Smernice za razvoj informacijskih rešitev

Skrb za zasebnost?
Pri nas je vgrajena!

INFORMACIJSKI
POOBLAŠČENEC

Namen dokumenta:	Smernice podajajo najpomembnejše zahteve, ki morajo biti upoštevane pri razvoju informacijskih rešitev, ki vključujejo obdelavo osebnih podatkov. Smernice so namenjene vsem tistim, ki se ukvarjajo z razvojem ali naročanjem rešitev na področju informacijsko-komunikacijskih tehnologij, ne glede na to, ali gre za nove proizvode, storitve, sisteme ali posamezne rešitve in aplikacije.
Ciljne javnosti:	Razvijalci informacijskih sistemov, rešitev in aplikacij ter naročniki teh storitev.
Status:	Javno
Verzija:	1.0
Datum verzije:	6.12.2010
Avtorji:	Informacijski pooblaščenec
Ključne besede:	Smernice, informacijski sistem, aplikacija, varstvo osebnih podatkov, sledljivost, sorazmernost, vgrajena zasebnost, Privacy by Design.

VSEBINA

4 O smernicah Informacijskega pooblaščenca

4 Uvod

5 Vgrajena zasebnost

5 *Proaktivnost namesto reaktivnosti*

6 *Zasebnost kot privzeta izbira*

6 *Zasebnost, ki je sestavni del dizajna rešitve*

6 *Polna funkcionalnost – igra s pozitivno vsoto*

6 *Zavarovanje podatkov v celotnem ciklu obdelave podatkov*

7 *Transparentnost*

7 *Spoštovanje posameznika*

8 Vgrajena zasebnost in smernice za razvoj informacijskih rešitev

8 *Minimizacija*

8 *Sorazmernost*

9 *Nadzor posameznika*

10 *Zavarovanje osebnih podatkov*

12 *Rok hrambe in pravica do pozabe*

13 *Povezovanje zbirk osebnih podatkov v javnem sektorju*

13 *Najpogostejše napake*

14 Zaključek

O smernicah Informacijskega pooblaščenca

Namen smernic IP je podati skupne praktične napotke za posameznike, katerih osebni podatki (OP) se obdelujejo ter za upravljavce in obdelovalce osebnih podatkov. Smernice naj bi na jasen, razumljiv in uporaben način odgovorile na najpogosteje zastavljena vprašanja na posameznem tematskem področju varstva osebnih podatkov. S pomočjo smernic želi Pooblaščenec doseči boljše poznavanje in spoštovanje informacijske zasebnosti ter določb 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 Pooblaščenca*:
  http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/
- *Brošure Pooblaščenca*:
  http://www.ip-rs.si/publikacije/prirocniki/
- *Smernice Pooblaščenca so objavljene na spletni strani:*
  http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/

Uvod

Uvod bo kratek, jasen in bralcu gotovo razumljiv. Navkljub drugačnemu prepričanju direktorjev nekaterih največjih internetnih podjetij, kot sta Facebook in Google, bo varovanje zasebnosti po našem mnenju ostala pomembna družbena norma, vsekakor pa drži, da je informacijska zasebnost v dobi informacijske družbe na precejšnjem udaru. Zakonodaja le stežka sledi hitremu tehnološkemu napredku, nanj pa se z zamikom odziva tudi zavest posameznikov, ki pogosto uporabljajo nova orodja brez treznega razmisleka. Žal jim tudi trezni premislek včasih ne pomaga. Govorimo namreč o na desetinah strani dolgih politikah zasebnosti, sistemih, ki delujejo na principu »vsi imajo vedno dostop do vseh podatkov brez nadzora«, rešitvah, ki hranijo podatke na zalogo, obdelavi večje količine osebnih podatkov zgolj zaradi prehoda iz papirnega poslovanja na elektronsko itd.

Če hočemo ohraniti zasebnost v informacijski družbi, se moramo držati določenih načel. V okviru teh smernic jih obravnavamo tehnološko nevtralno, njihov domet pa naj bi bil izrazito širok. Namenjene so namreč komurkoli, ki razvija produkt ali storitev v domeni informacijske družbe, ki bo povezana z obdelavo osebnih podatkov. Če razvijate ali uvajate sistem elektronskih vozovnic v javnem prometu, projekt sekcijskega merjenja hitrosti na avtocestah, »plačaj-kot-voziš« zavarovanja, nov CRM sistem, orodja za upravljanje z mailing seznami, sistem za spremljanje nakupnih navad vaših strank - in še bi lahko naštevali – potem so te smernice namenjene vam. Pravočasen razmislek o zakonskih pogojih in upoštevanje koncepta vgrajene zasebnosti (angl. Privacy by Design), vam lahko prihrani stroške, dvigne zaupanje pri strankah in vas obvaruje pred kršitvami zakonodaje. S pričakovano uvedbo obveznega poročanja o varnostnih incidentih v evropskem prostoru (npr. če izgubite podatke vaših strank) in s tem povezanimi stroški, bo pomen pravočasne vgradnje zasebnosti v poslovne prakse še toliko večji.

Vgrajena zasebnost bo morda našla svoje mesto tudi v bodoči evropski ureditvi varstva osebnih podatkov, vsekakor pa predstavlja temelj za naše smernice.

Vgrajena zasebnost

Koncept vgrajene zasebnosti temelji na 7 temeljnih načelih. Vgrajena zasebnost je dejansko nastala kot odziv na zahtevo po »vgrajenem nadzorovanju« (angl. Surveillance by Design) – skovanko iz sredine 90-ih, ko naj bi informacijsko-komunikacijska orodja že v svoji zasnovi omogočala dostop do podatkov organom pregona in obveščevalnim agencijam. Upoštevanje koncepta vgrajene zasebnosti bi morali prepoznati kot konkurenčno prednost, orodje za dvig zaupanja posameznikov, povsem verjetno pa se bo ta koncept znašel tudi v bodoči evropski zakonodaji o varstvu osebnih podatkov. V svetu, kjer pravo čedalje bolj zaostaja za bliskovitim tehnološkim razvojem (spomnimo se, koliko let štejeta Facebook in Google in kako drugačen je bil svet 10 let nazaj), je morda koncept vgrajene zasebnost eno od orodij, ki lahko ohrani našo zasebnost v informacijski družbi.

V tesno povezavo s konceptom vgrajene zasebnosti sodijo tudi presoje vplivov na zasebnost (angl. Privacy Impact Assesment - PIA), in uporaba tehnologij, ki ohranjajo zasebnost (angl. Privacy Enhancing Technologies - PETs). Presoje vplivov na zasebnost bi lahko uvrstili kot del vgrajene zasebnosti, gre pa za 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. Uporabljajo se tako v javnem kot v zasebnem sektorju, kjerkoli pa so bile uvedene, so se tudi uveljavile in obstale.

Presoje vplivov na zasebnost so torej bistven gradnik koncepta vgrajene zasebnosti, ki temelji na sedmih temeljnih načelih.

1. Proaktivnost namesto reaktivnosti

Koncept vgrajene zasebnost temelji na proaktivnem delovanju, na izogibanju težavam namesto reaktivnega odpravljanja posledic. Potencialne težave z vidika varstva osebnih podatkov in zasebnosti naj bi pravočasno predvideli in dizajn sistema vnaprej prilagodili na način, ki zmanjšuje tveganja za zlorabe namesto čakanja na udejanjenje teh tveganj. Če koncept vgrajane zasebnosti ne bo upoštevan in ko bo enkrat takšna rešitev oblikovana in v uporabi, vas bo prilagajanje rešitve stalo časa, sredstev in ugleda, v nekaterih primerih pa vas lahko naknadno popravljanje sistema stane več, kot če bi sistem porušili in postavili na novo.

2. Zasebnost kot privzeta izbira

Zasebnosti prijazne nastavitve naj bi bile v informacijskih rešitve opredeljene kot privzete (angl. default). Primeri takšnih nastavitev so lahko:

- potrditvena polja, s katerimi posameznik potrdi strinjanje z obdelavo svojih podatkov naj bodo privzeto prazna – strinjanje naj posameznik z izpolnitvijo aktivno poda;
- nastavitve javnosti podatkov (npr. na spletnih družbenih omrežjih) naj bodo privzeto nastavljene na zaupnost podatkov.

3. Zasebnost, ki je sestavni del zasnove rešitve

Zasebnost naj bi bila vgrajena v samo zasnovo in arhitekturo informacijskih rešitev in poslovnih praks, ne pa pa naknadno dodana. Zasebnost mora biti obravnavana že v fazi postavljanja funkcionalnih zahtev sistema, prav tako pa morajo biti predvideni naknadni načini zagotavljanja zasebnosti v celotnem življenjskem ciklu sistema.

4. Polna funkcionalnost - igra s pozitivno vsoto

Bistven element koncepta vgrajene zasebnosti je zagotavljanje polne funkcionalnosti – z vgradnjo zasebnosti ne bi smeli žrtvovati učinkovitosti delovanja sistema ali drugih legitimno zasledovanih ciljev. Pogosto slišimo, da moramo žrtvovati zasebnost zaradi višje varnosti, praktičnosti ali ekonomičnosti, koncept vgrajene zasebnosti pa temelji na iskanju rešitev, ki nas ne silijo v izbiranje med navedenimi, temveč zagotavljajo oboje. In da, to praviloma terja znanje in čas, včasih tudi višja sredstva, toda prav tako praviloma se da ohraniti zasebnost in kljub temu doseči zasledovane cilje.

5. Zavarovanje podatkov v celotnem ciklu obdelave podatkov

Zavarovanje podatkov je pomemben element varstva osebnih podatkov in se nanaša na preprečevanje nepooblaščene obdelave osebnih podatkov ter slučajne ali namerne spremembe ali izgube osebnih podatkov. Skrb za ustrezno zavarovanje osebnih podatkov moramo obravnavati kot proces in ne le kot posamezne naloge, ki so končane, ko so enkrat opravljene. Proces zavarovanja osebnih podatkov mora temelji na načrtovanju, izvajanju, preverjanju in reagiranju na odkrite nepravilnosti in pomanjkljivosti. Pooblaščenec v tem oziru vsem upravljavcem osebnih podatkov priporoča upoštevanje smernic mednarodno uveljavljenih standardov varovanja informacij, kot so standardi iz družine standardov ISO/IEC 27000, kakor tudi periodično preverjanje prisotnosti znanih ranljivosti, ki lahko popolnoma izničijo ostale ukrepe.

Praktični primer – sektorsko merjenje hitrosti na avtocestah

Številne države za dvig varnosti v prometu uvajajo projekta sektorskega merjenja hitrosti na avtocestah. Sistem deluje tako, da se vozilo na točki A fotografira in zabeleži čas vstopa, na koncu predvidenega odseka se v točki B se zapiše čas izstopa in izračuna povprečna hitrost vozila na odseku. Če ta presega zakonsko dovoljeno hitrost, je bil storjen prekršek in se zoper voznika uvede prekrškovni postopek. Takšno merjenje hitrosti je seveda lahko izvedeno na zasebnosti prijazen način, ali pa tudi ne. Pri slednjem gre lahko za masovno nadzorovanje voznikov in ustvarjanja velike centralizirane zbirke podatkov, obdelavo podatkov tudi tistih, ki niso storili nobenega prekrška, prekomerno hrambo podatkov in podobno. Ob upoštevanju koncepta vgrajene zasebnosti lahko poseg v zasebnost skrčimo na minimum, obenem pa zadostimo vse zasledovanim ciljem. Koncept vgrajene zasebnosti v konkretnem primeru predvideva:

- *fotografiranje vozila iz zadnje strani,*
- *avtomatsko pretvorbo registrske številke v t.i. DNA vozila z uporabo enosmernih zgoščevalnih algoritmov – uporaba psevdonimizacije,*
- *ukrepe za preprečitev nepooblaščenega dostopa in obdelave podatkov v celotnem procesu obdelave (od merjenja do posredovanja prekrškovnemu organu),*
- *takojšnje zavrženje vhodnih podatkov, ki nimajo ustreznih izhodnih podatkov na točki B,*
- *takojšnje zavrženje podatkov, kjer ni prišlo do prekoračitve hitrosti,*
- *minimalni rok hrambe vhodnih podatkov, ki nimajo para med izhodnimi (npr. nekaj ur).*

6. Transparentnost

Zaprte rešitve, ki domnevno zagotavljajo varstvo osebnih podatkov in ki temeljijo na našem zaupanju vanje, kljub temu, da jih ni mogoče preveriti, niso v skladu s konceptom vgrajene zasebnosti. In obratno, rešitve z vgrajeno zasebnostjo morajo omogočati neodvisen zunanji pregled in potrditev dejanskega varovanja osebnih podatkov. Iz sveta kriptografije so na primer znani primeri, ko so bile uporabljene skrite kriptografske metode, ki naj bi bile zaradi te tajnosti tudi varne, a se je žal večkrat pokazalo, da so res varne le tiste rešitve, ki so bile povržene javni presoji in na katerih so si »zobe polomili« tudi najboljši raziskovalci z vsemi razpoložljivimi sredstvi. Povprečen razvijalec bo le stežka zapisal varen kripto algoritem, zato se je v tem oziru treba držati preverjenih kriptografskih metod. Javnost seveda sama po sebi še ni zagotovilo, da bo neka rešitev varnostno neoporečna, a bi javna presoja morala biti v določenih primerih nujna – takšen primer je recimo uvajanje bodočih pametnih osebnih izkaznic.

7. Spoštovanje posameznika

Dizajn rešitev bi moral upoštevati tudi vidik posameznika in mu omogočiti ustrezno informiranost glede obdelave osebnih podatkov, privzete enostavno uporabne nastavitve zasebnosti in podobno. Rešitve, ki informacije o obdelavi osebnih podatkov zakrivajo v neberljivih politikah zasebnosti in v kompliciranih in preveč tehnološko usmerjenih nastavitvah, ki jih običajni uporabnik sploh ne razume, ne zadostijo konceptu vgrajene zasebnosti.

Koncept vgrajene zasebnosti predstavlja osnovo za smernice za razvoj informacijskih rešitev, ki jih v nadaljevanju podrobneje predstavljamo.

Praktični primer

Ali je za uporabo mesečne vozovnice potrebno obdelovati osebni podatek o lokaciji in času vstopa na sredstvo javnega prevoza?

- *za upravljanje prometnih tokov, ugotavljanje obremenjenosti linij in posameznih sredstev prevoza ter druge statistično-analitične namene praviloma ne potrebujemo osebnih podatkov, temveč lahko obdelujemo le anonimizirane podatke, ki se jih ne da povezati z določljivim posameznikom!*
- *če je naš namen slediti uporabniku in mu glede na njegove poti ponuditi določene storitve (npr. popuste, prilagojeno oglaševanje in ponudbo ipd.), potem za ta namen lahko obdelujemo temu sorazmeren nabor osebnih podatkov, za katerega pa potrebujemo pravno podlago (osebno privolitev posameznika)!*

Vgrajena zasebnost in smernice za razvoj informacijskih rešitev

Minimizacija

V začetnih fazah projekta (ko določamo želene funkcionalnosti) moramo 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 za izpolnitev zadanega cilja zadostujejo že anonimizirani ali statistični podatki),
- če brez osebnih podatkov ne gre, potem upoštevamo načelo sorazmernosti.

Bodimo pozorni na to, da lahko različni nameni zahtevajo različen obseg osebnih podatkov, zato je nepravilno določiti en obseg osebnih podatkov (običajno je to unija vseh relevantnih obsegov podatkov) in ga posplošiti za vse namene!

Sorazmernost

Če smo ugotovili, da dejansko moramo obdelovati določene vrste osebnih podatkov, potem sledimo naslednjim smernicam sorazmernosti:

- **Uporabi manj občutljive od bolj občutljivih podatkov.**

Če lahko izbiraš, potem uporabi raje negovoreče identifikatorje (npr. številčni niz, rezultate enosmernih zgoščevalnih algoritmov ipd.) kot govoreče (npr. EMŠO). Podobno velja za kategorije osebnih podatkov – kjer se da, raje uporabi »navadne« osebne podatke in ne občutljivih osebnih podatkov .

- **Ne zbiraj več enoličnih identifikatorjev, če to ni nujno potrebno.**

- Uporabi princip «je zadetek/ni zadetka« kjerkoli je to možno.

Pogosto ni nobene dejanske potrebe, da med rezultati prikazujemo tudi vhodne podatke ali druge podatke, ki uporabnika sploh ne zanimajo.

- **Raje uporabi psevdonime kot »surove« osebne podatke**

POZOR – s psevdonimi običajno zmanjšamo tveganja za zlorabo dejanskih osebnih podatkov, zato priporočamo njihovo uporabo, a tudi psevdonime moramo praviloma obravnavati kot osebne podatke, če se uporabljajo v povezavi z določenim ali določljivim posameznikom; med psevdonime uvrščamo tudi rezultate (enosmernih) zgoščevalnih algoritmov (hash funkcij).

Na sorazmernost pazimo v vseh fazah (vgrajena zasebnost) – tudi na primer pri:

- **oblikovanju iskalnikov** (kakšni so možni iskalni kriteriji, kaj se izpiše pri rezultatih iskanja) – več prikazanih podatkov na zaslonu pomeni večje zahteve za sledljivost dostopov do podatkov.
- **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: minimalen nabor podatkov,
vnaprej določene osebe, sledljivo!

Nadzor posameznika

Dr. Alan Westin je v 70-ih definiral zasebnost kot pravico posameznika da nadzoruje, uporablja upravlja in izbriše informacije o sebi in da se lahko odloča kdaj, kako in v kakšnem obsegu bo informacije posredoval drugim. Žal ima posameznik v informacijski družbi pogosto težave pri uresničevanju omenjenih postulatov in ne ve, kdo vse bo obdeloval njegove podatke, komu bodo naprej posredovani in za kakšne vse namene bodo uporabljeni.

Marsikje je mogoče zasledovane cilje uresničiti tudi s takšnimi načini obdelave osebnih podatkov, ki predvidevajo hrambo in/ali obdelavo osebnih podatkov pri posamezniku. Klasični primeri takšne obdelave so v bodočem sistemu elektronskega cestninjenja, ki temelji na plačevanju po natančno prevoženi razdalji. Zasebnosti prijazne rešitve ohranjajo surove podatke o prevoženih poteh pod nadzorom posameznika, podobne načine izvedbe pa poznamo npr. pri biometrijskih ukrepih, kot je opisano v okvirčku. Iluzorno bi bilo trditi, da takšen premik procesorske moči v smer proti uporabniku nima finančnih posledic, vendar je treba pri ocenjevanju finančnih posledic upoštevati tudi stroške, ki lahko nastanejo zaradi zlorabe osebnih podatkov. Ti stroški so lahko tudi izjemno visoki in naraščajo s številom posameznikov, katerih podatke obdelujemo, prav gotovo pa je le vprašanje časa, kdaj bo obveznost poročanja o varnostnih dogodkih (angl. mandatory data breach notification) postala tudi zakonska obveznost za vse upravljavce osebnih podatkov. S »premikom« podatkov pod nadzor posameznika se lahko izognemo tveganju in potencialni odgovornosti.
Če obdelava na strani posameznika ni smiselna, lahko še vedno uporabniku omogočimo nadzor nad svojimi osebnimi podatki, s tem da mu ponudimo **možnost elektronskega vpogleda v lastne osebne podatke**, izvoz lastnih osebnih podatkov in podobna orodja.

Pozor – posameznik je upravičen le do lastnih podatkov in ne do podatkov o konkretnih osebah, ki so dostopale do njegovih podatkov (»kdo me je gledal«). Zakonitost teh dostopov lahko preveri državni nadzornik za varstvo osebnih podatkov, ki ima pooblastila za dostop do teh podatkov.

Uresničevanje koncepta samo-determinacije glede svojih osebnih podatkov je seveda brezpredmetno, če nismo ustrezno predhodno informirani o obdelavi osebnih podatkov. V mislih imamo zlasti politike zasebnosti na spletnih mestih, ki so v trenutni obliki popolnoma neberljive za končne uporabnike in ne dosežejo svojega cilja. Uporabniku je namreč bistveno podatki naslednje odgovore:

- kateri podatki se bodo obdelovali,
- kdo bo njegove podatke obdeloval,
- za katere namen,
- ali jih bi posredoval tretjim in osebam in katerim,
- kako dolgo se bodo podatki hranili in,
- kako se lahko seznani s hranjenimi podatki,
- kako lahko svoje osebne podatke zbriše iz baz.

Te podatke lahko posamezniku predstavite na zelo kratek, razumljiv in enostavno dosegljiv način – če ne gre drugače, jih ločite od pravniških pogojev uporabe. Oglejte si tudi Smernice Informacijskega pooblaščenca za oblikovanje izjave o varstvu osebnih podatkov na spletnih straneh.

Praktični primer – biometrija v fitnes centru

Biometrijski ukrepi so v našem pravnem redu zelo strogo regulirani. Koncept vgrajene zasebnosti na primeru biometrije (npr. uporaba prstnih odtisov za vstop v fitnes center) zagovarja rešitve, ki ohranjajo posameznikov nadzor nad lastnimi osebnimi podatki in izbor rešitev, ki še vedno zadovoljijo cilje organizacije. Fitnes center si legitimno želi več članov in želi preprečiti posojanje vstopnih kartic ter vidi biometrijo kot tehnologijo, ki lahko to omogoči na praktičen način. Z izbiro rešitev, ki hranijo biometrijske podatke oziroma njihove pretvorbe v stalni posesti posameznika (npr. na obesku za ključe, zapestnici ali kartici), se lahko izognejo centralni hrambi prstnih odtisov in s tem nastanku zbirke osebnih podatkov, posledično višjim zahtevam glede zavarovanja podatkov, zakonski obveznosti po pridobitvi predhodnega dovoljenja in drugim zakonskim zahtevam, obenem pa dosežejo vse zasledovane cilje in izkoristijo prednosti, ki jih omogoča biometrija. Posameznikovi biometrijski podatki se ne nahajajo v centralni zbirki in posameznik ohranja nadzor nad svojimi podatki, fitnes center pa si je efektivno zmanjšal tveganje za zlorabe osebnih podatkov z minimalnimi stroški.

Zavarovanje osebnih podatkov

Zavarovanje osebnih podatkov je tako široka tema, da bi njeno podrobno opisovanje preseglo namen teh smernic, zato se v nadaljevanju osredotočamo na nekatere najbolj izpostavljene elemente zavarovanja osebnih podatkov, kot so dostopne pravice in sledljivost.

V grobem pa lahko priporočimo upoštevanje mednarodno uveljavljenih standardov varovanja informacij, kot so standard družine ISO/IEC 27000, zlasti pa bi radi opozorili na to, da varovanje informacij in osebnih podatkov ne pomeni samo tehničnih, temveč tudi (ali morda celo predvsem) izvajanje organizacijskih ukrepov, kot so izobraževanje uporabnikov, notranji in zunanji nadzor, sprejem in izvajanje varnostnih politik in podobno.

Ukrepi za zavarovanje morajo biti ustrezni glede na naravo in tveganje, ki jih prinaša obdelava osebnih podatkov. Karikirano povedano – frizerka in univerzitetni klinični center se drastično razlikujeta glede obsega, narave in tveganj, ki pretijo osebnim podatkom, ki jih imata ta dva upravljavca. Ukrepi za zavarovanje morajo biti temu primerni. V tem oziru je izjemnega pomena analiza tveganja, katere rezultat je glavni vhodni podatek za sprejem ukrepov, s katerimi bomo to tveganje zmanjšali. Na žalost Informacijski pooblaščenec v praksi pogosto ugotavlja, da marsikatero podjetje in organ javne uprave ni opravil niti bistvene faze, ki je predpogoj za ustrezno zavarovanje – to je analiza stanja: katere osebne podatke imamo, kateri so naši informacijski viri in sredstva ipd. Če ne vemo niti, katere osebne podatke imamo, potem jih zagotovo ne moremo ustrezno varovati.

Posebej želimo opozoriti razvijalce informacijskih rešitev na uporabo uveljavljenih kriptografskih metod, s katerimi lahko zagotovimo celovitost in zaupnost podatkov. Kriptografske metode imajo široko polje uporabe, od varne hrambe podatkov v kriptirani obliki, prenosa podatkov v neberljivi obliki, uporabe istih podatkov za različne namene z medsebojno nepovezljivimi kriptografskimi pretvorbami do zagotavljanja nespremenljivosti podatkov.

Zaradi možnih izrab ranljivosti v računalniških sistemih, zaradi katerih so lahko delno ali v celoti izpostavljeni osebni podatki in izničena vsa skrb za zasebnost, posebej poudarjamo pomembnost pravočasnega in stalnega odkrivanja in odpravljanja tovrstnih napak. Še posebej je pomembno, da so v računalniških

sistemih, ki kakorkoli obdelujejo OP, v razvojni in vzdrževalni cikel periodično vgrajene aktivnosti za iskanje znanih in pogosto izrabljenih napak.

Dostopne pravice

Dostopne pravice uporabnikov morajo biti jasne in skladne z nalogami, ki jih opravljajo uporabniki. Dostopne pravice morajo biti ažurno upravljane (ažurno dodeljevanje, spremenjene in ukinjene), hierarhične in dokumentirane. Prepovedana mora biti uporaba skupnih dostopnih pravic, saj onemogoča naknadno ugotavljanje kdo, kdaj in do katerih osebnih podatkov je dostopal oziroma jih obdeloval. Prav tako mora biti izrecno prepovedano kakršnokoli posojanje sredstev za avtentikacijo in avtorizacijo uporabnikov, kot so uporabniška imena in gesla, kartice ipd., razen izjemoma, iz razloga nujnosti.

Beleženje dostopov do podatkov (sledljivost)

Upravljavci zbirk osebnih podatkov so dolžni osebne podatke, ki jih obdelujejo, ustrezno zavarovati . Glede na zahteve ZVOP-1 se sledljivost obdelave osebnih podatkov nanaša na širok pojem »obdelava osebnih podatkov«, ki po definiciji iz 3. točke 6. člena ZVOP-1 pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklicanje, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje; obdelava je lahko ročna ali avtomatizirana (sredstva obdelave). Z drugimi besedami to pomeni, da je glede na tveganje in naravo podatkov, ki se bodo obdelovali, potrebno zagotoviti popolno revizijsko sled, torej tudi beleženje vsakega dostopa do podatkov. Odstopanje od tega načela je možno le na podlagi ustrezne analize in obravnave tveganj.

Beleženje dostopov mora biti takšno, da omogoča naknadno preverjanje, kdo je, kdaj in do katerih osebnih podatkov dostopal; identifikacija osebe, ki je stopila v stik s podatki, mora biti enolična, torej se mora nanašati na posamezno konkretno osebo.

Pri tem je potrebno posebno pozornost nameniti dvema pomembnima (in medsebojno povezanima) vprašanjema – nadzoru nadzornikov ter avtentičnosti in celovitosti revizijske sledi. Vprašanje nadzora nadzornikov se nanaša predvsem na vprašanje pooblastil administratorjev z najvišjimi pravicami. Revizijska sled obdelave osebnih podatkov mora namreč biti avtentična in celovita, zato je treba poskrbeti za primerne tehnične in organizacijske ukrepe, s katerimi se uvaja nadzor tudi nad dejanji administratorjev z najvišjimi pooblastili. Sistem mora delovati tako, da beleženja dostopov ni možno za določen čas izključiti, prav tako pa tudi najvišjim (sistemskim) administratorjem ne sme biti dana možnost naknadnega popravljanja, spreminjanja ali brisanja dela ali celotne revizijske sledi. Pri tem je smiselno upoštevati izvedbene možnosti, ki omogočajo nezatajljivost, avtentičnost in celovitost revizijskih sledi, z ukrepi kot so: ločeno shranjevanje revizijskih sledi (na lokacije izven dosega oseb, katerih aktivnosti so zabeležene), sistem »štirih oči«, shranjevanje revizijskih sledi na neizbrisen način , shranjevanje podatkov o dostopu do revizijskih sledi. Nihče ne sme imeti nenadzorovane možnosti popravljanja revizijskih sledi, ki se nanašajo na njegove ali aktivnosti drugih, ali možnosti nenadzorovanega začasnega ali trajnega »izklopa« beleženja podatkov v revizijske sledi.

Sledljivost obdelave osebnih podatkov se nanaša tako na notranjo kot na zu-

nanjo sledljivost. Notranjo sledljivost obdelave opredeljuje že omenjeni 24. člen ZVOP-1, zunanjo sledljivost ali sledljivost posredovanja pa narekuje 3. odstavek 22. člena ZVOP-1, ki določa, da mora upravljavec osebnih podatkov za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja osebnih podatkov.

Zahteve glede sledljivosti so manjše, če se trdno držite načela sorazmernosti! Na to pomislite pri oblikovanju poizvedb in iskalnikov (kakšni so možni iskalni kriteriji, kaj se izpiše pri rezultatih iskanja – več prikazanih podatkov na zaslonu pomeni večje zahteve za sledljivost dostopov do podatkov), pri oblikovanju uporabniškega vmesnika (kaj se nahaja na posameznem zaslonu, zavihku ipd.) in pri drugih elementih informacijske rešitve, kjer si lahko zmanjšate obremenitve z vidika zagotavljanja sledljivosti.

Praktični primer

Vzemimo za ponazoritev primer, ko uporabnik informacijskega sistema v zdravstvu išče po kriteriju »Novak« in se mu prikaže seznam 100 pacientov in (nekateri, ne nujno vsi) osebni podatki teh pacientov. Kako lahko naknadno ugotovimo, da se je uporabnik s takšno poizvedbo seznanil z določenimi osebnimi podatki (vzemimo hipotetični scenarij, ko mediji objavijo podatek, da ima znana osebnost AIDS). Obstajata dve poti za zagotavljanje sledljivosti:
a) takšna poizvedba se zabeleži pri vsakem od pacientov, katerega osebni podatki so bili prikazani v določenem trenutku na izhodni enoti. Pri posamezniku se mora v tem primeru zabeležiti, kdo in kdaj je s pomočjo poizvedbe prišel do osebnih podatkov posameznika.
b) poizvedba mora dati ob ponovitvi enak rezultat, torej se beleži rezultat poizvedbe v času. Zabeležiti se mora, kdo je izvedel poizvedbo, kdaj in kakšen je bil rezultat poizvedbe v tem času.

Oba načina sta sprejemljiva, odločitev pa je prepuščena razvijalcu, ki bo pr tem upošteval funkcionalne, finančne in druge vidike. V obeh primerih je ključno, da se beleži, kdo je izvedel določeno poizvedbo, saj se lahko le na ta način določi odgovorno osebo v primeru zlorabe osebnih podatkov, kar je tudi namen sledljivosti.
Če ni možno zagotoviti naknadnega ugotavljanja, do katerih OP je na ta način uporabnik dostopil (do nekaterih ali do vseh), je potrebno predvidevati, da se je uporabnik s poizvedbo seznanil z vsemi prikazanimi osebnimi podatki in temu ustrezno to zabeležiti v dnevniški zapis.

Rok hrambe in pravica do pozabe

Življenjski cikel osebnih podatkov igra pomembno vlogo pri zagotavljanju pravice posameznika do samo–odločitve. Poseben problem zlasti na internetu predstavlja uresničevanje pravice do pozabe (izbrisa podatkov), potem ko je bodisi potekel namen uporabe podatkov bodisi je posameznik preklical privolitev za obdelavo podatkov. V Franciji je država spodbudila sprejem ustreznih kodeksov obnašanja za zagotovitev pravice do pozabe na spletnih družbenih omrežjih in pri spletnih iskalnikih. Podpisniki kodeksa so se zadolžili, da bodo ustrezno informirali posameznika o tem, komu zaupa katere podatke in za kakšne namene bodo uporabljeni, na podlagi teh informacij pa se lahko posameznik prostovoljno odloči, ali bo za obdelavo podatkov podal svojo privolitev, obenem pa mu zagotavljajo tudi pravico do nasprotovanja obdelavi osebnih podatkov. Tudi Evropska komisija je najavila, da bo uresničitev pravice do pozabe vključena v spremembah evropske direktive o varstvu osebnih podatkov.

Po določbah naše zakonodaje 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. Rok hrambe podatkov mora torej slediti namenu obdelave osebnih podatkov, zato je priporočljivo, da se ga vnaprej opredeli, pri tem pa se upošteval načelo sorazmernosti. Hramba na zalogo brez utemeljenih argumentov ni dopustna. Če rok ni določen, je priporočljivo, da je posameznik o tem dejstvu obveščen.

Povezovanje zbirk osebnih podatkov v javnem sektorju

Povezovanje zbirk osebnih podatkov iz uradnih evidenc in javnih knjig je posebej urejeno v ZVOP-1. Pooblaščenec v zvezi s povezavo zbirk osebnih podatkov opozarja, da mora biti takšno povezovanje določeno v zakonu ter, da v primeru, če katera od zbirk, ki naj bi se jih povezovalo, vsebuje občutljive osebne podatke (19. točka 6. člena ZVOP-1) ali je za izvedbo povezovanja potrebna uporaba istega povezovalnega znaka (EMŠO, št. zdravstvenega zavarovanja ali davčna številka), povezovanje ni dovoljeno brez predhodnega dovoljenja Pooblaščenca. Več o tem v smernicah Informacijskega pooblaščenca: Varstvo osebnih podatkov pri povezovanju zbirk osebnih podatkov v javni upravi .

Najpogostejše napake

Pravijo, da so tisti, ki ne poznajo preteklosti, obsojeni na ponavljanje napak iz preteklosti. Najpogostejše napaka v povezavi z informacijskimi rešitvami in varstvom osebnih podatkov so po naših izkušanjih iz prakse naslednje.

ZAVAROVANJE OSEBNIH PODATKOV

Na področju zavarovanja osebnih podatkov gre praktično za odstopanja od uveljavljenih standardov varovanja informacij. Na nekatere morajo biti pozorni razvijalci informacijskih rešitev, določene ukrepe (zlasti organizacijske), pa morajo izvajati uporabniki takšnih rešitev:

- dostopne pravice uporabnikov niso opredeljene,
- dostopne pravice ne ustrezajo naravi in zahtevam dela,
- obstajajo skupinske pravice (npr. »ambulanta2«),
- sredstva za avtentikacijo in avtorizacijo se posojajo,
- sistem ne zagotavlja sledljivosti obdelave osebnih podatkov,
- sledljivost obstaja, ne zabeležijo pa se izvozi podatkov,
- administratorji lahko nenadzorovano prikrijejo sledi dostopa do podatkov za seboj,
- uporabniki ne izvajajo politik čistega zaslona,
- občutljivi osebni podatki so pošiljajo po navadni e-pošti,
- sledljivost ne omogoča izsleditve odgovorne osebe,
- brez ločevanja testnega, šolskega in produkcijskega okolja,
- zagotavljanje tehničnih ukrepov, odsotnost organizacijskih ukrepov (npr. izobraževanje uporabnikov, notranji nadzor ipd.)

UPORABA ISTIH POVEZOVALNIH ZNAKOV NA DOLOČENIH PODROČJIH

Isti povezovalni znaki ali enolični identifikatorji imajo glede varstva osebnih podatkov dvojni obraz. Po eni strani je njihove uporaba problematična predvsem zato, ker so idealni za povezovanje različnih zbirk osebnih podatkov , prav tako pa omogočajo nabiranje osebnih podatkov (angl. harvesting). Po drugi strani so lahko tudi varuhi vaših podatkov – pomislite, kolikšno količino podatkov morate včasih dati ob uveljavljanje garancije, iskanju pomoči pri delovanju izdelka ali storitve, prijavi škode zavarovalnici in podobno, kjer bi za vašo identifikacijo

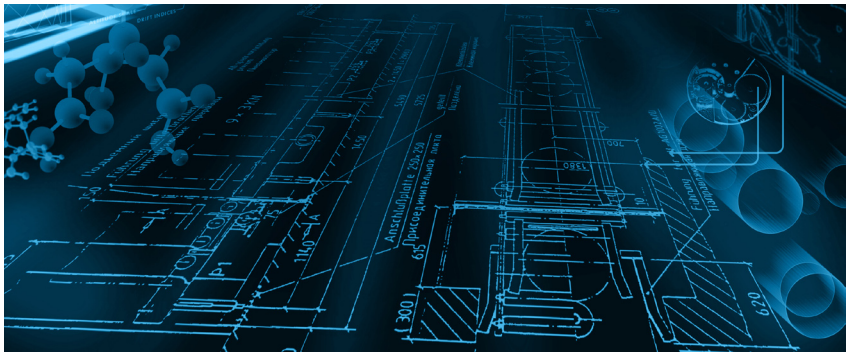
zadostoval isti povezovalni znak, kot je šifra kupca, številka naročniške pogodbe ali police.

ZVOP-1 izrecno prepoveduje uporabo istih povezovalnih znakov na način, da bi se za pridobitev osebnega podatka uporabil samo ta znak (20. čl. ZVOP-1). Navedeno ne velja za vse zbirke, temveč le za pridobivanje 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. Z drugimi besedami – na teh področjih ni dovoljeno iskanje samo z EMŠO, samo po davčni številki ali samo po številki kartice zdravstvenega zavarovanja.

NEUPOŠTEVANJE NAČEL MINIMIZACIJE IN SORAZMERNOSTI

Simptomi, ki kažejo na neupoštevanje načel minimizacije in sorazmernosti, se včasih pokažejo v izjavah, kot so »to rabimo, sicer me sistem me ne spusti skozi), sicer pa gre za naslednje napake:

- zbirajo se podatki čeprav bi sistem lahko učinkovito deloval tudi brez njih,
- (ponovno) se zbirajo podatki, ki jih upravljavec že ima (npr. uveljavljanje garancije, zahtevkov iz naslova zavarovanja),
- podatke se zbira na zalogo (»jih bomo morda kdaj rabili«),
- zahteva se več enoličnih identifikatorjev hkrati,
- roki hrambe niso opredeljeni ali so predlogi.



Zaključek

Zagovorniki koncepta vgrajene zasebnosti vidijo v njem pomembno orodje za ohranitev zasebnosti v informacijski družbi, seveda pa ima na poti do polne uveljavitve še kar nekaj težav. Pogledi nanj se namreč razlikujejo med regulatorji, menedžmentom in oblikovalci rešitev. Če je koncept vgrajene zasebnosti za regulatorje zelo intuitiven in naraven, je za menedžment še vedno bistven odgovor na vprašanje – ali se nam bo to splačalo? Odgovor regulatorjev je pričakovan – vprašati bi se raje morali, koliko nas bo stalo, če tega ne upoštevamo od samega začetka – regulatorni okvir se bo v prihodnje gotovo gibal v tej smeri. Strošek naj ne bi bil vlaganje v zasebnost, temveč odsotnost vlaganja v zasebnost. Navedeno so na lastni koži že izkusili nekateri upravljavci tako v tujini kot v Sloveniji. Oblikovalci pa so lahko zadržani, saj se deloma izkazuje strah, da bi vgraditev zasebnosti lahko v začetku spodrezal inovativne pristope in nove storitev. Čas bo pokazal, ali bo možno priti do integralnega pristopa do koncepta vgrajene zasebnosti, do takrat pa upamo, da so vam bile te smernice v pomoč pri gradnji informacijskih rešitev in izogibanju najpogostejšim napakam.