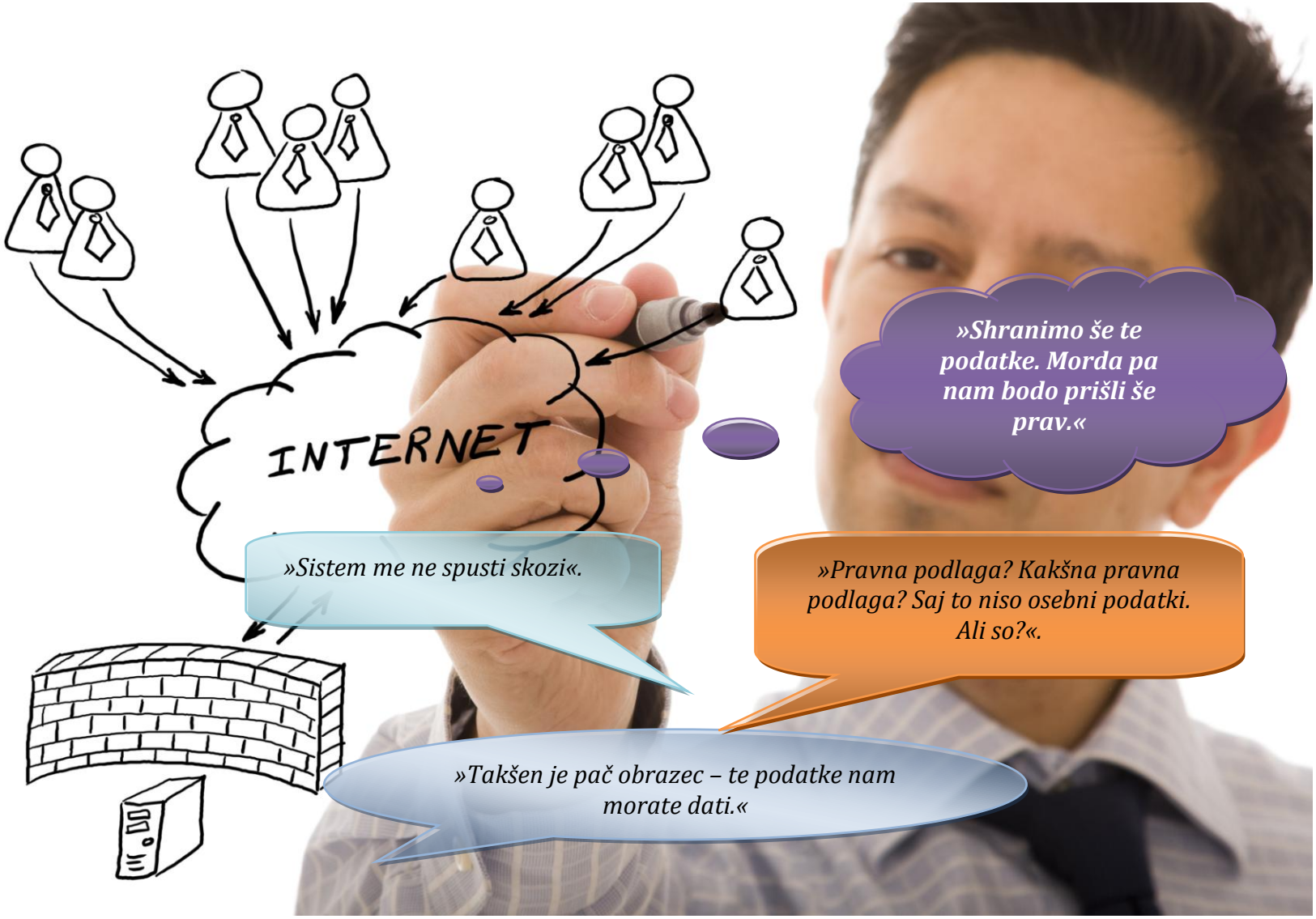
Presoje vplivov na zasebnost pri projektih eUprave

Smernice Informacijskega pooblaščenca

INFORMACIJSKI POOBLAŠČENEC



Namen dokumenta:	Namen smernic je predstaviti mehanizem presoj vplivov na zasebnost (angl. Privacy Impact Assessment) kot orodja za identifikacijo, analizo in zmanjševanje tveganj nezakonitih ravnanj z osebnimi podatki s poudarkom na uporabi v okviru strategij razvoja eUprave.
Ciljne javnosti:	Snovalci politik, upravljavci zbirk osebnih podatkov, razvijalci storitev, ponudniki IKT storitev in ostali deležniki strategij razvoja eUprave.
Status:	Javno
Verzija:	1.0
Datum izdaje:	22.7.2010
Avtorji:	Informacijski pooblaščenec
Ključne besede:	Smernice, presoje vplivov na zasebnost, PIA, PVZ, vgrajena zasebnost, osebni podatki, povezovanje, Privacy by Design, eUprava, SREP.

KAZALO

O SMERNICAH INFORMACIJSKEGA POOBLAŠČENCA

Namen smernic IP je podati praktične in razumljive napotke za posameznike, katerih osebni podatki (OP) se obdelujejo, ter za pravne in druge osebe, ki upravljajo z zbirkami osebnih podatkov glede na določbe Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju ZVOP-1).

Pravno podlago za izdajo smernic Pooblaščencu 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: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/
- Brošure IP: http://www.ip-rs.si/publikacije/prirocniki/

Smernice IP so objavljene na spletni strani: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/

UVOD

Junija 2009 je bila sprejeta **Strategija razvoja elektronskega poslovanja ter izmenjave podatkov iz uradnih evidenc – SREP**, katere namen je določitev okvira in ciljev za nadaljnje uresničevanje novih in že zastavljenih dejavnosti razvoja elektronskega poslovanja v javni upravi. SREP v poglavju, ki se nanaša na zagotavljanje horizontalnih funkcij, predvideva pripravo skupnih metodologij in politik (poglavje 6.5.4), med katerimi je predvidena tudi priprava **metodologije z izvedbo presoj vplivov na zasebnost**.

Izboljševanje učinkovitosti delovanja javnega sektorja in razvoj storitev eUprave terjata od države čedalje obsežnejše in intenzivnejše povezovanje podatkovnih virov, s katerimi upravlja javni sektor, med katerimi so tudi obsežne zbirke osebnih podatkov, pri tem pa se država hitro znajde v precepu in tehtanju med izpolnjevanjem svojega poslanstva in spoštovanjem temeljnih človekovih pravic s poudarkom na varovanju zasebnosti posameznika pred prekomernimi in nezakonitimi posegi državne administracije. Pri številnih projektih informatizacije, povezovanja podatkovnih virov, razvoja novih storitev in ne nazadnje pri predlogih sprememb zakonodaje je upoštevanje varstva zasebnosti in osebnih podatkov zanemarjeno in se šele naknadno v inšpekcijskem nadzoru odkrijejo nepravilnosti in nezakonitosti. Odprava nepravilnosti in prevzemanje odgovornosti zanje lahko terjata visoke stroške, izgubo časa in ugleda. Presoje vplivov na zasebnost so orodje, s katerim se lahko izognemo takšnim situacijam.

Presoje vplivov na zasebnost so se izkazale kot učinkovito orodje, s katerim lahko **pravočasno identificiramo tveganja in zahteve**, ki jih glede obdelave osebnih podatkov določa zakonodaja, in se na ta način izognemo kršitvam zakonodaje, izgubi ugleda in ne nazadnje neučinkoviti in nesmotrni porabi sredstev. Presoje vplivov na zasebnost so lahko zelo dolgotrajne in administrativno zahtevne, vendar je po mnenju Pooblaščenca treba uravnovesiti in

optimizirati učinkovitost takšnega orodja s potrebnimi vložki in administrativnimi bremeni. Smernice Informacijskega pooblaščenca so zato kratke, jedrnate in osredotočene na učinkovitost in minimizacijo potrebnih sredstev za izvedbo.

PRVO POGLAVJE – KAJ JE PRESOJA VPLIVOV NA ZASEBNOST

Presoja vplivov na zasebnost (angl. Privacy Impact Assessment – PIA[1] oz. PVZ) je orodje za identifikacijo, analizo in zmanjševanje tveganj glede nezakonitih ravnanj z osebnimi podatki, do katerih lahko pride pri določenem projektu, sistemu ali uporabi tehnologije. Tovrstne presoje so bolj uveljavljene v okoljih, kjer je zakonodajni in nadzorni poudarek na varstvu zasebnosti (angl. privacy) in ne toliko na varstvu osebnih podatkov (angl. data protection). Presoje vplivov na zasebnost so tako pogosto uporabljeno (in včasih tudi obvezno) orodje pri snovalcih zakonodaje, politik in projektov v Kanadi, Avstraliji in ZDA, počasi pa si utirajo pot tudi v evropskem prostoru, kjer je večji poudarek na varstvu osebnih podatkov[2]. Uporabljajo se tako v javnem kot v zasebnem sektorju, kjerkoli pa so bile uvedene, se se tudi uveljavile in obstale.

PVZ temeljijo na sistematični in pravočasni identifikaciji tveganj za nezakonita ravnanja z osebnimi podatki, s katerimi se lahko tveganja pravočasno identificira in tudi lažje odpravi, zmanjša ali sprejme. Po eni strani so PVZ podobne inšpekcijskemu nadzoru zakonitosti obdelave osebnih podatkov po ZVOP-1, ki ga izvaja Informacijski pooblaščenec in kjer je poudarek na ugotavljanju skladnosti z ZVOP-1, medtem ko je namen PVZ predhodna analiza tveganj in optimizacija postopkov za doseganja zakonske skladnosti.

Zakaj so PVZ koristne?

Informacijski pooblaščenec se je v praksi pogosto znašel v situaciji, ko je v teku inšpekcijskega nadzora odkril nepravilnosti in kršitve zakona, do katerih ne bi prišlo, če bi zavezanec (upravljavec ali pogodbeni obdelovalec osebnih podatkov), pred izvedbo določnega projekta ali uporabo določene tehnologije pravočasno izvedel PVZ in tako sam zmanjšal tveganje za nastanek nezakonitosti ali takšno tveganje v celoti izničil.

Pomen in učinkovitost PVZ narašča z velikostjo in intenzivnostjo obdelave osebnih podatkov v projektu, pri čemer lahko za »projekt« štejemo:

- spremembo zakonodaje,
- uvedbo, povezovanje ali razvoj novih informacijskih rešitev,
- konkretno uporabo določene tehnologije,
- razširitev namena obdelave že zbranih osebnih podatkov ali načina obdelave (npr. izvoz podatkov),
- drugo pomembno spremembo v poslovnem okolju s pomembnejšim vplivom na varstvo osebnih podatkov.

[1] Več o zgodovinskem ozadju in značilnostih PVZ: http://www.rogerclarke.com/DV/PIAHist-08.html.
[2] Zlasti po uveljavitvi Direktive 95/46 ES o varstvu osebnih podatkov.

Marsikdaj je namreč mogoče cilje projekta doseči na način, ki ne zahteva obdelave osebnih podatkov, ali pa z manjšo količino in težo osebnih podatkov oziroma z upoštevanjem koncepta vgrajene zasebnosti (angl. Privacy by Design) poskrbeti za skladnost s temeljnimi načeli in zahtevami zakona. «Zberimo še te podatke – nam bodo že kdaj prišli prav!«, ali pa »Nič ne bomo brisali podatkov, kaj veš, kdaj jih bomo še potrebovali.« in »Tehnologija omogoča zbiranje in obdelavo teh podatkov, torej moramo to tudi izkoristiti.«, so klasična napačna razmišljanja, ki kasneje vodijo v težave pri doseganju skladnosti z ZVOP-1.

Z izvedbo PVZ in spoštovanjem načela vgrajene zasebnosti se lahko tudi izognemo t.i. »function creep« pojavu, ko se podatki primarno zberejo za določen namen, s časom pa se začnejo uporabljati za druge namene, s strani drugih, prej neznanih obdelovalcev in uporabnikov.

Smernice PVZ dajejo poudarek na enostavnosti, praktičnosti, ekonomičnosti - s ciljem izogibanja nezakonitim situacijam, nikakor pa ne povečevanju administrativnih ovir v smislu kompliciranega formalnega postopka PVZ. Smernice za izvedbo PVZ so zato kratke in jedrnate.

Kakšni so konkretni primeri koristi PVZ?

Naštejmo tri primere, s katerimi se je srečal Informacijski pooblaščenec:

- Izvedeno je bilo povezovanje zbirk osebnih podatkov iz uradnih knjig in javnih evidenc v javnem sektorju, pri tem pa ni bila pridobljena potrebna predhodna odločba IP, s čim so bili upravljavci zbirk v prekršku.
- Sistem za elektronske vozovnice v javnem potniškem prometu je nepotrebno beležil osebne podatke o času in kraja vstopa potnikov, s čimer je prišlo do nesorazmerne obdelave osebnih podatkov – potrebni so bili dragi in zamudni popravki informacijskega sistema.
- Trgovec, ki izdaja kartice zaupanja, je želel začeti z zbiranjem osebnih podatkov o nakupnih navadah kupcev – po izvedeni PVZ je pravočasno ustavil načrt pisnega obveščanja kupcev o načrtovanem zbiranju teh osebnih podatkov s predvidevanjem *tihe privolitve* kupcev in je uvedel pravilno zbiranje *aktivno podanih* osebnih privolitev posameznikov, ter si s tem prihranil verjetno visoko globo in zahtevo po brisanju podatkov.

Kdo lahko izvede PVZ?

Poznamo **interno** in **zunanjo** PVZ, obe pa se na bolj neformalni ravni že uporabljata tudi pri nas. Interno PVZ izvede upravljavec osebnih podatkov sam, pri zunanji pa gre bodisi za najem zunanjega svetovanja ali pa za posvet pri pristojnem organu za varstvo osebnih podatkov – Informacijskemu pooblaščencu. Ta izdaja neobvezna pisna mnenja, prav tako pa obstaja možnost posvetovanja s strokovnjaki Informacijskega pooblaščenca pred uvedbo projekta, kjer obstajajo večja tveganja z vidika varstva osebnih podatkov. Pooblaščenec prav tako daje in objavlja predhodna mnenja državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke, kar se čedalje bolj tudi uveljavlja in upošteva.

Pričujoče **smernice so namenjene predvsem interni izvedbi PVZ**, katere rezultat pa je lahko tudi predmet kasnejšega posvetovanja s Pooblaščencem.

Katera so temeljna načela PVZ?

Temeljna načela PVZ gradijo na temeljnih načelih varstva osebnih podatkov:

Zakonitost

Načelo zakonitosti pomeni, da morajo biti splošna pravila obdelave osebnih podatkov predpisana z zakonom (predvsem nabor osebnih podatkov in namen obdelave). Zakonitost obdelave osebnih podatkov pomeni, da se osebne podatke v Republiki Sloveniji (v skladu z 2. odstavkom 38. člena Ustave Republike Slovenije) lahko obdeluje le v skladu z zakonom, oziroma na podlagi splošnega pooblastila iz zakona. Slednje velja zlasti za pravne osebe zasebnega prava, za katere so splošno pooblastilo in splošna pravila za obdelavo osebnih podatkov določena predvsem v sistemskem zakonu (ZVOP-1), podrobnejša pravila pa v osebni privolitvi posameznika, pogodbi in podobno. Načelo določenosti obdelave osebnih podatkov v zakonu pa praviloma velja v javnem sektorju.

Poštenost in transparentnost

Poštenost in transparentnost se logično nanašata na to, da mora obdelava osebnih podatkov potekati na pošten in transparenten način do posameznika. Ta mora vedeti, kateri njegovi podatki bodo obdelovani, kdo jih bo obdeloval in za kakšne namene, komu in pod kakšnimi pogoji bodo posredovani. V javnem sektorju naj bi ti načeli zagotovili z upoštevanjem načela zakonitosti (določenost v zakonu), v zasebnem sektorju pa je bistvena ustrezna informiranost posameznika, da lahko na podlagi zadostnih informacij poda svojo privolitev kot prostovoljno izjavo volje v obdelavo določenih osebnih podatkov za določene namene.

Sorazmernost

Sorazmernost pomeni, da je dopustno zbrati in obdelovati le **najmanjši obseg osebnih podatkov**, ki je **potreben za dosego namena obdelave** osebnih podatkov. Sorazmernost lahko pomeni predvsem to, da **če osebni podatki niso potrebni za dosego cilja, jih ni primerno zbirati**. Polega samega obsega podatkov se sorazmernost nanaša tudi na uporabo manj občutljivih podatkov od tistih, katerih narava oziroma zloraba ima večjo težo (**psevdonimi** so boljši kot navadni podatki, govoreče šifre so slabše od naključnih nizov ipd.). Prav tako se sorazmernost nanaša tudi na časovni vidik – tako je prekomerna hramba ali obdelava osebnih podatkov nedopustna in je treba podatke po dosegu namena oziroma po preteku zakonsko ali drugače določenega roka izbrisati, uničiti ali anonimizirati.

Nekaj zelo očitnih primerov nesorazmernosti:

- zahtevati EMŠO pri nakupu kruha;

- hramba podatkov o času in lokaciji vstopu potnika na mestni avtobus, če ta uporablja mesečno, pavšalno vozovnico;
- zahtevanje več enoličnih identifikatorjev hkrati (npr. EMŠO in DAVČNE številke);
- hramba podatkov brez utemeljenega namena, »na zalogo«;
- zbiranje podatkov, ki jih sploh ne potrebujemo (»sistem me ne spusti skozi«, »takšen obrazec pač imamo«, »to pač morate izpolniti«).

Točnost in ažurnost

Načelo točnosti in ažurnosti narekuje, da morajo biti podatki, ki se obdelujejo, točni in ažurni. Točnost pomeni, da podatki niso napačni ali nepopolni, ažurnost pa pomeni, da se uporablja zadnji, ažuren podatek. Osebni podatki so lahko točni, niso pa ažurni, kar pomeni, da se uporablja podatek, ki je sicer točen in veljaven v določenem obdobju ali trenutku, vendar pa obstaja novejši, bolj ažuren podatek. Pogosto slišani argument »saj nimam kaj skrivati« hitro zvodeni, če ni spoštovano načelo točnosti in ažurnosti in so o vas v določeni evidenci nahajajo napačni ali neažurni podatki.

Rok hrambe

Rok hrambe je v tesni povezavi z načelom sorazmernosti in določa, da se osebni podatki lahko shranjujejo le toliko časa, dokler je to potrebno za dosego namena, zaradi katerega so se zbirali ali nadalje obdelovali. Po izpolnitvi namena obdelave se osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, če niso na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo, oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače.

Eden od bistvenih elementov PVZ je tudi preučitev in določitev ustreznega roka hrambe osebnih podatkov, pri čemer je ta rok lahko že določen v zakonodaji, bistveno pa je, da rok hrambe ni odprt, temveč mora biti opredeljen.

Zavarovanje osebnih podatkov

Zavarovanje osebnih podatkov je ožji pojem od varstva osebnih podatkov in se nanaša na organizacijske in tehnične ukrepe, s katerimi s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov. Z drugimi besedami – podatke imamo lahko izjemno dobro zavarovane, kljub temu pa lahko pride do njihove zlorabe, zlasti ob neupoštevanju ostalih načel (npr. obdelava podatkov brez prave podlage, uporabe za namene, ki so različni od namena zbiranja podatkov, predolga hramba podatkov ipd.).

Upoštevanje pravic posameznika

Eno od bistvenih načel varstva osebnih podatkov se nanaša na posameznika, katerega osebne podatke obdelujeta javni in zasebni sektor. Posameznik ima namreč pravico do seznanitve z lastnimi osebnimi podatki, v primeru ugotovljenih nepravilnosti pa tudi pravico do dopolnitve, popravka, blokiranja, izbrisa in ugovora.

DRUGO POGLAVJE – KAKO IZVEDEMO PRESOJO VPLIVOV NA ZASEBNOST (PVZ)

Modeli PVZ

Informacijski pooblaščenec je preučil več modelov in pristopov k izvedbi PVZ in ugotavlja, da ne obstaja en model PVZ za vse situacije. Zaslediti je možno PVZ, ki so uporabne v določenih okoljih, zelo obsežne PVZ kot tudi skrajšane PVZ. Ločimo lahko:

a) obsežne PVZ (angl. full-scale PIA),
b) manj obsežne PVZ (angl. small-scale PIA),
c) kontrolne sezname za skladnost z zakonodajo, ki ureja področje zasebnosti in
d) kontrolne sezname za skladnost na področju varstva osebnih podatkov.

Pooblaščenec zato predlaga za projekte eUprave uporabo v nadaljevanju opisanega pristopa, medtem ko je za drugačne okoliščine priporočljiva uporaba prilagojenih smernic za PVZ. Pooblaščenec se je odločil za pripravo smernic za izvedbo **manj obsežnih PVZ v kombinaciji s kontrolnimi seznami za skladnost na podlagi praktičnih izkušenj Pooblaščenca pri že opravljenih neformalnih presojah vplivov na zasebnost.** Te po našemu mnenju predstavljajo v obdobju, ko se formalne PVZ v našem prostoru šele uveljavljajo, najboljše razmerje med **formalnostjo** in **učinkovitostjo** postopka. Manj obsežne PVZ predstavljajo manjše administrativno breme in so najprimernejše za uporabo pri posameznih projektih.

Izvedba PVZ

Informacijski pooblaščenec predlaga konsolidacijo običajnih faz PVZ (preliminarna faza, identifikacija tveganj, identifikacija ukrepov, zaključno poročilo) v **zgoščeni kontrolni seznam**. Organizacija naj bi s pomočjo kontrolnega seznama:

- pravočasno identificirala relevantne zakonske obveznosti ter tveganja za nezakonita ravnanja z osebnimi podatki in neskladnosti z ZVOP-1,
- identificirala ukrepe za izogibanje ali zmanjševanje tveganj, kot so uporaba anonimnih podatkov, minimizacija nabora podatkov, rokov hrambe ipd.
- pridobila napotitve na podrobnejše informacije v že objavljenih gradivih (zakonodaja, smernice ipd.).

PVZ in standard varovanja informacij ISO 27001

Analize tveganj v PVZ imajo načeloma širši obseg kot analiza tveganj, ki je bistvena faza po standardu varovanja informacij ISO 27001. PVZ namreč temeljijo na temeljnih načelih varstva osebnih podatkov, od katerih je zavarovanje osebnih podatkov, ki je sorodno cilju varovanja informacij po ISO 27001, samo eno od temeljnih gradnikov varstva osebnih podatkov. PVZ namreč obravnava, ali se obdeluje prekomerno število podatkov, za kakšne namene se podatki obdelujejo, ali obstaja pravna podlaga za obdelavo osebnih podatkov, ali so podatki ustrezno zavarovani itd. Segment zavarovanja osebnih podatkov (angl. data security) pa je tisto stično področje med PVZ in ISO 27001 in tu standard ISO 27001 s fazami, kot so analiza tveganja in načrt obravnave tveganja, odlično sovpada za zahtevo zakonodaje po ustreznem zavarovanju osebnih podatkov.

Kontrolni seznam

Namen kontrolnega seznama je na enostaven in pregleden način opozoriti na nekatere najbolj pomembne elemente zakonodaje in mesta, kjer se lahko s pravočasno identifikacijo tveganj izognemo naknadnim težavam. Velja opozoriti, da se kontrolni seznam nanaša le na sistemski zakon (ZVOP-1) in temeljna načela varstva osebnih podatkov, pomembna pa je tudi preučitev področne zakonodaje, ki se nanaša na obdelavo osebnih podatkov.

Kontrolni seznam se začne s pripravo **osebne izkaznice projekta**, kjer razmislimo o tem, kateri osebni podatki se bodo obdelovali, kdo, kdaj in pod kakšnimi pogoji jih bo obdeloval in podobno.

V nadaljevanju sledijo najpomembnejši elementi varstva osebnih podatkov, na katere ne smemo pozabiti, kot so pravna podlaga, zavarovanju osebnih podatkov ipd.

Če bomo šli skozi kontrolni seznam z značilnostmi našega projekta, bomo lahko pravočasno identificirali morebitna tveganja in se jim poskušali izogniti oziroma jih zmanjšati.

Kako formalno naj uporabimo kontrolni seznam? Odločitev je prepuščena vam, na vse elemente lahko poiščete odgovore glede na projekt in to tudi zapišete, lahko pa kontrolni seznam uporabite zgolj kot opomnik. Bistveno je, da s formalnostjo ne pretiravate, a da obenem ne izpustite katerega od pomembnih vidikov.

		Podrobnejša razlaga	Več informacij
OSEBNA IZKAZNICA PROJEKTA	**Nabor osebnih podatkov**	Nabor osebnih podatkov, ki se bodo obdelovali, moramo čim prej določiti. Pri tem pazimo na to, da: • **obdelava** pomeni **kakršnokoli ravnanje z osebnimi podatki,** • je osebni podatek **katerikoli podatek**, ki se nanaša na **določeno** ali **določljivo** osebo, • na določljivost ne smemo gledati samo skozi naše sposobnosti, podatke in znanje – temveč tudi, ali bi kdo drug brez nesorazmerno veliko naporov, časa, ali sredstev lahko ugotovil, na koga se podatek nanaša, • ZVOP-1 pokriva tiste osebne podatke, ki so **del zbirke osebnih podatkov** ali so **namenjeni vključitvi v zbirko osebnih podatkov,** • za obdelavo osebnih podatkov potrebujemo **pravno podlago**.	Če potrebujete odgovor na konkretno vprašanje, preverite, ali ga ni že kdo postavil: Mnenja Informacijskega pooblaščenca: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/ Smernice informacijskega pooblaščenca: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/
	Ravnanja z osebnimi podatki	Premislimo in si zapišimo: • kako se bodo osebni podatki pridobivali (iz uradnih evidenc/ od posameznika/elektronsko/na papirju/…), • kje se bodo hranili (v informacijskem sistemu/v fasciklih/…), • komu se bodo posredovali (drugim organom/uporabnikom/…), • kdo bo delal z osebnimi podatki (kateri oddelki), • kako bodo podatki zavarovani pred naključnimi ali namernimi zlorabami, izgubo ali uničenjem (tehnično/organizacijsko), • kako dolgo jih bomo hranili, • kako jih bomo po preteku obdelave uničili (komisijsko/sami/prek pogodbenega partnerja).	
	Področna zakonodaja	Preveriti določbe področne zakonodaje, ki urejajo obdelavo osebnih podatkov, predvsem z vidika: • namena obdelave, • nabora podatkov, • roka hrambe, • zahtev glede zavarovanja, • pogojev dajanja na razpolago ipd.	

Sorazmernost	Pri zakonskih podlagah bi moral načelo sorazmernosti upoštevati že zakonodajalec. Pri projektih morajo odgovorni na projektu določiti **minimalni zadostni nabor osebnih podatkov,** s katerim lahko dosežemo **namen obdelave**: • če določeni osebni podatki niso potrebni, potem naj se jih ne zbira (pogosto zadostujejo **anonimizirani** ali **statistični** podatki), • če so osebni podatki potrebni, potem uporabiti manj občutljive od bolj občutljivih, ne zbirati več enoličnih identifikatorjev, če to ni nujno potrebno. Nabor osebnih podatkov poskusimo skrčiti na minimum. Na sorazmernost pazimo v vseh fazah (Privacy by Design)- tudi npr. pri: • oblikovanju iskalnikov (kakšni so možni iskalni kriteriji, kaj se izpiše pri rezultatih iskanja). • uporabniških pravicah (ali določen uporabnik res potrebuje dostop do določenih podatkov-nivojski dostop) - več podatkov pomeni večje zahteve za sledljivost! **DOSTOP DO OSEBNIH PODATKOV:** **NAROBE: Vsi, vse, vedno, brez sledi!** **PRAVILNO: Vnaprej določene osebe, minimalen nabor podatkov, sledljivo!** Kjer je možno - ohraniti osebne podatke pod nadzorom posameznika! (npr. biometrijski vzorci, podatki o lokacijah posameznika ipd. je bolj pošteno in sorazmerno imeti na kartici, s katero razpolaga posameznik). Preverimo, ali lahko zmanjšamo tveganje za zlorabe in se izognemo centralizirani hrambi podatkov?	glej 3. člen ZVOP-1
Pravna podlaga	Pravno podlago za obdelavo osebnih podatkov lahko daje zakon ali osebna privolitev zakona, za javni sektor je pravna podlaga natančneje opredeljena v 9. členu ZVOP-1. POZOR! Pri določenih vrstah obdelave je potrebna **posebna pravna podlaga** ali	glej 9. člen ZVOP-1 - pravne podlage v javnem sektorju

	odločba Informacijskega pooblaščenca (biometrija, povezovanje zbirk, iznos podatkov v tretje države). Če je pravna podlaga **privolitev posameznika,** ne pozabite: • preučiti način pridobivanja, dokazovanja in preklica privolitve, • da se kot **privolitev ne šteje molk** posameznika, • da se za privolitev šteje le **prostovoljna** in **svobodna izjava volje** posameznika, da se določeni njegovi osebni podatki obdelujejo za določene namene, • da je **informiranost posameznika le predpogoj** za pravno podlago, ne nadomesti pa njegove privolitve, • da je privolitev lahko pisna, ustna ali tudi na drug način podana privolitev (npr. klik na povezavo ali gumb na spletni strani), • da je na spletnih straneh pravilno postaviti potrditvena okenca privzeto prazna, ne pa vnaprej zapolnjena.	
Pogodbena obdelava	Če bo določena opravila nad osebnimi podatki izvajal pogodbeni obdelovalec, moramo upoštevati zahteve 11. člena ZVOP-1 – **pisna pogodba** in **konkretizirani postopki za zavarovanje osebnih podatkov pri pogodbenem partnerju**. POZOR – obdelava pomeni kakršnokoli ravnanje z osebnimi podatki – tudi samo shranjevanje, pošiljanje ali uničenje podatkov se šteje za obdelavo osebnih podatkov! Pri tem je nepomembno celo, ali pogodbeni obdelovalec (ne) ve, na koga se osebni podatki nanašajo! Na pogodbeno obdelavo moramo gledati skozi oči posameznika – **ali bi lahko prišlo do zlorabe osebnih podatkov pri pogodbenem obdelovalcu**. Pogodbenega obdelovalca imamo pravico in dolžnost **nadzorovati**, saj gre le za našo podaljšano roko! Tako kot bi sami morali varovati osebne podatke, jih mora tudi pogodbeni obdelovalec. POZOR! Zaposleni pri pogodbenem obdelovalcu morajo biti natančno poučeni, kaj smejo in kaj ne smejo z osebnimi podatki!	glej 11. člen ZVOP-1

Točnost in ažurnost	Osebni podatki morajo biti točni in ažurni. Pred vnosom osebnih podatkov v zbirko se lahko preveri točnost podatkov z vpogledom v osebni dokument.	glej 18. člen ZVOP-1
Informiranje posameznika	Posameznika je treba o obdelavi osebnih podatkov ustrezno obvestiti. Če se osebni podatki zbirajo neposredno od posameznika, na katerega se nanašajo, je treba posamezniku sporočiti naslednje informacije, če z njimi posameznik še ni seznanjen: • **podatke o upravljavcu** osebnih podatkov in njegovem morebitnem zastopniku (osebno ime, naziv oziroma firma in naslov oziroma sedež), • **namen obdelave** osebnih podatkov. Če je treba, da se zagotovi zakonita in poštena obdelava, pa tudi druge podatke (glej 19. člen ZVOP-1). Pri spletnih straneh moramo oblikovati ustrezno politiko zasebnosti oziroma **izjavo o varstvu osebnih podatkov na spletnih straneh.**	glej 19. člen ZVOP-1 glej Smernice Informacijskega pooblaščenca za oblikovanje izjave o varstvu osebnih podatkov na spletnih straneh
Uporaba istega povezovalnega znaka	Isti povezovalni znaki so npr. **EMŠO**, **davčna številka**, **številka zdravstvenega zavarovanja**. Pri pridobivanju osebnih podatkov iz zbirk osebnih podatkov s področja zdravstva, policije, obveščevalno-varnostne dejavnosti države, obrambe države, sodstva in državnega tožilstva ter kazenske evidence in prekrškovnih evidenc ni dovoljena uporaba istega povezovalnega znaka na način, da bi se za pridobitev osebnega podatka uporabil samo ta znak. Izjeme so možne. Iskalnike in uporabo različnih šifrantov moramo ustrezno prilagoditi!	glej 20. člen ZVOP-1 glej smernice Varstvo osebnih podatkov pri povezovanju zbirk osebnih podatkov v javni upravi
Rok hrambe	Osebni podatki se lahko shranjujejo le toliko časa, **dokler je to potrebno za**	glej 21. člen ZVOP-1

	dosego namena, zaradi katerega so se zbirali ali nadalje obdelovali. Po izpolnitvi namena obdelave se zbrišejo, uničijo, blokirajo ali anonimizirajo, če niso na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo, oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače. Če zakon ne določa roka, ga je priporočljivo določiti z upoštevanjem načela sorazmernosti – najkrajši rok, ki je potreben za dosego namena obdelave. Izbris podatkov v elektronski obliki mora biti ustrezen (komisijsko fizično uničenje, večkratno naključno prepisovanje nosilcev podatkov ipd.)!	
Posredovanje	Osebne podatke se lahko posreduje uporabnikom osebnih podatkov, ki razpolagajo z ustrezno pravno podlago.	glej 22. člen ZVOP-1
Zavarovanje		
Interni akti	Interni akt mora določati postopke in ukrepe za zavarovanje osebnih podatkov. Ob uvedbi novega projekta je treba posodobiti interni akt! Pri pisanju internega akta naj sodelujejo tako pravniki kot informatiki!	glej 2. odst. 25. člena ZVOP-1
Določitev odgovornih oseb	Določen, dokumentiran ter ažuriran mora biti **nabor odgovornih oseb** za posamezno zbirko osebnih podatkov ter **oseb, ki imajo pooblastila za dostop** do osebnih podatkov (dostopne pravice/varnostna shema).	glej 2. odst. 25. člena ZVOP-1
Notranja sledljivost obdelave	Sistem mora omogočati poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil. Zavarovanje je potrebno in dopustno prilagoditi naravi in tveganju, ki ga prinaša obdelava določenih vrst osebnih podatkov.	glej 5. točka 1. odstavka 24. člena ZVOP-1

	Pri občutljivih osebnih podatkih, pri velikih zbirkah osebnih podatkov in v primerih, kjer je tveganje za zlorabe ali »vrednost« osebnih podatkov velika, je treba slediti vsak vpogled v osebne podatke. Posebno pozornost nameniti nadzoru sistemskih administratorjev in verodostojnosti revizijskih sledi/dnevnikov aktivnosti! Pri zbirkah, ki se vodijo na papirju (npr. kadrovska evidenca), izvesti analizo tveganja in prilagoditi ukrepe za zavarovanje.	
Sledljivost posredovanja (zunanja sledljivost)	Za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni pravni podlagi.	glej 3. odst. 22. člena ZVOP-1
Sistem za upravljanje varovanja informacij (SUVI)	Pri kompleksnejših projektih velja razmisliti o uvedbi **celovitega in sistematičnega pristopa k varovanju informacij** - uvedbi sistema za upravljanje varovanja informacij (SUVI). Priporočila podaja npr. standard ISO 27001.	http://en.wikipedia.org/wiki/ISO/IEC_27001
Postavitev odgovornih oseb za varstvo osebnih podatkov	Pri kompleksnejših projektih velja razmisliti o **določitvi odgovornih oseb za varstvo osebnih podatkov** (angl. Data Protection Officer) - individualne odgovorne osebe, ki je specializirana za zagotavljanje skladnosti z zakonodajo.	
Interni nadzor	Ali znamo odkriti zlorabe osebnih podatkov? Ali znamo ločiti, če naši zaposleni uporabljajo osebne podatke za legitimne in zakonite namene, ali gre za radovednost in usluge prijateljem?	
Izobraževanje	Varnost osebnih podatkov temelji tudi na ustrezni izobraženosti in ozaveščenosti zaposlenih - človeški faktor je pogost vzrok zlorab. Kdaj so bili nazadnje naši zaposleni in zaposleni pri pogodbenih obdelovalcih seznanjeni z zahtevami ZVOP-1? Ali naš interni pravilnik zgolj nabira prah?	

Katalogi in register informacijskega pooblaščenca	Za vsako zbirko osebnih podatkov moramo **pravočasno oblikovati katalog** (opis) zbirke osebnih podatkov. Določene podatke moramo sporočiti v **register Informacijskega pooblaščenca** (http://www.ip-rs.si/varstvo-osebnih-podatkov/register-zbirk/). Roke, obseg podatkov in izjeme določa zakon.	glej 26. člen ZVOP-1 glej 27. člen ZVOP-1 izjeme - glej 7. člen ZVOP-1
Iznos osebnih podatkov v tretje države	Če se bodo osebni podatki iznašali v države izven EU ali v države, za katere še ni zagotovljeno ustrezno varstvo osebnih podatkov, mora **iznos odobriti Informacijski pooblaščenec**.	glej 63.-71. člen ZVOP-1 seznam držav z ustreznim varstvom: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm
Videonadzor	ZVOP-1 določa pogoje glede dopustnosti uvedbe videonadzora. Tudi pri videonadzoru je pomembna **sorazmernost** - snemanje morda ni potrebno ves čas, področje snemanja naj se omeji samo na tista področja, kjer je to potrebno za varovanje premoženja ali ljudi. Izognimo se snemanju na delovnem mestu, če res ni nujno potrebno.	glej 74.-77. člen ZVOP-1 glej Smernice za izvajanje videonadzora
Biometrija	ZVOP-1 določa posebne kriterije glede dopustnosti uvedbe biometrijskih ukrepov. Potrebna je **predhodna pozitivna odločba IP**, biometrijski ukrepi pa se lahko izvajajo **le nad zaposlenimi**, ki morajo biti o tem pisno obveščeni (potrebni ne pa zadostni pogoj za uvedbo).	glej 78.-81. člen ZVOP-1 glej Smernice glede uvedbe biometrijskih ukrepov
Povezovanje zbirk osebnih podatkov	Za povezovanje zbirk osebnih podatkov je potrebna posebna, **izrecna pravna podlaga**. Pozor – povezovanje ni isto kot posredovanje osebnih podatkov (podrobnejšo razlago najdete v smernicah).	glej 84.-86. člen ZVOP-1 glej smernice Varstvo osebnih podatkov pri povezovanju zbirk osebnih podatkov v javni upravi

ZAKLJUČEK

Presoje vplivov na zasebnost (PVZ) so kot orodje za identifikacijo, analizo in zmanjševanje tveganj glede nezakonitih ravnanj z osebnimi podatki v našem prostoru še na začetku poti in pričujoče smernice predstavljajo enega prvih tovrstnih pripomočkov v našem okolju. Nedvomno bo to orodje možno v prihodnosti še izboljšati, prav tako pa je želja Informacijskega pooblaščenca pripraviti PVZ, ki bi bile prilagojene za uporabo tudi na drugih področjih (npr. v zasebnem sektorju). Smernice bodo dosegle svoj namen, če jih bodo v roke pravočasno prijeli oblikovalci politik in konkretnih rešitev v okviru eUprave, in se s tem izognili nepotrebnemu tratenju časa, sredstev ter ugleda. Pričujoče smernice pa imajo tudi bolj idealističen in v prihodnost zazrt cilj – upoštevanje koncepta vgrajene zasebnosti (angl. Privacy by Design), ki postaja eno od temeljnih načel varstva osebnih podatkov, in s tem boj proti drsenju v družbo nadzora z nepreudarno uporabo sodobnih tehnologij.

VIRI in UPORABNE POVEZAVE

- Office of the Privacy Commissioner – Privacy Impact Assesment Fact Sheet: http://www.priv.gc.ca/fs-fi/02_05_d_33_e.cfm

- Office of the Privacy Commissioner – Privacy Impact Assessment (PIA) handbook (Version 2): http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

- Office of the Privacy Commissioner – Privacy by design (report): http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf

- Office of the Privacy Commissioner of Canada – Privacy Impact Assessments http://www.priv.gc.ca/pia-efvp/index_e.cfm

- Office of the Privacy Commissioner (New Zealand), Privacy Impact Assessment Handbook http://www.privacy.org.nz/library/privacy-impact-assessment-handbook

- Smernice informacijskega pooblaščenca: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/

- Mnenja Informacijskega pooblaščenca: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/