO ili drugih stranih entiteta, neophodna su obaveštenja u skladu sa međunarodnim ugovorima i GDPR propisima. Obaveštavanje mora biti vršeno u skladu sa ugovorenim procedurama i rokovima koji se odnose na bezbednost podataka u međunarodnim kontekstima.
 Obaveštavanje javnosti	U slučaju incidenata od javnog značaja, obaveštavanje mora biti uravnoteženo sa propisima o slobodi pristupa informacijama i zaštiti podataka. Vodi se računa o stepenu tajnosti i mogućim posledicama po javni interes. Propisi o transparentnosti i

Mera

Opis

obaveštavanju javnosti treba da budu usklađeni sa međunarodnim pravima i lokalnim zakonodavstvom.

10. Zaključna razmatranja

Postupanje u slučaju incidenta sa tajnim podacima predstavlja ključni aspekt očuvanja bezbednosne stabilnosti i institucionalnog kredibiliteta organa javne vlasti i pravnih lica koji obrađuju tajne podatke od značaja za nacionalnu bezbednost, odbranu, unutrašnje i spoljne poslove. S obzirom na visoku osetljivost ovih podataka, od suštinske je važnosti da svaka organizacija koja u svom delokrugu rada obrađuje tajne podatke ima jasno definisane procedure, odgovornosti i mehanizme postupanja u slučaju nastanka bezbednosnog incidenta.

Polazna osnova ovog vodiča jeste primenljivi pravni okvir, pre svega **Zakon o tajnosti podataka** („Sl. glasnik RS“, br. 104/2009) i **Zakon o informacionoj bezbednosti** („Sl. glasnik RS“, br. 6/2016, 94/2017 i 77/2021), koji, zajedno sa pratećim podzakonskim aktima i internim opštim aktima, utvrđuju obavezu primene mera zaštite, obaveštavanja, postupanja i kontrole. Ovim propisima su utvrđene obaveze svih subjekata sistema, od rukovaoca tajnih podataka, preko rukovodstva organizacija, do samih korisnika tajnih podataka.

Poseban značaj ima primena sistemskih i preventivnih mera, kao što su definisanje nadležnosti u okviru unutrašnjeg sistema zaštite tajnih podataka, utvrđivanje tačnih kontakt tačaka za prijavu incidenata, obezbeđivanje tehničkih i organizacionih uslova za bezbednu obradu i skladištenje tajnih podataka, kao i redovno sprovođenje obuka i provera. Unapređenjem internih akata, evidencija, pristupnih prava i bezbednosne infrastrukture, smanjuje se verovatnoća nastanka incidenata i gradi se kultura odgovornog postupanja sa svim štićenim podacima, a posebno sa tajnim podacima.

Operativni postupci nakon incidenta moraju biti precizni, efikasni i usmereni na ograničenje štete, sprečavanje daljeg širenja posledica, identifikaciju uzroka i aktera, kao i obnovu bezbednosnog kapaciteta. Proces otkrivanja, prijavljivanja i reagovanja mora biti pravovremen, a komunikacija sa nadležnim organima, pre svega Kancelarijom Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, obavezna i dokumentovana. Sprovođenje interne forenzičke analize, pregled tehničke i fizičke bezbednosti, kao i izrada izveštaja sa merama za otklanjanje posledica, predstavljaju neizostavan deo postupka.

Ne manje važno, pitanje **odgovornosti i sankcionisanja** mora biti jasno utvrđeno. Utvrđivanje propusta u primeni mera zaštite, odgovornosti lica zaduženih za čuvanje i obradu tajnih podataka, kao i eventualne namerne ili nehatne radnje koje su dovele do incidenta, moraju biti predmet disciplinskih, upravnih, prekršajnih ili krivičnih

postupaka, u skladu sa težinom povrede. Ovo predstavlja ključni element održavanja pravne sigurnosti i poverenja u sistem zaštite tajnih podataka.

Istovremeno, ovaj vodič ima za cilj da podstakne i ojača bezbednosnu svest i kulturu unutar organa javne vlasti. To podrazumeva ne samo primenu propisanih procedura, već i podizanje svesti o značaju zaštite tajnih podataka na svim nivoima — od najviših rukovodilaca do izvršilaca u sistemu. Bezbednosna kultura ne postiže se samo aktima, već svakodnevnom primenom pravila, redovnom komunikacijom o rizicima, ohrabrivanjem prijavljivanja nepravilnosti i kontinuiranom edukacijom.

U tom kontekstu, unapređenje sistema zaštite tajnih podataka mora biti kontinuiran proces, prilagođen tehnološkom razvoju, promenama u pravnom i bezbednosnom okruženju, kao i rezultatima iz prethodno analiziranih incidenata. Izveštavanje, evidencija, analiza i povratne informacije treba da služe ne samo radi ispunjenja zakonske forme, već i kao poluga za realno unapređenje sistema.

Na kraju, uvođenjem ovog vodiča kao obaveznog alata u praksi, organizacije dobijaju jasnu strukturu postupanja u kriznim situacijama, ali i stabilnu osnovu za izgradnju otpornijeg, bezbednijeg i odgovornijeg sistema rukovanja tajnim podacima. Na taj način se ne štite samo tajni podaci, već i legitimitet, integritet i operativna sposobnost celokupnog sistema nacionalne bezbednosti.