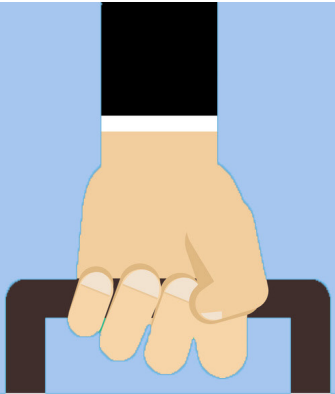




Bring Your Own Device



Smernice Informacijskega pooblaščenca

Uporaba zasebnih naprav v službene namene (BYOD)

o smernicah Informacijskega pooblaščenca

Namen smernic IP je podati skupne praktične napotke za upravljavce zbirk osebnih podatkov (OP) na jasn, razumljiv in uporaben način in s tem odgovoriti na najpogostejše zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci zbirk OP. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju ZVOP-1).

Pravno podlago za izdajo smernic Pooblaščenca daje 49. člen ZVOP-1, ki med drugim določa, da Pooblaščenec daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način ter pripravlja in daje neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju.

Oglejte si tudi:

Mnenja IP: <https://www.ip-rs.si/vop/>

Brošure IP: <https://www.ip-rs.si/publikacije/prirocniki-in-smernice/>

Smernice IP so objavljene na spletni strani:

<http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/>

Namen dokumenta:	Namen smernic je upravljavce opozoriti na primeren pristop pri dopuščanju uporabe zasebnih naprav v službene namene (t.i. koncept »Bring Your Own Device« - BYOD). Smernice predstavijo prednosti in tveganja BYOD ter priporočila za zakonito in varno uvedbo takšnih rešitev.
Ciljne javnosti:	Upravljavci zbirk osebnih podatkov v javnem in zasebnem sektorju, ponudniki sistemov za upravljanje mobilnih naprav, sistemski integratorji.
Status:	Javno
Verzija:	1.0
Datum verzije:	5.5.2016
Avtorji:	Informacijski pooblaščenec
Ključne besede:	Smernice, BYOD, zavarovanje osebnih podatkov, presoja vplivov na zasebnost, informacijska varnost, upravljanje tveganj.

Kazalo

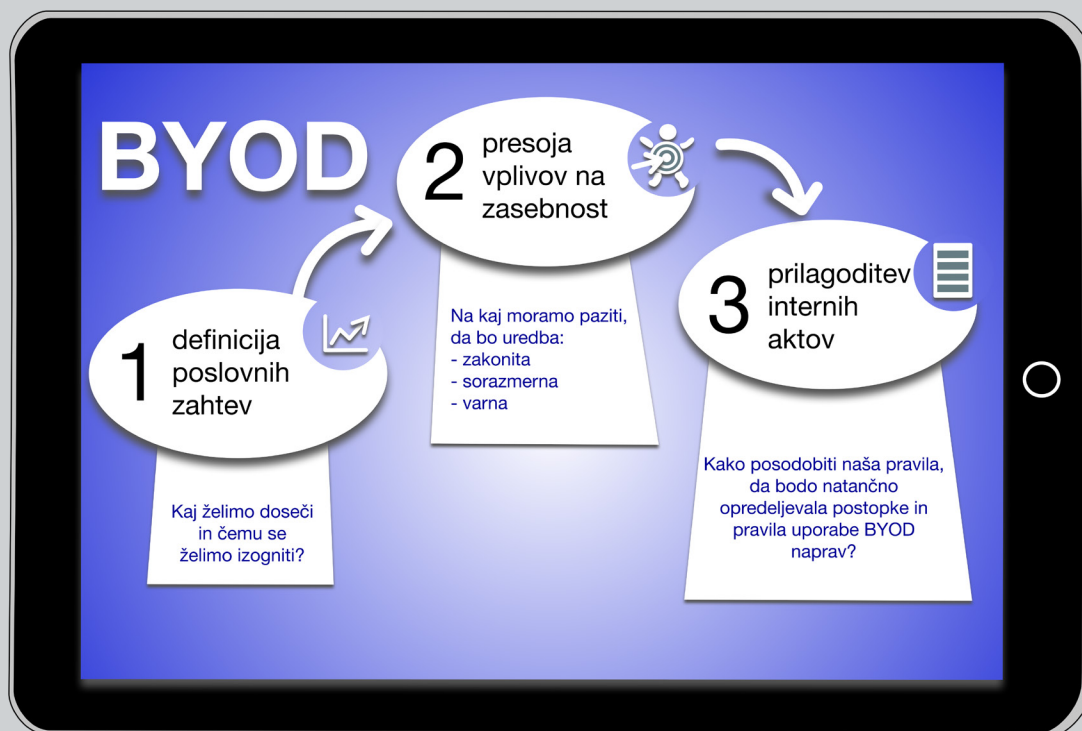
POVZETEK	4
1. KAJ JE BYOD?	5
2. PREDNOSTI BYOD	5
3. TVEGANJA BYOD	6
3.1 TVEGANJA GLEDE ZAKONITOSTI OBDELAVE OSEBNIH PODATKOV	7
3.2 TVEGANJA GLEDE ZAVAROVANJA OSEBNIH PODATKOV	8
4. BYOD – ZAKONITO IN VARNO	9
4.1. DEFINIRANJE POSLOVNIH ZAHTEV	9
4.2. IZVEDBA PRESOJE VPLIVOV NA ZASEBNOST (PIA)	10
4.2.1. Zakonitost	10
4.2.2. Sorazmernost	11
4.2.3. Namenskost	11
4.2.4. Točnost in ažurnost	11
4.2.5. Pravice posameznika	11
4.2.6. Roki hrambe	11
4.2.7. Zavarovanje (informacijska varnost)	12
4.3. PRILAGODITEV INTERNIH AKTOV	13
5. POGOSTA VPRAŠANJA	14
6. ZAKLJUČEK	15

POVZETEK

Prevladujoča vloga namiznih in prenosnih računalnikov v tipičnem delovnem okolju v informacijski družbi se neizogibno zmanjšuje – pot si vtirajo pametni telefoni, tablice in druge prenosne naprave, ki omogočajo stalno povezanost in opravljanje dela kjerkoli. Med pametnimi mobilnimi napravami pa je čedalje več takih, ki so v lasti zaposlenih, a jih ti uporabljajo tudi v službene namene. Prednosti za zaposlene so predvsem v navajenosti na lastne naprave in njihovi stalni dostopnosti, poleg tega pa odpade potreba po prenašanju več naprav, službenih in zasebnih. Večja mobilnost, produktivnost in dosegljivost zaposlenih pa so vedno bili v interesu delodajalcev. Če vse to lahko dosežemo z napravami, ki jih delodajalec sploh ne rabi kupiti, potem toliko bolje – številne organizacije zato omogočajo uporabo zasebnih naprav tudi v službene namene (t.i. koncept »Bring Your Own Device« -BYOD).

Seveda pa dopuščanje zasebnih naprav v službenih okoljih neizogibno odpira niz pravnih, tehnoloških in varnostnih izzivov, ki jih je treba pravočasno identificirati in obravnavati. Ne gre namreč za izziv, kako pripeljati lastne naprave na delo, temveč kako delo spraviti na naprave uporabnikov, ne da bi ogrozili varnosti ali zakonsko skladnost poslovanja¹.

Pred vpeljavo BYOD je ključno, da se opravi premislek o poslovnih potrebah oziroma zahtevah, ki jih zasleduje organizacija, izvede analiza tveganj po temeljnih načelih varstva osebnih podatkov ter ustrezno dopolnijo interni akti organizacije.



¹ <http://www.dataconnectors.com/events/2013/08washingtondc/pres/fixmo.ppsx>

1. KAJ JE BYOD?

Koncept »Bring Your Own Device« (BYOD) se nanaša na prakso, ko zaposleni v službeno okolja prinašajo svoje zasebne naprave (prenosnike, tablice, pametne telefone), prek katerih potem dostopajo do poslovnih, osebnih in drugih podatkov v informacijskem sistemu organizacije. Pogosto so namreč njihove zasebne naprave bolj zmogljive od tistih, ki so jim na voljo v službenem okolju (zlasti pri vodstvenih kadrih) oziroma so nanje bolj navajeni, omogočajo jim večjo mobilnost in dostopnost do podatkov, zato bi jih radi uporabljali tudi v službene namene. To je seveda povezano s številnimi tveganji tako glede varnosti poslovnih informacij kot varstva osebnih podatkov, do katerih na ta način dostopajo.

Zavedati se moramo, da z dopuščanjem uporabe zasebnih naprav v službene namene odpiramo resna varnostna vprašanja. Statistike kažejo, da se vsak teden na letališčih v ZDA izgubi 12000 prenosnikov, 53% zaposlenih, ki delajo s podatki, pa ima na svojih zasebnih napravah zaupne podatke poslovne narave². Po drugi strani si številni zaposleni že zdaj službeno elektronsko pošto in podatke preusmerjajo na zasebne predale elektronske pošte oziroma za službeno komunikacijo uporabljajo svoje zasebne naprave, saj jih stroge varnostne politike, ki jih podjetje vsiljuje na službenih sredstvih, odvrta od uporabe službenih naprav in komunikacijskih kanalov. Pri tem pa ne opravijo presoje, ali so njihove zasebne naprave tudi dovolj varne. Kar nekaj vodilnih politikov je bilo tako v zadnjem času ujetih pri tem, da so se namesto službenih telefonov in komunikacijskih kanalov zaradi večje uporabnosti in udobja zatekli k lastnim napravam, s tem pa ogrozili varnost zaupnih informacij.

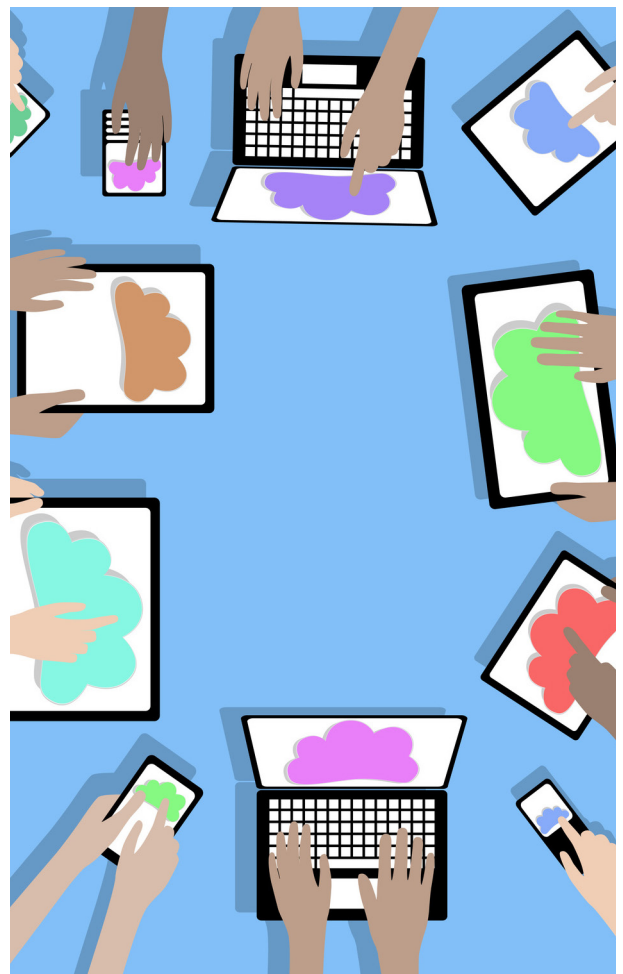
S porastom takšne uporabe mobilnih naprav v zadnjih letih raste tudi trg rešitev za upravljanje mobilnih naprav (ang. **Mobile Device Management** ali **MDM**), ki bolj ali manj uspešno naslavlja varnostne vidike uporabe zasebnih naprav v službenih okoljih. Zavedati pa se moramo, da ne gre zgolj za varnostna tveganja, temveč tudi za tveganja glede zagotavljanja skladnosti z zakonodajnimi zahtevami varstva osebnih podatkov, tajnih podatkov, delovnega in konkurenčnega prava. Vsaka organizacija, ki se zato odloča za vpeljavo koncepta BYOD, mora pravočasno analizirati tveganja ter zagotoviti postopke in ukrepe, s katerimi bo zmanjšala ali izničila tveganja za zahtevano raven zakonitosti in varnosti svojega poslovanja.

² <https://www.ponemon.org/news-2/8>, <http://www.zdnet.com/article/forrester-53-of-employees-use-their-own-devices-for-work/>

2. PREDNOSTI BYOD

Koncept BYOD obljublja večje zadovoljstvo in boljšo mobilnost zaposlenih, ter posledično njihovo večjo storilnost in produktivnost. Če ga organizacija vpelje na premišljen način, tj. po predhodni podrobni analizi in po ustrezni prilagoditvi varnostne politike, lahko vsekakor pripeva k bolj učinkovitemu doseganju ciljev organizacije. Dalje, zavedanje varnostnih vidikov, ki so pri uvajanju in uporabi BYOD nekoliko specifični, lahko poveča tudi splošno dojemanje in razumevanje varnosti ter s tem varstva osebnih podatkov znotraj organizacije. Prav tako lahko omogoči večjo varnost tudi za delavčeve lastne podatke, npr. z zahtevami po uporabi antivirusnega programa, PIN-a, oz. možnosti zaklepanja podatkov na mobilniku na daljavo v primeru kraje, ki jih sicer zaposleni na svoji napravi ne bi uporabljal.

A namen teh smernic ni v izpostavljanju prednosti BYOD – te bodo organizacijam pogosto razvidne same, vsekakor pa jim jih bodo predstavili ponudniki tovrstnih rešitev. Namen je predvsem opozoriti na tveganja pri vzpostavitvi BYOD in primerne pristope k upravljanju teh tveganj.



3. TVEGANJA BYOD

Izhodiščno se moramo zavedati, da gre pri BYOD za naprave, ki jih je kupil, jih uporablja in vzdržuje **zaposleni (posameznik) sam**, pri tem pa ni bil vezan na varnostno politiko organizacije, v katero prinaša zasebno napravo. In tudi ko napravo prinese v službeno okolje, ostaja njegova last. Posledično so **možnosti organizacije za nadzor nad varnostjo** določene naprave in podatkov, ki so dostopni prek nje, **pomembno omejene**. Pravil, ki sicer veljajo za službeno opremo, namreč ni dopustno nediskriminatorno uveljaviti tudi za zasebno opremo. Velik del vprašanj glede BYOD je tako povezan z vidiki informacijske varnosti, posebno pozornost pa je vendarle treba nameniti tudi vprašanjem spoštovanja delavčeve zasebnosti. Gre torej za preplet različnih tveganj.

Iz teh razlogov številni svarijo pred nepremišljenim uvajanjem BYOD. Smernice Bele hiše za zvezne agencije³ tako opozarjajo, da gre za preplet varnostnih, tehničnih in pravnih izzivov, smernice za britanske državne organe⁴ pa navajajo, da je koncept BYOD sicer možen, a ga vseeno ne priporočajo prav zaradi različnih tehničnih in drugih tveganj. Francoska varnostno-obveščevalna agencija (ANSSI)⁵ celo odsvetuje uporabo BYOD, nemški zvezni urad za informacijsko varnost BSI⁶ poudarja, da naraščajoča uporaba zasebnih naprav v službenih okoljih predstavlja številne izzive za varnost in varstvo osebnih podatkov, zato je na BYOD treba gledati kot na strateški izziv z vidika samega vodstva organizacije. Pri tem poudarja, da zgolj tehnični ukrepi ne zadostujejo oz. da morajo biti podprti z ustreznimi organizacijskimi ukrepi, v skladu s krovno strategijo in cilji organizacije.

Mednarodna delovna skupina za varstvo osebnih podatkov v telekomunikacijah (IWGDPT), katere član je tudi Informacijski pooblaščenec, je leta 2014 sprejela delovni dokument⁷ na temo zasebnosti in varnosti pri uporabi BYOD naprav v službenih okoljih, v katerem so med drugim zapisana tudi določena priporočila in opozorila organizacijam. S strani varuhov zasebnosti sta poleg IWGDPT svoje smernice med drugim izdala kanadski⁸ ter britanski⁹ informacijski pooblaščenec.

3 <http://www.whitehouse.gov/digitalgov/bring-your-own-device#key-considerations>

4 <https://www.gov.uk/government/publications/end-user-devices-security-guidance-introduction>

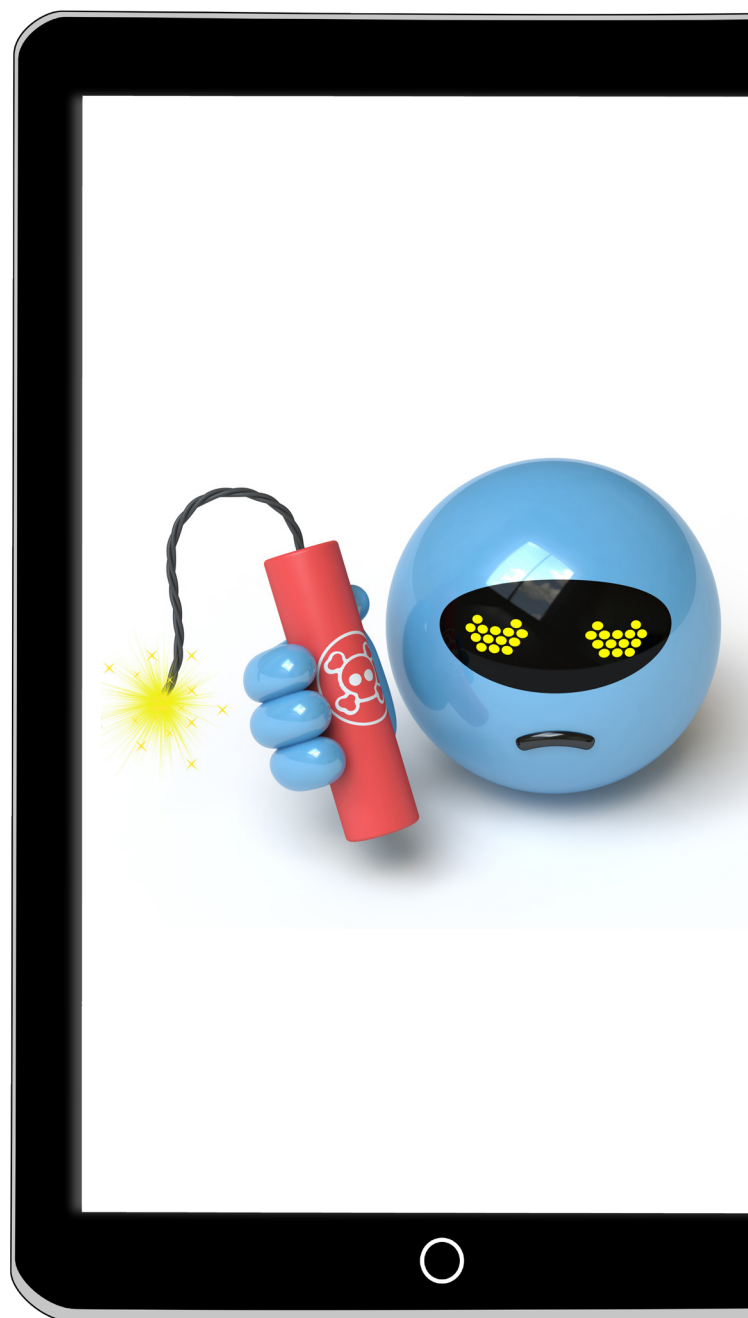
5 http://www.ssi.gouv.fr/IMG/pdf/Communique_de_presse_Assises_de_Monaco_2012_v2.pdf

6 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/Ueberblickspapiere/Ueberblickspapiere_node.html

7 https://datenschutz-berlin.de/attachments/1082/675.49.10_WP_Own_Devices.pdf?1419853968

8 http://www.ipc.on.ca/site_documents/pbd-byod.pdf

9 http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/byod



3.1 TVEGANJA GLEDE ZAKONITOSTI OBDELAVE OSEBNIH PODATKOV

Z vidika zakonitosti obdelave osebnih podatkov pri konceptu BYOD moramo ločiti:

- a) osebne podatke **uporabnika naprave in drugih oseb**, ki lahko uporabljajo napravo (npr. družinski člani);
- b) **osebne podatke, s katerimi upravlja organizacija** in do katerih ima uporabnik dostop preko BYOD naprave.

Delodajalca kot upravljavca **osebnih podatkov svojih zaposlenih** omejuje zakonodaja, ki mu nalaga, da pri zbiranju osebnih podatkov upošteva pravice zaposlenih. Zakon o delovnih razmerjih (ZDR-1) tako med drugim določa:

- 46. člen: delodajalec mora spoštovati in varovati delavčevo osebnost ter upoštevati in ščititi delavčevo zasebnost;
- 48. člen - varstvo delavčevih osebnih podatkov: Osební podatki delavcev se lahko zbirajo, obdelujejo, uporabljajo in posredujejo tretjim osebam samo, če je to določeno s tem ali drugim zakonom ali če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem.

Zakon o evidencah na področju dela in socialne varnosti (ZEPDSV) pa dalje določa, katere evidence sme oziroma mora delodajalec voditi o zaposlenih.

Mobilne naprave so naši stalni spremljevalci in praviloma vsebujejo ogromno količino naših osebnih podatkov, bodisi da se hranijo na sami napravi bodisi do njih pridemo preko naprave (npr. imeniki, elektronska pošta, koledarji, podatki o uporabi spleta, fotografije, video zapisi...). Med njimi bomo hitro našli tudi podatke, ki jih lahko štejemo za **občutljive osebne podatke**, kot so npr. podatki o zdravstvenem stanju, verski, politični, nacionalni pripadnosti, katerih delodajalec praviloma sploh ne sme zbirati ali jih dalje obdelovati.

Delodajalci bi v skrbi za varnost lastnih podatkov s prestrogimi varnostnimi ukrepi in **preširokim nadzorom BYOD naprav lahko posegli v pravice zaposlenega in ostalih uporabnikov njegove naprave** – takšen primer je recimo dodeljevanje polnih pravic administratorjem organizacije nad BYOD napravami (vključno z dostopom do povsem zasebnih podatkov) ter možnost popolnega brisanja na daljavo (npr. v primeru izgube ali kraje BYOD naprave; ang. remote wipe), kjer bi lahko prišlo do izgube podatkov zasebne narave in zasebne korespondence uporabnika. Nekateri sistemi za upravljanje mobilnih naprav omogočajo tudi lociranje naprave na daljavo, kot

sistem avtentikacije in identifikacije pa tudi prepoznavo prstnih odtisov. Nedorečeni organizacijski ukrepi prav tako lahko vodijo v nedopustne posege v pravice zaposlenih (npr. postopki ob prekinutvi delovnega razmerja in s tem povezan umik dostopnih pravic in brisanja podatkov).

Delodajalec, ki dopušča BYOD naprave v svojem okolju, mora zato zelo previdno in jasno ter vnaprej določiti **meje med zasebno in službeno uporabo ter politike dostopa do različnih podatkov**.

Če je delodajalec omejen pri zbiranju osebnih podatkov zaposlenih, je toliko bolj **omejen pri zbiranju osebnih podatkov oseb, ki niso njegov zaposleni**, lahko pa uporabljajo BYOD napravo (npr. otroci zaposlenega, drugi družinski člani...). Za zbiranje in obdelavo njihovih osebnih podatkov praviloma ne bo možno najti pravne podlage, saj bi bila tudi njihova privolitev kot družinskih članov zaposlenega zelo vprašljiva. Nekatere od teh težav že rešujejo sistemi za upravljanje mobilnih naprav.



3.2 TVEGANJA GLEDE ZAVAROVANJA OSEBNIH PODATKOV

Tveganja z vidika informacijskega varnosti so pri dopuščanju BYOD naprav številna in raznovrstna, izhajajo pa iz naslednjih dejavnikov:

- stalna prisotnost, povezanost in mobilnost naprave - tudi izven službenega okolja;
- široka uporaba naprave – za zasebne in službene namene:
 - komunikacija, socialna omrežja, upravljanje multimedijskih vsebin, telefoniranje, sporočila,
 - sinhronizacija imenikov,
 - sinhronizacija dokumentov,
 - nameščanje aplikacij in druge programske opreme,
 - posojanje naprave drugim osebam;
- mešanje uporabe in nadzora:
 - varnostna (ne)ozaveščenost uporabnikov,
 - uporabnik je "administrator" naprave z vsemi pravicami,
 - omejevanje uporabe naprave je mogoče le s posebnimi programi.

Poleg v prejšnji točki opisanih tveganj za poseg v zasebnost uporabnikovih podatkov je torej treba identificirati **tveganja**, ki nastajajo zaradi uporabe BYOD naprave **glede zbirk osebnih podatkov, ki jih vodi organizacija**, oz. širše, **glede informacijskih sistemov organizacije, do katerih bo preko takšne naprave omogočen dostop**. Nedorečena varnostna politika, zanemarjanje tveganj glede nameščenja aplikacij, nepooblaščenih dostopov itd. lahko namreč ogrozijo varnost osebnih podatkov v zbirkah osebnih podatkov, ki jih vodi organizacija, oz. varnost drugih zaupnih poslovnih informacij. V skrajnem primeru bi se organizacije zaradi dopuščanja uporabe BYOD naprav lahko znašle celo v postopku zaradi **kršitev zakonodaje o varstvu osebnih podatkov**, oziroma bi ogrozile zaupnost lastnih poslovnih informacij.

Na BYOD naprave zaposleni pogosto nameščajo in nadgrajujejo aplikacije po lastni presoji, ki so na prvi pogled sicer nenevarne, a ob nezadostnem ločevanju poslovnega in zasebnega lahko omogočijo dostop do zaupnih podatkov (osebnih podatkov, poslovnih skrivnosti ipd.) tretjim osebam (npr. razvijalcem aplikacij in operacijskih sistemov, ponudnikom oglaševanja, ponudnikom storitev). Naprave, kot so prenosniki, tablice in pametni telefoni - zasebni toliko bolj kot službeni - so vsepovsod z nami, in so vsakodnevno predmet izgub in kraji, s tem pa so ogroženi tudi podatki od organizacije.

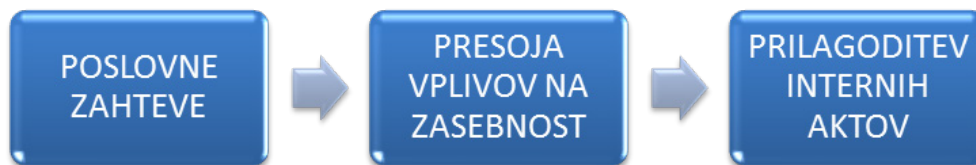
Mednarodna delovna skupina za varstvo osebnih podatkov v telekomunikacijah (IWGDPT) v nedavnem delovnem dokumentu na temo zasebnosti in varnosti pri uporabi BYOD naprav v službenih okoljih¹⁰ opozarja na naslednja tveganja glede informacijske varnosti:

- za razliko od službenih naprav je pri BYOD napravah težko prilagoditi obstoječe operacijske sisteme v smeri večje varnosti in s tem povodom omejene uporabnosti;
- BYOD naprave pogosto uporabljajo manj varne povezave v različnih okoljih, vključno z javnimi lokacijami;
- uporabljane aplikacije in mrežna infrastruktura morda ne morajo zagotoviti varnega dostopa s strani BYOD naprav;
- obstoječe politike dopustne rabe službenih sredstev ne naslavlja ustrezno uporabe BYOD naprav;
- uporabniki svoje zasebne naprave delijo z drugimi uporabniki;
- določene storitve, kot je avtomatsko izdelovanje varnostnih kopij ali ostala programska oprema, lahko povzročijo nenačrtovano in neodobreno uporabo oblačnih storitev;
- uporabniki lahko svoje naprave izpostavljajo večjim varnostnim tveganjem kot pri službenih napravah (npr. zaradi možnosti nameščenja aplikacij);
- podatki z naprav se ob zavrženju ali nadaljnji predaji naprave ne pobrišejo ustrezno;
- nesorazmerna uporaba rešitev za upravljanje mobilnih naprav se lahko odrazi v nezakonitem zbiranju podatkov o zaposlenih in drugih uporabnikih naprave.

¹⁰ https://datenschutz-berlin.de/attachments/1082/675.49.10_WP_Own_Devices.pdf?1419853968

4. BYOD – ZAKONITO IN VARNO

Kako torej zakonito in varno uporabljati BYOD? Uvedba naj sledi naslednjih korakom:



4.1. DEFINIRANJE POSLOVNIH ZAHTEV

Pred vpeljavo BYOD oziroma MDM sistemov je ključno, da se opravi premislek o **poslovnih potrebah oziroma zahtevah**, ki jih sploh zasleduje delodajalec. Poslovne potrebe oziroma zahteve je treba definirati, gre pa za odgovore na vprašanja, kot so **KAJ ŽELIMO DOSEČI**, npr.:

- zaposlenim želimo omogočiti dostop do elektronske pošte, dokumentnega sistema, oz. zalednega spletišča (intraneta); tj. dostop do informacij, ki jih potrebujejo za vsakdanje delo;
- zaposlenim želimo omogočiti širši dostop do službenega omrežja in tam dosegljivih storitev (v smislu VPN);
- zaposlenim želimo omogočiti uporabo namenskih mobilnih aplikacij za opravljanje dela neposredno z mobilne naprave.

Od stopnje dostopa do službenih podatkov, ki jih bodo imeli zaposleni preko svojih BYOD naprav, so potem odvisni želeni varnostni cilji:

- želimo imeti šifriranje podatkov med prenosom in podatkov v hrambi;
- za prijavo v službeni način delovanja želimo prijavo s PIN ali geslom (ne pa npr. s kretnjo oziroma gestami);
- želimo, da naprava uporablja operacijski sistem _____ verzije _____ ali višje in da je varovana z antivirusnim programom _____;
- želimo preprečiti kopiranje poslovnih podatkov iz službenih aplikacij v zasebne aplikacije (npr. Facebook, Twitter, Gmail...);
- želimo imeti možnosti brisanja poslovnih podatkov na mobilnih napravah brez brisanja celotne naprave na daljavo (npr. ob kraji ali izgubi mobilne naprave);
- želimo imeti inventar strojne in programske opreme (verzije operacijskih sistemov in aplikacij ...).
- itd.

...kakor tudi **ČESA NE ŽELIMO DOSEČI**, npr:

- povečati tveganja za izgubo nezaščitene naprave, ki ima dostop do naših poslovnih podatkov;
- ne želimo uporabljati lokacijskih storitev, beležiti dostopov do podatkov o uporabi različnih omrežij (SSID);
- ne želimo spremljati zgodovine klicev ali poslanih sms sporočil;
- ne želimo imeti dostopa do zasebnih sporočil, zasebnih aplikacij in zasebnih dokumentov uporabnika;
- itd...

Ko bomo enkrat dobro definirali poslovne zahteve, bomo toliko lažje poiskali rešitve, s pomočjo katerih bodo naše poslovne zahteve realizirane skladno z zakonodajo.

Delodajalec, ki dopušča BYOD naprave v svojem okolju, mora zelo previdno in jasno določiti **meje med zasebno in službeno uporabo** ter **politike dostopa do različnih podatkov**. Pri tem mora predhodno skozi presojo vplivov na zasebnost celovito analizirati, ali obstajajo glede na definirane zahteve kakšna tveganja za nezakovitosti.

Pred uvedbo **BYOD** in **MDM** rešitev je zato priporočljivo v naslednjih korakih:

1. **izvesti** presojo vplivov na zasebnost (**PIA**), t.j. **analizo tveganj po temeljnih načelih varstva osebnih podatkov**.
2. Podobno kot pri drugih segmentih nadzora nad uporabo elektronskih sredstev je **na podlagi PIA** uporabo BYOD in MDM priporočljivo **vnapij opredeliti v internih aktih**.

Kako izvesti presojo vplivov na zasebnost in kaj je treba opredeliti v internih aktih?

Gre za **analizo tveganj po temeljnih načelih varstva osebnih podatkov**, njen rezultat pa je priporočljivo v pisni obliki: glej [SMERNICE O PRESOJAH VPLIVOV NA ZASEBNOST](#).

4.2. IZVEDBA PRESOJE VPLIVOV NA ZASEBNOST (PIA)

V nadaljevanju opisujemo, katera vprašanja naj bi PIA obravnavala na primeru uvedbe BYOD.

4.2.1. Zakonitost

Za osebne podatke, ki se bodo zbirali pri uporabi BYOD oz. MDM rešitev, moramo imeti pravno podlago (glej 8. oz. 9. in 10. člen ZVOP-1). Neposredne zakonske podlage za uporabo BYOD/MDM rešitev praviloma ne bomo našli, zato bo pravna podlaga podana kvečjemu v:

- **Zakonu o delovnih razmerjih (ZDR-1), ki določa:**
 - **48. člen (varstvo delavčevih osebnih podatkov)**
(1) Osební podatki delavcev se lahko zbirajo, obdelujejo, uporabljajo in posredujejo tretjim osebam samo, če je to določeno s tem ali drugim zakonom ali če je to potrebno zaradi uresničevanja pravic in obveznosti iz delovnega razmerja ali v zvezi z delovnim razmerjem.
- **4. odstavku 9. člena ZVOP-1 oziroma 3. odstavku 10. člena ZVOP-1** (prevladujoči interesi) oziroma v
- **privolitvi posameznika ob upoštevanju spodaj navedenih omejitev.**

Pri tem se moramo glede privolitve zaposlenih zavedati, da:

- je **veljavnost privolitve v delovno-pravnih razmerjih vprašljiva**, saj je zaposleni praviloma šibkejša stranka in je njegovo »privolitev« mogoče izsiliti;
- če se zanašamo na privolitev mora biti ta **neizsiljena, prostovoljna izjava volje zaposlenega, informirana in aktivno podana**; zaposleni, ki ne da privolitve, ne sme trpeti negativnih posledic – takšne so tudi usmeritve glede privolitve v Splošni uredbi o varstvu osebnih podatkov (General Data Protection Regulation), katere predvidena veljavnost je od leta 2018 naprej.

V tesni povezavi z načelom zakonitosti je tudi načelo transparentnosti oz. informiranja uporabnikov – zaposleni morajo biti obveščeni o temu:

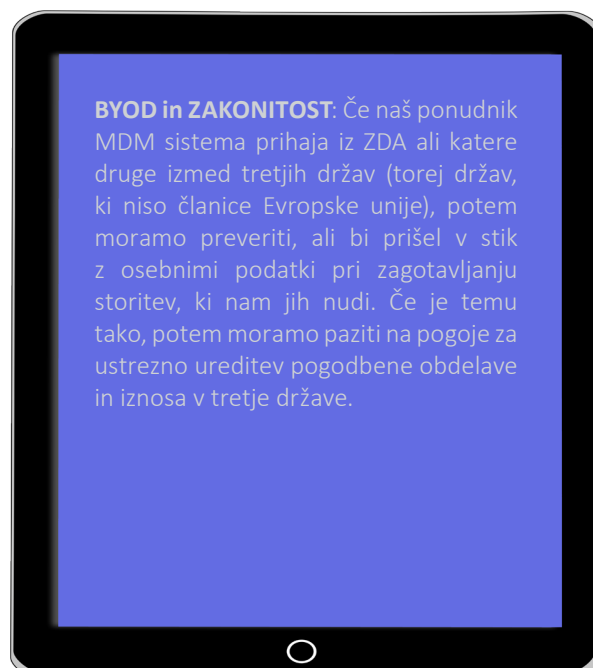
- **kateri podatki** se bodo zbirali oziroma obdelovali (npr. ali bo delodajalec vodil popis nameščenih aplikacij, ali je predviden dostop do zasebnih datotek ipd.),
- za **katere namene** se bodo obdelovali.

Navedeno ima vpliv tudi na **utemeljenost pričakovanja**

zasebnosti, ki je v sodni praksi¹¹ ključni test v naknadnih presojah, ali je bila obdelava osebnih podatkov s strani delodajalca upravičena in zakonita ali ne. Netransparentna ali prikrita obdelava osebnih podatkov, o kateri zaposleni niso vnaprej natančno in pošteno obveščeni, se je v sodni praksi izkazala kot izrazito problematična.

Pozornost velja tudi ustrezni ureditvi oziroma izpolnjevanju pogojev glede:

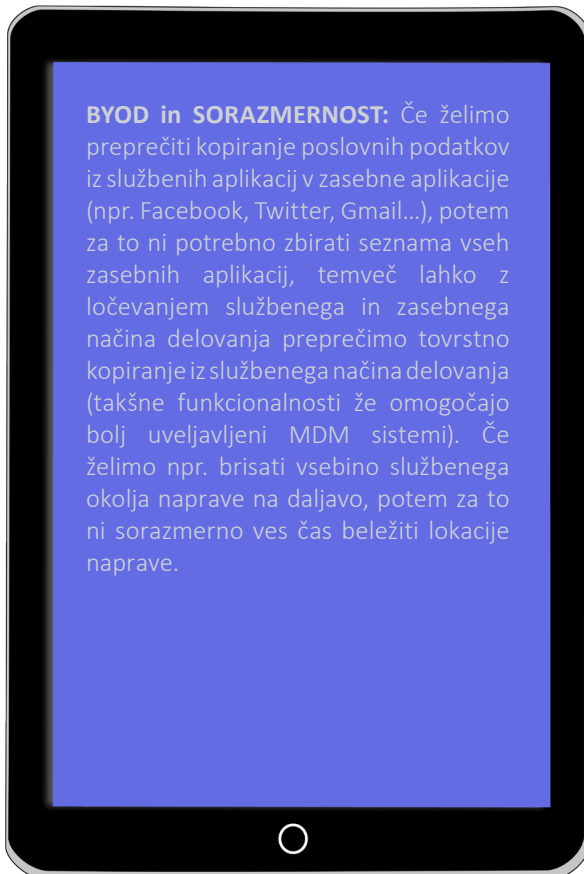
- a) **pogodbene obdelave osebnih podatkov**, npr. če najemate pogodbene obdelovalce, kot je zunanji ponudnik MDM rešitev, ki med zagotavljanjem storitev pride v stik z osebnimi podatki: glej [SMERNICE O POGODBENI OBDELAVI](#);
- b) **iznosa v tretje države** – če je zunanji ponudnik MDM rešitev, ki med zagotavljanjem storitev pride v stik z osebnimi podatki, iz tretje države: glej [SMERNICE O IZNOSU V TRETJE DRŽAVE](#);
- c) **morebitne obvezne uporabe biometrijskih načinov avtentikacije in identifikacije** (npr. odklepanje naprave s čitalnikom prstnih odtisov): glej [SMERNICE O BIOMETRIJI](#);



¹¹ Glej npr. sodbe evropskega sodišča v zadevah (Halford proti Združenemu kraljestvu (20605/92), Copland proti Združenemu kraljestvu (62617/00), Köpke proti Nemčiji (420/07), Bărbulescu proti Romuniji (61496/08)), kasacijskega sodišča Francije (Societe Nikon France, SA proti Onof iz leta 2001, Bruno B proti Giraud et Migot, 2009, M. X. proti Young & Rubicam France, 2013) ter sodbe Vrhovnega in Ustavnega sodišča RS.

4.2.2. Sorazmernost

Pred uvedbo BYOD moramo – kot smo že izpostavili – izhajati iz poslovnih potreb. Načelo sorazmernosti nam tu nalaga, da premislimo, kateri osebni podatki so res nujni in brez katerih lahko dosežemo cilje oziroma se jim lahko izognemo.

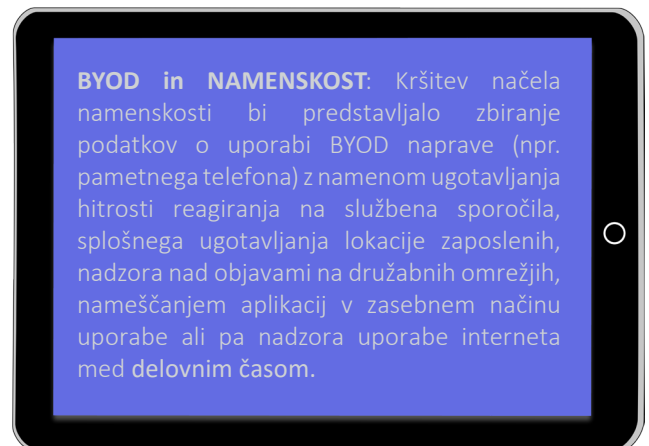


Z upoštevanjem načela sorazmernosti se izognemo nepotrebnim tveganjem, saj se s povečanjem obsega in intenzitete osebnih podatkov povečujejo tudi naše dolžnosti glede ustreznega zavarovanja teh podatkov, že v začetku pa moramo imeti za njihovo zbiranje pravno podlago. **Vprašati se torej moramo, kateri podatki o uporabi naprave se res nujni v kontekstu BYOD in zbirati samo tiste.**

4.2.3. Namenskost

Vsaka obdelava osebnih podatkov naj bi potekala samo za vnaprej določene namene. Uporaba osebnih podatkov za druge namene je v nasprotju za zakonom. Pri uvedbi BYOD moramo razmisliti, za katere namene bodo zbrani določeni podatki, te namene pa moramo jasno predstaviti uporabnikom BYOD naprav. Jasna

opredelitev namenov je koristna tudi iz razloga, da ne prihaja do naknadnega širjenja namenov in uporabe za nekompatibilne namene.



4.2.4. Točnost in ažurnost

Osebni podatki, ki jih upravljavci vodijo v svojih zbirkah osebnih podatkov, morajo biti točni in ažurni – govorimo konkretno o podatkih, ki jih vodi delodajalec, ki se odloča za morebitno uvedbo BYOD. Če so poslovne zahteve takšne, da naj bi uporabniki prek BYOD naprav lahko tudi **vnašali ali spreminjali osebne podatke v zbirkah podatkov, ki jih vodi organizacija** (npr. posodabljali statuse pri naročnikih, vnašali podatke o poslih, fizičnih osebah ipd.), potem je treba zagotoviti **ustrezno sinhroniziranje in celovitost podatkov**, da ne bi prišlo do težav s podvajanjem podatkov, netočnostjo podatkov in drugimi nevšečnostmi. Pred uvedbo BYOD je tako treba preveriti, kakšni so postopki sinhronizacije in varnostnega kopiranja podatkov.

4.2.5. Pravice posameznika

Posameznik ima pravico do seznanitve z lastnimi osebnimi podatki, kakor tudi pravico do dopolnitve, popravka in ugovora (glej člen 30. ZVOP-1 in dalje). Če se z uvajanjem BYOD zbirajo dodatni osebni podatki zaposlenih, potem mora biti uporabnik s tem seznanjen, posledično pa lahko uveljavlja svoje pravice (npr. zahteva seznanitev z osebnimi podatki, ki so bili o njemu zbrani pri uporabi BYOD, kot so npr. MAC in IP naslovi, morebitna imena naprav, SSID omrežij, na katere se povezuje naprava itd.).

4.2.6. Roki hrambe

Glede rokov hrambe moramo – kot tudi sicer – ločiti med različnimi podatki:

- a) osebni podatki v zbirkah osebnih podatkov

- organizacije (strank, naročnikov, in drugih fizičnih oseb, ki jih vodi organizacija in podatki o dostopih do njih s strani uporabnikov,
- b) osebni podatki uporabnika, ki se beležijo ob uporabi BYOD naprave.

Roki hrambe podatkov pri točki a) niso odvisni od uporabe BYOD, določa jih zakonodaja ali organizacija sama in tudi uvedba BYOD praviloma ne bi smela vplivati na te roke.

Glede rokov hrambe podatkov, ki so specifični in nastajajo predvsem ob uporabi BYOD, npr. podatki o zbranih IP in MAC naslovih, morebitnih nazivih naprave ipd., če se zbirajo, pa je priporočljivo **roke hrambe teh podatkov vnaprej določiti glede na namene z upoštevanjem načela sorazmernosti** – hranili naj bi se samo toliko časa, kot je to potrebno **glede na namene uporabe BYOD**, sami nameni pa izvirajo iz poslovnih zahtev za uvedbo BYOD.

4.2.7. Zavarovanje (informacijska varnost)

Izzivi informacijske varnosti so med najpomembnejšimi tveganji, ki jih moramo obravnavati pri uvajanju BYOD. Tveganja glede zavarovanja oziroma informacijske varnosti smo že navedli, v okviru PIA pa moramo predvideti tudi ustrezne ukrepe za obravnavo varnostnih tveganj. Različni MDM sistemi že vsebujejo širok nabor varnostnih funkcionalnosti v te namene.

Med **primere dobrih praks** sodijo:

- Ločevanje poslovnega in zasebnega načina delovanja.
- Zaklepanje mobilne naprave (uporaba vzorca se odsvetuje pri dostopu do poslovnega dela).
- Zaklepanje določenih aplikacij s kodami (npr. pri dajanju telefona otrokom).
- Poslovni del:
 - nadzor nad uporabo in dostopi do poslovnih podatkov,
 - kjer je mogoče uporabljati šifriranje poslovnih podatkov,
 - varno brisanje podatkov iz poslovnega dela,
- uporaba samo preverjenih in vnaprej odobrenih aplikacij in programske opreme ter omejitve glede nameščanja aplikacij z neuradnih programskih trgov,
- detekcija prevzema nadzora nad napravo (angl. jailbreak, root) in izogibanja vsiljenim varnostnim rešitvam,
 - uporaba programske opreme za zaščito mobilne naprave,
 - izogibanje nekriptiranim povezavam.

Varnostni postopki in ukrepi morajo biti **opredeljeni v internih aktih organizacije**, kar je tudi naslednji korak pri uvajanju BYOD.

4.3. PRILAGODITEV INTERNIH AKTOV

Po definiranju poslovnih zahtev in izvedeni presoji vplivov na zasebnost je treba opraviti ustrezne prilagoditve internih aktov organizacije (varnostne politike, pravilniki, navodila.). Ključni vsebinski elementi, ki jih morajo »pokriti« spremembe internih aktov ob uvajanju BYOD, so:

- a) informiranost uporabnikov,
- b) zakonitost obdelav osebnih podatkov ter
- c) informacijska varnost.

Poslovne zahteve in zaključki PIA se morajo odraziti v določbah internih aktov tako, da je jasno, čemu se uvaja BYOD.

Zaposlene je treba vnaprej jasno obvestiti **o vseh vidikih, ki imajo lahko vpliv na raven varnosti osebnih podatkov, ki jih zbira organizacija, oziroma ki vplivajo na raven pričakovane zasebnosti, ki jih glede zasebnega načina pričakuje uporabnik.** Uporabniki morajo zato biti vnaprej nedvoumno in natančno obveščeni o:

- dopustni rabi spleta, e-pošte, uporabe tržnic aplikacij, nameščanja aplikacij,
- obsegu zbiranja podatkov, namenih in postopkih, kot so:
 - možnosti lociranja mobilnih naprav;
 - načinih ločevanja med službenimi in zasebnimi načini delovanja ter varnostnimi postopki v povezavi s tem (npr. zahteve po vnosu PIN);
 - obsegu beleženja dogodkov in varnostnega kopiranja;
 - upravljanju incidentov (npr. postopki ob kraji ali izgubi BYOD naprave) in uporabi ostalih varnostnih mehanizmov (npr. možnosti brisanja podatkov, zaklepanja naprave na daljavo);
 - odgovornosti za varnost BYOD naprav;
 - postopkih »razdolževanja« opreme (kako se ob prekinitvi delovnega razmerja oz. prenehanju uporabe BYOD naprave onemogoči dostop do poslovnih podatkov in izbrišejo podatki, shranjeni v poslovnem delu/ načinu uporabe).

IWGDPT opozarja, da je treba **varnostne politike pred uvedbo BYOD dopolniti**, tako da ustrezno pokrivajo naslednje postopke in ukrepe:

- varna avtentikacija uporabnikov in varnost komunikacij pri dostopu z BYOD naprav;
- nadgradnja varnosti aplikacijskih sistemov, ki bodo dostopni z BYOD naprav;
- nadgradnja komunikacijske infrastrukture, da bo ta

- zagotavljala »end-to-end« šifriranje komunikacij;
- vzpostavitev in redno vzdrževanje registra odobrenih BYOD naprav in uporabnikov teh naprav;
- opredelitev postopkov za takojšnji odvzem dostopnih pravic v primeru prekinitve delovnega razmerja ali prenehanje potrebe po dostopu;
- opredelitev postopkov za redno izvajanje varnostnih kopij poslovnih podatkov, ki se hranijo na BYOD napravah;
- opredelitev postopkov za oddaljeno brisanje poslovnih podatkov, ki se hranijo na BYOD napravah;
- dodatno izobraževanja uporabnikov BYOD naprav glede varnostnih tveganj;
- izolacija BYOD naprav v ločeno omrežje;
- implementacija, testiranje in validacija tehničnih ukrepov, kot so požarni zidovi in t.i. sandboxing z namenom preprečevanja nepooblaščenih dostopov do poslovnih podatkov ob upoštevanju pravic do zasebne rabe BYOD naprave;
- ustrezen, primeren in sorazmeren nadzor nad varnostnimi elementi na BYOD napravi ob upoštevanju pravice uporabnikov do zasebnosti;
- opredelitev postopkov za potrjevanje skladnosti BYOD naprav z naprej določenimi varnostnimi zahtevami organizacije (npr. verzija operacijskega sistema, tipi naprav, zahtevani načini avtentikacije in avtorizacije, uporaba šifriranja in zaščite pred zlonamerno kodo);
- opredelitev postopkov za odkrivanje in preprečevanje (ne pa tudi nadzora same) uporabe programske opreme, katere uporaba ni dovoljena v varnostnih politikah organizacije (npr. aplikacije za P2P deljenje datotek).

S pravili je treba zaposlene **vnaprej seznanimi**, pravila morajo biti **enostavno dostopna** (npr. na intranetu) in **ažurna**.

5. POGOSTA VPRAŠANJA

Q: Ali se lahko delodajalec seznani z zasebnim delom naprave, ki jo zaposleni uporablja (tudi) v službene namene oziroma s čim in pod kakšnimi pogoji?

Pri uporabi BYOD se mora delodajalec izogibati vsakršnemu dostopu do zasebnega dela ali zasebnega načina delovanja naprave, kot npr. do podatkov:

- kdo je kdaj koga klical,
- katere spletne strani je obiskoval,
- s kom, kdaj in kaj je komuniciral,
- kje in kdaj se je gibal.
- ter zasebni korespondenci, datotekam in aplikacijam zasebne narave,

Ob upoštevanju korakov uvedbe BYOD posledično priporočamo uporabo MDM rešitev, ki omogočajo striktno ločevanje poslovnega in zasebnega dela. Problematično je lahko tudi zbiranje informacij o naloženih aplikacijah ter izbris na daljavo, kadar je prevečkrat vnesen napačen PIN. Imena mnogih aplikacij lahko kažejo na popolnoma zasebno sfero zaposlenega in celo na občutljive osebne podatke (npr. na zdravstvene težave, na zasebne aktivnosti, na spolno usmerjenost ipd). Zbiranje takih informacij s strani delodajalca ni potrebno in primerno za izvajanje pogodbe o zaposlitvi kot to določa ZDR-1.

Q: Ali lahko v varnostni politiki opredelimo postopek, da se v primeru izgube ali kraje BYOD naprave zaradi nujnosti varovanja poslovnih informacij pobriše vsebina celotne naprave in da se uporabnik tega mora zavedati oz. da s tem soglaša? Z določbami varnostne politike bi zaposlene vnaprej seznanili, novo zaposleni pa ob prihodu podpišejo izjavo o seznanjenosti z internimi akti podjetja.

Izbris celotne naprave na daljavo prav tako pomeni obdelavo osebnih podatkov, ki se nahajajo na napravi (njihov izbris), zadeva pa lahko vse osebne podatke, ki jih uporabnik hrani (npr. fotografije, video posnetke, dokumente, druge osebne podatke) in ne samo tiste, ki so na napravi in so z zvezi z delovnim razmerjem. Pravne podlage za tako obdelavo osebnih podatkov po mnenju Informacijskega pooblaščenca delodajalec nima¹², s takšnim dejanjem pa bi se lahko izpostavil tudi tožbam s strani zaposlenega, ki so mu bili pobrisani zanj zelo pomembni zasebni podatki in datoteke. Določba v internem pravilniku delodajalca v tem primeru pred tem ne more obvarovati, zato raje priporočamo, da se uporabijo takšne rešitve, ki omogočajo striktno

ločevanje poslovnega in zasebnega dela in obenem omogočajo izbris samo poslovnega dela na daljavo.

Q: Ali smemo zahtevati, da uporabnik na svoji napravi uporablja vnos PIN in ne kretnje, kot jih je sicer navajen, če želi uporabljati zasebno napravo tudi za dostop do službenih aplikacij? Ali smemo beležiti inventar strojne opreme in beležiti sumarne statistike o prenosu podatkov (npr. koliko GB je prenesel k sebi v določenem mesecu)?

Sama opredelitev zahteve po vnosu PIN po mnenju Informacijskega pooblaščenca ni sporna, saj ima delodajalec pravico postaviti pogoje, pod katerimi dopušča uporabo zasebnih sredstev v službene namene. Prav tako se nam ne zdi sporen inventar strojne opreme in sumarni podatki o prenosu podatkov.

Q: Zaposlenim dovoljujemo, da uporabljajo svoje pametne telefone tudi za dostop do službene e-pošte. Ali lahko blokiramo ali omejimo uporabo zasebnih aplikacij na teh napravah, kot sta npr. Facebook in Twitter, da ne bi uporabniki v takšna omrežja kopirali podatkov iz službene e-pošte?

Zavedati se morate, da so te naprave primarno še vedno zasebne naprave in da zgolj zato, ker ste zaposlenim na njih omogočili dostop do določenih službenih virov, še niso enakovredne službenim napravam, zato tudi nimate pravice blokirati ali omejevati dostopa do zasebnih aplikacij (čeprav je te tehnično mogoče), razen če so se tudi zaposleni s tem strinjali ob vnaprej določenih pogojih in situacijah in v to niso bili nikakor prisiljeni (glej str.14 glede privolitve). Pri tem poudarjamo, da gre za *strinjanje z blokado*, ne pa za *strinjanje z nadzorom uporabe*, za kar privolitev zaposlenih ne bo primerna podlaga.

¹² Podrobnejša obrazložitev v mnenju št. 0712-1/2015/1113, dostopno na: https://www.ip-rs.si/vop/uporaba-sistema-za-upravljanje-mobilnih-naprav-2568/?tx_jzvopdecisions_pi1

6. ZAKLJUČEK

Vedno večje potrebe po mobilnosti in dosegljivosti zaposlenih bodo številne organizacije postavile pred vprašanja, ali dopustiti uporabo zasebnih naprav v službene namene in kako delavcem omogočiti čim večjo dostopnost do poslovnih podatkov, aplikacij in sistemov. Tehnološke rešitve omogočajo tako vključevanje zasebnih naprav v poslovna okolja kot nabor funkcionalnosti, s katerimi rešujemo težave glede ločevanja zasebne in službene uporabe ter številne varnostne izzive. Pri uvajanju BYOD se moramo zavedati, da ne gre zgolj za tehnološke izzive, temveč za preplet pravnih, kadrovskih in organizacijskih tveganj. Če jih nismo sposobni ustrezno identificirati ter obvladovati, se postavlja vprašanje, ali smo pripravljeni sprejeti posledice nepremišljenih odločitev.

Morebitno uvajanje BYOD mora potekati premišljeno in – kot smo opisali v smernicah – izhajati iz natančnega definiranja poslovnih zahtev, opravljene analize tveganja in presoje vplivov na zasebnost ter z ustreznimi prilagoditvami internih politik in aktov. V nasprotnem primeru lahko ogrozimo varnost naših poslovnih informacij, osebnih podatkov naših strank ter zasebnost in zaupanje naših zaposlenih.

