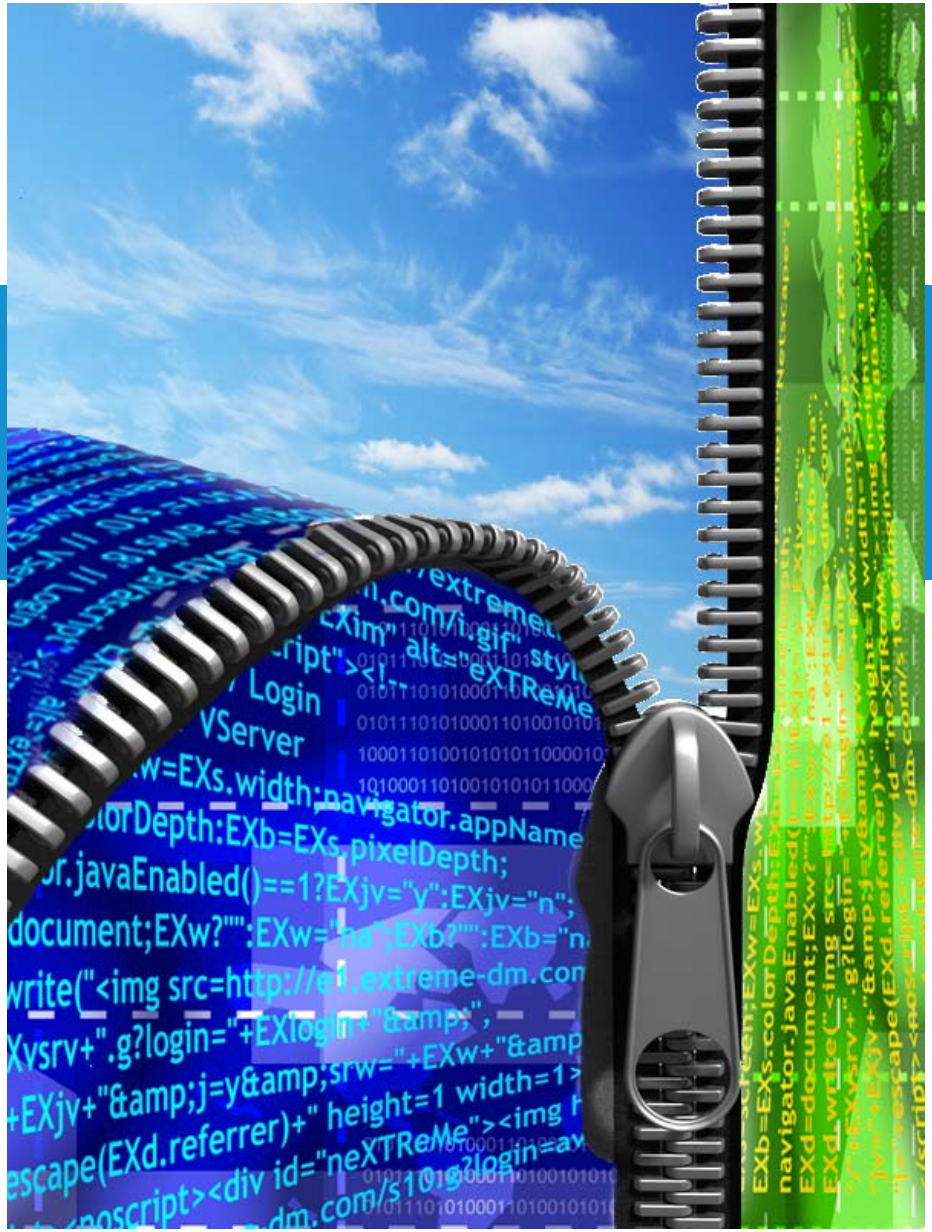
Varstvo osebnih podatkov pri povezovanju zbirk osebnih podatkov v javni upravi



INFORMACIJSKI POOBLAŠČENEC

Namen dokumenta:	Smernice podajajo predstavitev zakonske ureditve povezovanja zbirk osebnih podatkov, s katerimi upravlja javni sektor, v luči sorazmernosti med interesi javnega sektorja za izvrševanje njegov zakonitih pristojnosti in obveznosti ter pravico posameznika do varstva osebnih podatkov.
Ciljne javnosti:	Upravljavci zbirk osebnih podatkov v javnem sektorju.
Status:	Javno.
Verzija:	1.0
Datum verzije:	15. 9. 2009
Avtorji:	Informacijski pooblaščenec.
Ključne besede:	Smernice, upravljavci v javnem sektorju, zasebnost, povezovanje zbirk, posredovanje.

VSEBINA

O SMERNICAH INFORMACIJSKEGA POOBLAŠČENCA 4

UVOD 4

VARSTVO OSEBNIH PODATKOV IN POVEZOVANJE ZBIRK OSEBNIH PODATKOV 5
Zbirka vseh zbirk? 6

PREGLED ZAKONODAJE S PODROČJA VARSTVA OSEBNIH PODATKOV 7
Evropska konvencija o človekovih pravicah (EKČP) 7
Direktiva 95/46/ES 8
Zakon o varstvu osebnih podatkov (ZVOP-1) 8
Povezovanje v primeru prekrškovnih in kazenskih evidenc 9
Komentar ureditve povezovanja v ZVOP-1 9
Pojasnilo glede termina povezovanje v kontekstu 6. poglavja VI. dela ZVOP-1 9
Posredovanje osebnih podatkov (22. člen ZVOP-1) 10
Povetovanje zbirk osebnih podatkov 10
Ožja definicija pojma povezovanje zbirk osebnih podatkov 11
Širša definicija pojma povezovanja zbirk osebnih podatkov 11

JE POVEZOVANJE PODATKOV RES REŠITEV? 12

NAČELI DOSTOPNOSTI IN ISKANJA PRI (OMEJENO) JAVNO DOSTOPNIH ZBIRKAH OSEBNIH PODATKOV 13

ZAHTEVE Z VIDIKA ZAVAROVANJA OSEBNIH PODATKOV 15
Osnovne zahteve glede zavarovanja 16
Nadzor nadzornikov ter avtentičnost in celovitost revizijske sledi 17
Zavarovanje osebnih podatkov kot proces 17

NAPOTKI ZA IZPOLNITEV VLOGE ZA IZDAJO PREDHODNEGA DOVOLJENJA ZA POVEZAVO ZBIRK OSEBNIH PODATKOV 18

ZAKLJUČEK 19

>>>

O smernicah Informacijskega pooblaščenca

Namen smernic Informacijskega pooblaščenca (v nadaljevanju Pooblaščenec) je podati skupne praktične napotke za upravljavce zbirk oseb-nih podatkov (OP) na jasen, razumljiv in uporaben način in s tem odgovoriti na najpogosteje 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-UPB1).

Pravno podlago za izdajo smernic Pooblaščencu daje 49. člen ZVOP-1-UPB1, 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

Izboljševanje učinkovitosti delovanja javnega sektorja in razvoj storitev e Uprave terjata od države čedalje obsežnejše in intenzivnejše povezovanje podatkovnih virov, s katerimi upravlja javni sektor, med katerimi so tudi obsežne zbirke osebnih podatkov. Izpolnjevanje zakonskih pristojnosti javnega sektorja, uresničevanje pričakovanj in obveznosti do posameznikov, napori na področju preprečevanja kriminalitete in varnosti države narekujejo trend večjega povezovanja zbirk 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 državnega aparata.

Smernice Informacijskega pooblaščenca glede povezovanja zbirk osebnih podatkov v javnem sektorju uvodoma opozarjajo na pomen spoštovanja temeljnih človekovih pravic in nevarnost drsenja v t.i. družbo nadzora, kjer se v skrajni inačici o posamezniku na neskončnem številu dostopnih mestih vse ve in v katerem je posameznik popolnoma nadzorovan subjekt, ki je izgubil pravico do zasebnosti. Upravljavci zbirk osebnih podatkov bodo v smernicah našli predstavitev določb zakonodaje glede povezovanja zbirk osebnih podatkov, načela dostopnosti in iskanja pri (omejeno) javno dostopnih zbirkah osebnih podatkov, usmeritve glede možnosti poizvedb po podatkih ter napotke glede pomembnejših vidikov zavarovanja osebnih podatkov.

Varstvo osebnih podatkov in povezovanje zbirk osebnih podatkov

Varstvo zasebnosti je široko priznana temeljna človekova pravica. Pojavlja se v različnih pravnih sistemih, ki so zgrajeni na različnih verah in kulturah po celem svetu. Zavarovana je s številnimi mednarodnimi dokumenti o človekovih pravicah (npr. Splošna deklaracija o človekovih pravicah, Evropska konvencija varstvu človekovih pravic in temeljnih svoboščin – v nadaljevanju Evropska konvencija o človekovih pravicah ipd.), njeno varstvo vključuje večina modernejših ustav posameznih držav. Varstvo osebnih podatkov predstavlja del širše pravice do varstva zasebnosti, in sicer kot varstvo informacijske zasebnosti.

Bistvo varstva osebnih podatkov je v zagotavljanju pravice posameznika, da »obdrži informacije o sebi, ker noče, da bi bili z njimi seznanjeni tudi drugi[1].« Ker gre za temeljno človekovo pravico, njen javnopravni značaj pomeni tudi **varstvo posameznika pred posegi države** in njenih organov. Zato je poseg v to pravico s strani države možen le izjemoma in le pod določenimi pogoji, ki jih lahko določa le zakon. V vsakem primeru pa mora biti poseg utemeljen in sorazmeren.

»Poskrbeti moramo tudi za svobodo, ne le za varnost. Če nič drugega zato, ker ravno svoboda zavaruje varnost.«

Karl Popper

"We must plan for freedom, and not only for security, if for no other reason than that only freedom can make security secure"

Kot že rečeno, pa mora država – tudi z namenom zagotavljanja in uveljavljanja pravic svojih državljanov, zagotavljati učinkovitost svojega delovanja. Poskrbeti mora, da posameznik hitro in pravočasno pridobi npr. podatke ali dokumentacijo, ki jo potrebuje za uveljavljanje kakšne svoje pravice (npr. socialno varstvo) ali pa npr. podatke o svojih obveznostih do države (npr. davčne obveznosti). Hkrati mora država zagotavljati učinkovito varstvo svojih državljanov pred npr. storilci kaznivih dejanj ipd.

Pri svojem vsakdanjem delu državni organi zbirajo in obdelujejo številne osebne podatke posameznikov. Med njimi so pogosto tudi občutljivi osebni podatki (npr. zdravstveno stanje, narodnost ipd.). Tendence zagotavljanja kakovostnih, hitrih in učinkovitih storitev za državljane seveda vodijo v čedalje bolj izrazite želje in potrebe po povezovanju različnih virov podatkov, ki jih obdeluje državna uprava, med njimi pa je seveda tudi ogromna količina osebnih podatkov. Državljanom prijazna uprava lahko zlasti s pomočjo sodobnih informacijsko-komunikacijskih tehnologij (e-uprava) nudi nove (kakovostnejše) storitve in skrajša čas izvedbe že obstoječih (npr. z odpravo čakalnih vrst pred okenci državnih organov s storitvami e-uprave ipd.). Marsikateri podatek lahko državni organi pridobijo od drugih državnih organov, ne da bi za to morali obremenjevati državljana, kot se to odraža tudi v zahtevi 139. člena Zakona o splošnem upravnem postopku. Bistvenega pomena pri razvoju storitev za državljane[2] (in podjetja[3]) pa je seveda vzpostavitev ter optimizacija in racionalizacija tako imenovanih zalednih storitev (»back-office« ali G2G[4]), prek katerih si organi medsebojno izmenjujejo podatke. Številni projekti iz sklopa programa projektov e-uprave (e Pravosodje, e Zdravje, e Sociala, e Davki) narekujejo večjo povezljivost zbirk osebnih podatkov, s katerimi upravlja država.

Poleg navedenih usmeritev sodobne državne uprave k zagotavljanju učinkovitih storitev za državljane, pa k željam in potrebam po večjem dostopu in povezovanju podatkov prispevajo tudi aktivnosti na področju pregona kriminala, kot so projekt vzpostavitve Nacionalnega preiskovalnega urada ali uresničevanje Resolucije o nacionalnem programu preprečevanja in zatiranja kriminalitete 2007-2001. Ob omenjenih tendencah se nepoučeni pogosto vprašajo, čemu takšna decentralizacija podatkovnih zbirk - mar ne bi za učinkovitost države, njeno uspešnost zagotavljanja storitev državljanom in pregona kriminala najbolje delovala velika, centralna podatkovna zbirka?

1 Čebulj J. v: Komentar Ustave RS, str. 409.

2 G2C – Government to Citizen
3 G2B – Government to Business
4 G2G – Government to Government

Zbirka vseh zbirk?

Povezovanje vseh zbirk podatkov, ki jih posedujejo državni organi, v eno samo zbirko bi pomenilo prekomeren poseg v posameznikovo zasebnost. S tem bi namreč nastala zbirka vseh zbirk, ki bi vsakemu, ki bi vanjo vpogledal, o posamezniku povedala pravzaprav vse – morda več, kot bi vedel sam (še posebej ob upoštevanju podatkov, zbranih s strani policije). Kljub najstrožjemu nadzoru nad takšno zbirko, bi še vedno obstajala zelo velika nevarnost nepooblaščenega dostopa ali vdora, ki pa bi zaradi vsebine zbirke pomenila lahko za posameznika katastrofalne posledice. Dejstvo je, da je zbirka toliko bolj zanimiva za nelegalen dostop oz. vpogled, kolikor več informacij o posamezniku vsebuje. Osebni podatki posameznika imajo lahko tudi veliko komercialno vrednost, zato je lahko vdor v takšno zbirko toliko bolj privlačen. Po drugi strani pa se postavlja tudi vprašanje upravičenosti državnega aparata, da upravlja s takšno, vseobsegajočo zbirko.

O nevarnostih vzpostavljanja centraliziranih baz podatkov o posameznikih – državljanih s strani države pa nas lahko nauči tudi zgodovina. Popolni, centralizirani nadzor države nad svojimi državljani je bil cilj in želja že v nacistični Nemčiji, prav tako v Stalinovi Sovjetski zvezi. Medtem ko je v petdesetih letih prejšnjega stoletja George Orwell pisal o popolnem nadzoru države nad svojimi državljani (Velikem bratu) v obliki znanstvenofantastičnega romana »1984«, pa se je temu kasneje skušala približati Vzhodna Nemčija (NDR) s Stasijem[5]. Orwellov telekran in Miselna policija se ob Stasijevem zbiranju vonjev svojih državljanov ne zdita več tako zelo nemogoča. Popoln - centraliziran nadzor nad državljani je sicer jasen cilj totalitarnih sistemov, vendar pa si vsaka država želi imeti določen nadzor nad svojimi državljani. Določen nadzor je seveda tudi potreben in koristen tudi za državljane, vendar pa se postavlja vprašanje, kje postaviti mejo. Treba je upoštevati dejstvo, da je meja med »golim« preverjanjem posameznika in upravljanjem z njim zelo tanka – obdelava podatkov posameznikov lahko hitro predstavlja ne le nadzor v smislu vedenja o tem, kaj posameznik počne, kakšen je ipd. temveč tudi nadzor v smislu upravljanja s posameznikom. To so pokazali ravno našteti primeri totalitarnih sistemov. Dejstvo je, da se v vsaki državi oblast menjava in se menjavajo tudi politični režimi. Nemogoče je predvideti, kako bo želela z informacijami o posameznikih razpolagati vsakokratna oblast. Zato vzpostavitev zbirke vseh zbirk – se pravi zbirke, ki bi povezovala vse zbirke vseh organov državnega aparata v eno centralizirano zbirko, predstavlja zelo nevarno približevanje navedenim primerom totalitarnih sistemov. Nadzor torej mora ostati v mejah, kjer je resnično potreben. Pri tem pa je ključnega pomena, da se trezno presoja tudi posamične korake, ki vodijo v povezovanje zbirk osebnih podatkov. Varstvo zasebnosti je namreč kategorija, ki je zelo izpostavljena gradualizmu, kjer so majhni in postopni, toda stalni posegi v zasebnost praktično nezaznavni, agregat dejanskega posega v zasebnost pa je zaznaven šele na dolgi rok.

"Zloraba oblasti, avtokracija in tema nikoli ne pridejo hipoma, vedno je vmesno obdobje mračenja, ko se dan preveša v noč; biti moramo pozorni opazovalci okolja in varuhi luči, da ne postanemo nemočni ujetniki teme."

William O. Douglas,
(1898-1980), sodnik vrhovnega sodišča ZDA

"As nightfall does not come all at once, neither does oppression. In both instances, there is a twilight when everything remains seemingly unchanged. And it is in such twilight that we all must be most aware of change in the air - however slight - lest we become unwitting victims of the darkness."

Nevarnost vedno novega povezovanja zbirk osebnih podatkov pa predstavlja tudi dejstvo, da s tem nastajajo nove zbirke osebnih podatkov, kar v praksi lahko pripelje do obdelave osebnih podatkov v nasprotju z namenom njihovega zbiranja[6]. Gre za enega največjih strahov organov za varstvo osebnih podatkov in zasebnosti, in sicer gre za t. i. pojav »function creep«, ko se podatki prvotno zbirajo z enim namenom (ta je lahko tudi povsem legitimen in zakonit), nato se pa

5 »Ocenjujejo, da je v Hitlerjevem tretjem rajhu prišel en gestapovec na 2000 državljanov, v Stalinovi ZSSR pa je prišel en agent KGB-ja na 5830 ljudi. V NDR je prišel en agent Stasija ali ovaduh na 63 ljudi. Če bi prišteli še občasne ovaduhe, je po nekaterih ocenah razmerje celo en ovaduh na vsakih 6,5 državljana« Funder A., Zloglasni Stasi, Dokumenti in izpovedi obeh strani, 1966, prevod: Leskovar M., Tržič: Učila International, 2005, s. 65

6 Bien S., v: Pric Musar N. et al., Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem, GV Založba, Ljubljana, 2006, str. 459;

podatki uporabljajo za druge namene, dostop do podatkov se širi in tako naprej. Treba se je namreč zavedati, da se, ko so podatki enkrat zbrani, pogosto pojavijo težnje pa razširitvi namena, podaljšanju rokov hrambe in širjenju dostopa do zbranih podatkov.

Seveda povezovanje zbirk osebnih podatkov prinaša pozitivne strani tudi za posameznika, in sicer predvsem v poenostavljenosti postopkov pred posameznimi državnimi organi in v ažurnosti njegovih podatkov[7]. Vendar pa je treba v vsakem posamičnem primeru povezovanja dveh ali več zbirk osebnih podatkov temeljito premisliti, ali je takšno povezovanje resnično potrebno in sorazmerno. V določenih primerih namreč pozitivne posledice ne odtehtajo potencialnih negativnih posledic, ki bi jih takšno povezovanje lahko prineslo. Potrebno se je namreč zavedati specifičnosti varstva zasebnosti kot ene izmed temeljnih človekovih pravic. Posegi v posameznikovo zasebnost in dostojanstvo so namreč pogosto takšni, da ne omogočajo vrnitve v prejšnje stanje, s tem pa se lahko posamezniku povzročijo nepopravljive posledice in trajna škoda. Kot primer si lahko predstavljate razkritja (s strani posameznika sicer skrbno varovanega in zaupnega) podatka o družbeno stigmatizirani bolezni ali spolni nagnjenosti. Ko je enkrat takšen podatek razkrit, posameznik nima nobene možnosti za odpravo posledic, škoda je storjena in posledice za posameznika so lahko zelo velike.

7 Enako izhaja tudi iz določb Evropske konvencije o človekovih pravicah, glej spodaj;

Pregled zakonodaje s področja varstva osebnih podatkov

Kot že rečeno je področje varstva zasebnosti (in posledično tudi varstva osebnih podatkov) urejeno s številnimi mednarodnimi in nacionalnimi dokumenti. V evropskem prostoru je seveda najpomembnejši dokument na tem področju Evropska konvencija o človekovih pravicah.

Evropska konvencija o človekovih pravicah (EKČP)

EKČP v 8. členu izrecno določa, da ima vsak pravico do spoštovanja svojega zasebnega in družinskega življenja, svojega doma in korespondence, državni in drugi oblastni organi pa vanjo ne smejo posegati, razen če je v demokratični družbi to nujno, ker tako narekujeta javna korist ali varstvo pravic drugih, posegi pa so določeni z zakonom. Poseg države v varstvo osebnih podatkov posameznika je torej možen le pod navedenimi pogoji. Navedena določba je izvedena preko Konvencije o varstvu posameznikov glede na avtomatsko obdelavo podatkov[8] (v nadaljevanju KonVOP), katere načela[9] (poleg Ustave) predstavljajo glavno merilo za ureditev varstva osebnih podatkov v zakonu[10].

Seveda pa je za slovensko zakonodajo bistvenega pomena tudi Direktiva o varstvu osebnih podatkov 95/46/ES[11], katere namen je poenotenje pravnega reda držav članic EU glede varstva osebnih podatkov. Direktiva je bila implementirana v slovenski pravni red z Zakonom o varstvu osebnih podatkov[12] (v nadaljevanju: ZVOP-1).

Podlago za sprejem ZVOP-1 predstavlja 38. člen Ustave, po katerem je zagotov-

8 Ur. l. RS (28. 2. 1994)-MP, št. 3-18/1994 (RS 11/1994)

9 Temeljna načela KonVOP se nanašajo predvsem na zakonito in pošteno obdelavo, zakonite namene, sorazmerno obdelavo, ažurnost osebnih podatkov, sledljivost vpogledov v osebne podatke, posebno varstvo občutljivih osebnih podatkov, zavarovanje podatkov, in pravice posameznikov do vpogleda, poprave ali izbrisa svojih osebnih podatkov.

10 Čebulj J. v: Komentar Ustave RS, .., str. 409.

11 Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, UL L 281, 23. 11. 1995;

12 Ur. l. RS, št. (Uradni list RS, št. 94/07, uradno prečiščeno besedilo, v nadaljevanju ZVOP-1).

ljeno varstvo osebnih podatkov in je prepovedana njihova uporaba v nasprotju z namenom njihovega zbiranja, njihovo zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti pa določa zakon. Ustava določa tudi pravico posameznika do seznanitve s svojimi osebnimi podatki in pravico do sodnega varstva ob morebitni njihovi zlorabi.

ZVOP-1 predstavlja sistemski zakon s področja varstva osebnih podatkov. Podrobneje lahko varstvo osebnih podatkov na določenih področjih uredi področna zakonodaja. Pri tem pa seveda ne sme nasprotovati temeljnim načelom ZVOP-1, kot so načelo zakonite in poštene obdelave osebnih podatkov, načelo sorazmernosti ter prepoved diskriminacije glede varstva osebnih podatkov.

Direktiva 95/46/ES

Z namenom poenotenja zakonodaj držav članic EU s področja varstva zasebnosti je bila v letu 1995 sprejeta Direktiva št. 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov.

Direktiva že v recitalu 2 izrecno poudarja, da so sistemi za obdelavo podatkov namenjeni temu, da služijo človeku, in morajo, ne glede na državljanstvo ali stalno prebivališče fizičnih oseb, spoštovati njihove temeljne pravice in svoboščine, predvsem pravico do zasebnosti, ter prispevati h gospodarskemu in socialnemu napredku, trgovinskemu razvoju ter blaginji posameznikov. Pri tem pa v recitalu 4 Direktiva izpostavlja, da napredek v informacijski tehnologiji občutno olajšuje obdelavo in izmenjavo osebnih podatkov.

Iz Direktive izhaja, da je **obdelava osebnih podatkov mogoča pod določenimi pogoji**:

- **transparentnost** – posameznik, čigar osebni podatki se obdelujejo, mora biti obveščen o obdelavi, o tem, kdo obdeluje njegove osebne podatke, ter s kakšnim namenom;
- **dostop do lastnih podatkov in možnost ugovora** – posameznik mora imeti možnost dostopa do svojih osebnih podatkov, ki se obdelujejo, in mora imeti možnost zahtevati popravek, blokiranje ali izbris podatkov, ki so nepopolni, nepravilni ali se obdelujejo protipravno;
- **pravna podlaga** – osebni podatki se lahko obdelujejo le, če za to obstaja pravna podlaga (npr. tako določa zakon, privolitev posameznika, nujnost za izvršitev pogodbe ipd.)
- **zakonit namen** obdelave;
- **sorazmernost** obdelave – osebni podatki se lahko obdelujejo le, če so primerni, ustrezni in ne pretirani glede na namen obdelave.

Vsi navedeni pogoji pa morajo biti seveda izpolnjeni tudi v primeru povezovanja zbirk.

V 39. recitalu Direktiva izrecno opozarja na **posredovanje osebnih podatkov tretjim osebam** in obveznost upravljavca, da v takih primerih posameznika, na katerega se nanašajo osebni podatki, obvesti, ko se podatki začnejo zbirati, oz. najpozneje takrat, ko se prvič posredujejo tretji stranki. Vendar pa glede na recital 40 takšne obveznosti ni treba izpolniti:

- če je posameznik, na katerega se osebni podatki nanašajo, o tem že obveščen,
- če **zbiranje ali posredovanje izrecno zagotavlja zakonodaja**,
- če se informiranje posameznika, na katerega se nanašajo osebni podatki, izkaže za nemogoče ali bi vključevalo nesorazmerne napore, kar bi se lahko zgodilo, kadar je obdelava namenjena zgodovinskim, statističnim ali znanstvenim ciljem. V tem pogledu se lahko upošteva število posameznikov, na katere se osebni podatki nanašajo, starost podatkov in vsi sprejeti nadomestni ukrepi.

Pomembne pa so tudi določbe Direktive v zvezi s posebnimi vrstami osebnih podatkov. Tako npr. v 5. odstavku 8. člena določa, da se lahko **obdelava podatkov v zvezi s prekrški, kazenskimi obsodbami ali varnostnimi ukrepi** izvaja samo pod nadzorom uradnega organa (upravljavca zbirke osebnih podatkov) ali pa, če nacionalna zakonodaja določi ustrezne posebne zaščitne ukrepe ob upoštevanju odstopanj, ki jih lahko zagotovi država članica na podlagi nacionalnih predpisov, ki določajo ustrezne posebne zaščitne ukrepe. Vendar pa se popoln register kazenskih obsodb lahko vodi samo pod nadzorom uradnega organa. Države članice lahko določijo, da se podatki v zvezi z upravnimi kaznimi ali sodbami v civilnih zadevah lahko tudi obdelujejo pod nadzorom uradnega organa.

Zakon o varstvu osebnih podatkov (ZVOP-1)

Povezovanje zbirk osebnih podatkov je urejeno v 26., 27., 84., 85. in 86. členu ZVOP-1.

Pogoji za povezovanje zbirk osebnih podatkov so v skladu z navedenimi členi ZVOP-1 naslednji:

1. zbirke osebnih podatkov iz uradnih evidenc in javnih knjig je dovoljeno povezovati le, če tako **določa zakon**;
2. upravljavci osebnih podatkov, ki povezujejo zbirke osebnih podatkov, ki se vodijo **za različne namene**, so dolžni o tem **predhodno pisno obvestiti Informacijskega pooblaščenca**;
3. upravljavci osebnih podatkov, ki povezujejo zbirke osebnih podatkov iz uradnih evidenc ter javnih knjig, **morajo podatke o povezanih zbirkah osebnih podatkov navesti v 12. točki katalogov zbirk podatkov** (26. člen ZVOP-1) ter navedene podatke skladno z določbami 27. člena ZVOP-1 **v osmih dneh po vzpostavitvi povezave za namene vodenja registra zbirk osebnih podatkov posredovati Pooblaščencu**;
4. podatki o povezanih zbirkah osebnih podatkov iz uradnih evidenc ter javnih knjig se morajo **v registru zbirk osebnih podatkov voditi posebej**[13];
5. **povezovanje ni dovoljeno brez predhodnega dovoljenja Informacijskega pooblaščenca**, če:
   - vsaj ena zbirka osebnih podatkov, ki naj bi se jo povezalo, vsebuje občutljive podatke, ali
   - bi povezovanje imelo za posledico razkritje občutljivih podatkov, ali
   - je za izvedbo povezovanja potrebna uporaba istega povezovalnega znaka (pri nas so to EMŠO, davčna številka in številka zdravstvenega zavarovanja);

V takšnem primeru Informacijski pooblaščenec dovoli povezavo na podlagi pisne vloge upravljavca, če ugotovi, da upravljavci zagotavljajo ustrezno zavarovanje osebnih podatkov (zavarovanje v skladu s 14. in 24. členom ZVOP-1).

Povezovanje v primeru prekrškovnih in kazenskih evidenc

V 85. členu ZVOP-1 izrecno prepoveduje:

- povezovati zbirke osebnih podatkov **iz kazenske evidence z drugimi zbirkami** osebnih podatkov;
- povezovati zbirke osebnih podatkov **iz prekrškovnih evidenc z drugimi zbirkami** osebnih podatkov;
- povezovati zbirke osebnih podatkov iz kazenske in prekrškovne evidence.

Za takšno ureditev obstaja več razlogov. Bistveni razlog je, da gre pri prekrškovnih in kazenskih evidencah za obdelavo občutljivih osebnih podatkov. Posledično tudi področna zakonodaja (Kazenski zakonik oz. Zakon o prekrških) določa stroge pogoje glede posredovanja podatkov iz kazenske oz. prekrškovne evidence.
Komentar ureditve povezovanja v ZVOP-1

Komentar ureditve povezovanja v ZVOP-1

Strogost pogojev za povezovanje zbirk osebnih podatkov je pogojena tudi z dejstvom, da upravljavcu o povezavi zbirk ni treba obvestiti posameznika, čigar osebni podatki se nahajajo v teh zbirkah. Zato je bilo treba določiti varovalke, ki preprečujejo nevarnosti in arbitrarnost pri povezovanju zbirk. Bistvenega pomena pri določanju zakonskih pogojev za povezovanje zbirk osebnih podatkov je bilo tudi dejstvo, da v slovenskem pravnem redu »prevladuje t. i. registrska ureditev, katere bistvo je v večnamenskem zbiranju podatkov v registrih in evidencah, ki dogodek zabeležijo čim bliže nastanku, in sicer v obliki, ki omogoča njihovo nadaljnjo uporabo[14]. Tak način organizacije države, kjer je z zakonom urejeno vodenje registrov na lokalni in nacionalni ravni, sicer kot že rečeno prinaša pozitivne posledice tako za državo (racionalizacija dela, ažurnost podatkov) kot tudi za posameznika (razbremenjevanje posameznika, ažurnost podatkov), vendar pa hkrati prinaša že navede nevarnosti zlorab, nesorazmernega centraliziranega nadzora nad posameznikom in obdelave osebnih podatkov v nasprotju s prvotnim namenom. Zato je bila postavitev določenih pogojev za vzpostavitev takšnih povezav nujna.

Pojasnilo glede termina povezovanje v kontekstu 6. poglavja VI. dela ZVOP-1

Do nerazumevanja pojma »povezovanje« v kontekstu ZVOP-1 prihaja iz razloga, ker navedeni pojem v zakonu ni definiran, zaradi česar si je pojem povezovanja mogoče različno predstavljati oziroma si ga predstavljamo na različnih ravneh.

13 http://www.ip-rs.si/varstvo-osebnih-podatkov/register-zbirk/povezava-zbirk-osebnih-podatkov/seznam-izdanih-odlocb-o-povezljivosti-zbirk-osebnih-podatkov/

14 Bien S., v: Pric Musar N. et al., Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem, 2006, str. 459, 460;

Tako lahko laično rečemo, da je tudi za uporabo elektronske pošte, obisk spletne banke ali oddajo dohodnine po elektronski poti potrebno neke vrste povezovanje, ki omogoča prenos podatkov med virom (npr. spletno mesto) in ponorom (obiskovalci spletnega mesta). Če namreč vir in ponor ne bi bila na tak ali drugačen način povezana, pretok podatkov ne bi bil možen. Vendar v teh primerih ne gre za povezovanje kot ga opredeljuje ZVOP-1. Določbe o povezovanju v kontekstu ZVOP-1 se nanašajo izključno na povezovanje zbirk osebnih podatkov iz **uradnih evidenc in javnih knjig**. Potrebna pogoja sta torej, prvič, da gre za osebne podatke, in drugič, da se ti podatki nahajajo v zbirki osebnih podatkov iz uradnih evidenc in javnih knjig. Povezovanje zbirk osebnih podatkov po določbi 1. odst. 84. čl. ZVOP-1 obsega le t.i. avtomatsko, elektronsko povezovanje zbirk osebnih podatkov.

Uvodoma je potreben razmislek o namenu (*ratio legis*) določbe o povezovanju osebnih podatkov iz javnih knjig in uradnih evidenc. Lahko trdimo, da je zakonodajalec želel preprečiti nastanek situacije, ko bi lahko upravljavec osebnih podatkov na enem mestu hkrati dostopal do osebnih podatkov določene osebe, ki se sicer nahajajo v različnih zbirkah osebnih podatkov enega ali več upravljavcev osebnih podatkov in se vodijo za različne namene. Če bi bile zbirke povezane, bi lahko upravljavec osebnih podatkov npr. na enem mestu dobil podatke iz CRP, evidence brezposelnih oseb, registra davčnih zavezancev, kazenske evidence in podobno. In obratno, če zbirke ne bi bile povezane, bi moral podatke pridobiti iz vsake zbirke posebej.

Na tem mestu je potrebno poudariti, da dostopa uporabnikov enega upravljavca do podatkov iz zbirk drugega upravljavca še ne moremo nujno šteti za povezanost v smislu povezovanja zbirk osebnih podatkov, čeprav drži, da morata biti tako uporabnik kot ponudnik podatkov na nek način povezana (uporabljati morata npr. iste protokole in kompatibilno računalniško opremo), da do izmenjave podatkov sploh lahko pride.

Ločiti moramo namreč **posredovanje** osebnih podatkov ter **povezovanje** osebnih podatkov (ožja in širša definicija).

Posredovanje osebnih podatkov (22. člen ZVOP-1)

Pri posredovanju osebnih podatkov gre za **razmerje med (enim) upravljavcem in (enim) uporabnikom podatkov**. Pri vpogledu ali dostopu do podatkov v zbirki osebnih podatkov, ne da bi tako pridobljene podatke neposredno in brez dodatnih posegov vključili v drugo zbirko, gre zgolj za posredovanje osebnih podatkov, ki je urejeno v 22. čl. ZVOP-1, in ne za povezanost zbirk osebnih podatkov, kot je urejena v 6. poglavju ZVOP-1. Pri tem je tehnična implementacija posredovanja ali povezanosti zbirk lahko različna, a ne more biti kriterij razlikovanja, ali gre za posredovanje ali za povezanost zbirk osebnih podatkov, temveč je pri tem ključen **namen in način obdelave osebnih podatkov**. Upravljavec osebnih podatkov mora 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. Na tem mestu je potrebno poudariti, da je prejemnik podatkov zgolj **uporabnik podatkov,** in ne upravljavec prejetih podatkov (če podatke nato vključi v svoje zbirke, pa seveda postane tudi upravljavec).

Primer posredovanja osebnih podatkov

Informacijski pooblaščenec (IP) uporablja za pridobitev določenih osebnih podatkov o kršiteljih v prekrškovnem postopku spletno storitev e Poizvedbe Zavoda za zdravstveno zavarovanje (ZZZS). V primeru, ko npr. nima podatka o EMŠO kršitelja, se s pomočjo digitalnega potrdila prijavi v spletno storitev e Poizvedbe in pridobi ta podatek z vnosom imena in priimka ter datuma rojstva iskane osebe. Opravljena poizvedba se sicer zabeleži tako na strani IP kot na strani ZZZS, vendar pa sistem ne omogoča neposrednega prenosa ali vključitve dobljenih podatkov v katero od zbirk IP, saj zbirke ZZZS in zbirke IO med seboj niso neposredno povezane. Gre torej za razmerje med upravljavcem osebnih podatkov (ZZZS) in uporabnikom (IP).

Povezovanje zbirk osebnih podatkov

Za razliko od posredovanja lahko za povezovanje štejemo, da sta zbirki osebnih podatkov povezani, če se določeni podatki iz ene zbirke neposredno vključijo

v drugo zbirko, s čimer se druga zbirka spremeni (poveča, ažurira ipd.), pri tem pa gre lahko zgolj za enosmeren tok podatkov. Povezanost zbirk osebnih podatkov torej predpostavlja vključitev podatkov v drugo zbirko na način, da se določeni podatki iz ene zbirke zaradi neposredne povezanosti zbirk prenesejo ali vključijo v drugo povezano zbirko. **Pri povezanosti zbirk osebnih podatkov uporabniku ni potrebno vstopati v vsako zbirko posebej.**

Ločimo lahko ožjo in širšo definicijo povezovanja.

Ožja definicija pojma povezovanje zbirk osebnih podatkov

Pri ožji definiciji povezovanja gre za integracijo podatkov, ki zasleduje cilje odprave neskladja virov, ažurnosti, točnosti, popolnosti in zanesljivosti zbranih podatkov predvsem z uveljavljanjem principa hrambe in ažuriranja na enem mestu ter uporabe ažuriranih podatkov na več mestih. Zbirke osebnih podatkov so po ožji definiciji povezane tako, da se sprememba **določenega podatka odrazi v vseh povezanih zbirkah**, bodisi samodejno oziroma v realnem času (»push« princip) bodisi na zahtevo povezane zbirke (»pull« princip).

Primer povezave v ožjem smislu:
Če se določen podatek spremeni v eni izmed povezanih zbirk (npr. sprememba podatka o stalnem prebivališču posameznika v CRP) se ta sprememba odrazi v vseh povezanih zbirkah.

Širša definicija pojma povezovanja zbirk osebnih podatkov

V primeru, ko so zbirke povezane na način, da upravljavec komunicira z eno zbirko osebnih podatkov, ta pa je v ozadju neposredno povezana z drugimi zbirkami (znotraj enega ali več upravljavcev), moramo tudi to šteti za povezovanje zbirk podatkov, **ne glede na to, da se podatki ne ažurirajo hkrati v vseh povezanih zbirkah**. Tudi v takšnih primerih lahko namreč uporabnik osebnih podatkov pri delu s svojo zbirko osebnih podatkov hkrati **pridobi tudi določene podatke iz (vseh) povezanih zbirk** in jih neposredno vključi v svojo zbirko, **ne da bi za to moral vstopati v vsako zbirko posebej**. O povezovanju v širšem smislu govorimo tudi takrat, ko uporabnik v svojo zbirko vnese določene osebne podatke posameznika, sistem pa za tem zbirko samodejno ali na zahtevo uporabnika dopolni še z določenimi podatki iz drugih povezanih zbirk. Takšno povezovanje ima seveda določene prednosti (hitrejša in enostavnejša pridobitev podatkov, odprava neskladja virov, večja ažurnost, točnost, popolnost ter zanesljivost podatkov), po drugi strani pa takšna povezava lahko pomeni tudi nezakonit in prekomeren poseg v zasebnost posameznika, saj si upravljavec osebnih podatkov na takšen način na enem mestu pridobi in združi podatke iz zbirk, ki se vodijo za različne namene.

Primer povezave v širšem smislu:
Zbirke je mogoče povezati na način, da upravljavec, ki v svoji zbirki osebnih podatkov opravi priklic podatkov določenega posameznika, s tem dejanjem prikliče tudi določene podatke o tem posamezniku iz tistih zbirk podatkov, ki so neposredno povezane z njegovo zbirko. Pri takšnem povezovanju se podatki ažurirajo samo v zbirki, v katero neposredno dostopa posameznik, ne pa tudi v drugih povezanih zbirkah. Podatki se pri takšnem povezovanju ažurirajo samo v času poizvedbe, kasnejša sprememba podatkov v izvorni zbirki pa se ne odrazi s spremembo podatkov v povezanih zbirkah. Kor primer lahko vzamemo organ javne uprave, kateremu se takoj za tem, ko je v svojo zbirko podatkov vnesel EMŠO, s pomočjo vzpostavljene neposredne povezave med njegovo zbirko in npr. centralnim registrom prebivalstva (CRP), v njegovo zbirko iz CRP prenesejo še podatki o osebnem imenu ter stalnem in začasnem prebivališču določene fizične osebe. Na ta način organ v tistem trenutku pridobi točne in ažurne podatke iz CRP, postopek pridobitve in vnosa podatkov se hitreje izvede, sami podatki pa so bolj točni in ažurni, kot bi bili v primeru, če bi organ osebno ime ter podatke o prebivališču vnesel ročno.

Podobno je v primeru avtomatizacije in informatizacije postopka izvršbe, katere eden izmed ciljev je tudi avtomatizirano preverjanje in pridobivanje podatkov iz zunanjih izvornih evidenc. Glavni namen povezave je namreč vzpostavitev vodenja postopka izvršbe na podlagi verodostojne listine do faze vročitve pravnomočnega sklepa o dovolitvi izvršbe, in sicer na enem mestu in s pomočjo učinkovite informacijske podpore. Udeležencem postopka – predvsem upnikom - se želi omogočiti, da v najkrajšem možnem času pridobijo sklep o dovolitvi izvršbe. V končni fazi je cilj, da lahko sodišče za namene vodenja izvršilnega postopka ter s tem povezanim vodenjem zbirke osebnih podatkov (izvršilni vpisnik), s pomočjo povezave zbirk osebnih podatkov pridobi točne podatke, ne da bi se morali za podatke obrniti na vsakega upravljavca zbirk osebnih podatkov posebej (npr. DURS, ZZZS, Banko Slovenije, KDD ipd.). Gre torej za povezovanje po širši definiciji povezovanja v kontekstu ZVOP-1, saj sistem po vnosu dolžnikovih osebnih podatkov v izvršilni vpisnik, s pomočjo vzpostavljene povezave med

izvršilnim vpisnikom in registrom davčnih zavezancev, v registru davčnih zavezancev samodejno preveri obstoj dolžnika in v primeru iskanja po imenu in priimku ter naslovu podatke v izvršilnem vpisniku dopolni še z davčno številko. Za tem sistem po pravnomočnosti sklepa o izvršbi, na podlagi davčne številke, v registru davčnih zavezancev sam pridobi še podatke o bankah, kjer ima dolžnik transakcijski račun ter podatke o dolžnikovi zaposlitvi, ter tako pridobljene podatke shrani v izvršilni vpisnik. Gre torej za povezovanje po širši definiciji povezovanja v kontekstu ZVOP-1, saj se podatki ažurirajo samo v zbirki, ki pridobiva podatke (izvršilni vpisnik), poleg tega pa se podatki ažurirajo samo v času poizvedbe, kasnejša sprememba podatkov v registru davčnih zavezancev pa se ne odrazi s spremembo že pridobljenih podatkov v izvršilnem vpisniku.

Pooblaščenec je mnenja, da 6. poglavje VI. dela ZVOP-1 ureja povezovanje tako po ožji kot po širši definiciji povezovanja. V obeh primerih namreč obstaja možnost, da upravljavec osebnih podatkov na enem mestu pridobi osebne podatke določene osebe, ki se sicer nahajajo v različnih zbirkah osebnih podatkov enega ali več upravljavcih, s tem pa lahko pride do tega, da se podatki uporabljajo v nasprotju s prvotnim namenom njihovega zbiranja (16. člen ZVOP-1). ZVOP-1 zato izrecno določa kavtele, ki preprečujejo nevarnosti in arbitrarnost pri povezovanju zbirk.

Bistveni element razlikovanja med posredovanjem podatkov iz 22. člena ZVOP-1 ter med povezovanjem zbirk osebnih podatkov iz 6. poglavja VI. dela ZVOP-1 je torej v tem, da mora odgovorna oseba v primerih posredovanja oz. pridobivanja podatkov po 22. členu ZVOP-1 vstopiti v **vsako zbirko posebej,** medtem ko je v primeru povezovanja zbirk osebnih podatkov potrebno **vstopiti le v eno zbirko, sistem pa ob tem omogoči pridobitev določenih osebnih podatkov tudi iz povezanih zbirk.**

Je povezovanje podatkov res rešitev?

Pojasnili smo pravne podlage za povezovanje zbirk osebnih podatkov v javnem sektorju, v nadaljevanju pa se posvečamo še vprašanju primernega pristopa k uresničevanju potreb po podatkih, ki jih ima javni sektor.

Kot smo navedli v uvodu, je z vidika spoštovanja temeljne človekove pravice posameznika do zasebnosti predvsem problematično povezovanje zbirk osebnih podatkov, ki se o posamezniku vodijo za različne namene. Iz navedenega razloga je zelo pomembno, da se pred dejanskim povezovanjem zbirk osebnih podatkov premisli o tem, ali je povezovanje dejansko potrebno oziroma ali bi lahko do podatkov, ki jih potrebujemo, prišli tudi na drug zakonsko dopusten in izvedbeno enostavnejši način.

Upravljavci zbirk osebnih podatkov bi po izkušnjah Pooblaščenca marsikdaj lahko podatke pridobivali na podlagi posamičnih zahtev, ki terjajo občutno manj vloženih sredstev kot povezovanje zbirk. Posamične zahteve po podatkih, ki jih lahko štejemo za posredovanje (in ne povezovanje zbirk osebnih podatkov) lahko temeljijo na sodobnih spletnih servisih, kjer se zagotovi preverjanje obstoja oz. ustreznosti pravne podlage ter beležijo podatki o izvedenih poizvedbah in posredovanih podatkih, na ta način pa je možno naknadno preverjanje upravičenosti in namenske uporabe podatkov. Ob tem je potrebno še zagotoviti, da je pridobivanje osebnih podatkov v mejah pooblastil posameznega uporabnika, kar pomeni, da lahko posamezni uporabnik pridobi le tiste vrste osebnih podatkov, za katere ima pravno podlago.

Posamično poizvedovanje se lahko izvede tudi kot paketno, seveda, če obstaja ustrezna pravna podlaga in sledljivost posredovanih podatkov. 3. odstavek 22. člena ZVOP-1 namreč 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.

Šele tam, kjer tovrstno posamično poizvedovanje po podatkih ne ustreza potrebam po podatkih (npr. zaradi nestrukturiranosti poizvedb oz. v času spreminjajočih se potreb po podatkih), je smiselno preučiti možnosti za stalnejšo povezavo z virom podatkov, ki pa mora seveda biti izvedena ob že omenjenih

zakonskih pogojih glede dopustnosti povezovanja in postopka obveščanja nadzornega organa oz. pridobitve ustreznega dovoljenja. Predvsem pa je potrebno paziti, da se iz ene zbirke v drugo prenašajo le podatki, ki so potrebni in zapisani v zakonu, in ne kar vsi podatki ene zbirke.

Načeli dostopnosti in iskanja pri (omejeno) javno dostopnih zbirkah osebnih podatkov

Informacijski pooblaščenec se je v praksi pogosto srečal tudi s težavami glede možnosti iskanja po javno objavljenih podatkih, in sicer zlasti takrat, ko naj bi določeni podatki bili javno dostopni, ni pa javno dostopna celotna zbirka podatkov.

Potrebno je ločevati med javno objavo podatkov in možnostmi iskanja po javno objavljenih podatkih, saj so posledice enega in drugega z vidika varstva osebnih podatkov lahko zelo različne. Specificiranje iskanja v smislu definiranja vhodnih in izhodnih podatkov ni smiselno takrat, ko je celotna zbirka podatkov javno dostopna. V takšnih primerih iskanje ne služi namenu varovanja oz. omejevanja dostopa do podatkov, temveč je zgolj metoda, ki olajša iskanje že objavljenih podatkov.

Ključni problem, ki ga je potrebno rešiti pri zbirkah, ki naj bi sicer bile javno dostopne, je varovanje osebnih podatkov, ki imajo lastnosti enoličnih identifikatorjev in se nahajajo v takšnih zbirkah. Če zbirka v celoti ni javno dostopna, je potrebno preprečiti možnosti t.i. zbiranja osebnih podatkov (angl. harvesting), in nenadzorovanega ustvarjanja novih zbirk osebnih podatkov, ki se lahko nato uporabijo za namene, ki niso skladni tistim, za katere so bili podatki primarno zbrani.

Pooblaščenec priporoča upoštevanje naslednjih načel glede iskanja po zbirkah, ki vsebujejo enolične identifikatorje (na primeru EMŠO) in ki niso v celoti javno dostopne:

- za pridobitev **več podatkov kot zgolj zadetek/ni zadetka** in preprečevanje zbiranja osebnih podatkov je potrebno vnesti toliko podatkov, da je posameznik enolično določen (npr. ime in priimek in EMŠO ali ime in priimek, naslov in rojstni datum, vse te podatke je potrebno vnesti torej kumulativno);
- EMŠO v nobenem primeru ne sme biti izhodni podatek. Lahko je vhodni podatek za iskanje (le pri principu zadetek/ni zadetka), lahko se nahaja v zbirki osebnih podatkov, v nobenem primeru pa ne sme biti izhodni podatek.

1. Vhodni podatek: EMŠO

Če je vhodni podatek samo EMŠO, potem lahko iskalnik vrne **samo podatek**, ali je oseba s tem EMŠO v zbirki ali ne (zadetek/ni zadetka, angl. hit/no hit). Zelo pomembno se je zavedati, da o sistemu zadetek /ni zadetka lahko govorimo le takrat, ko sistem ne poda nobenih drugih izhodnih podatkov, ki bi omogočale nadaljnje iskanje. Iskalnik tako lahko vrne tudi podatek o opravilni številki zadeve le v primeru, da opravilna številka ni vhodni podatek za nadaljnje iskanje - analogno velja za vse ostale izhodne podatke, ki bi lahko omogočali nadaljnje iskanje.

Na tem mestu opozarjamo tudi na določbe 20. člena ZVOP-1, ki za določene zbirke osebnih podatkov (s področja zdravstva, policije, obveščevalno-varnostne dejavnosti države, obrambe države, sodstva in državnega tožilstva ter kazenske evidence in prekrškovnih evidenc) izrecno prepoveduje pridobivanje osebnih podatkov na način, da bi se uporabil samo isti povezovalni znak (ta določba se ne uporablja za zemljiško knjigo in sodni register). Ta se izjemoma lahko uporabi za pridobivanje osebnih podatkov, če je to edini podatek v konkretni zadevi, ki lahko omogoči, da se odkrije ali preganja kaznivo dejanje po uradni dolžnosti, da se zavaruje življenje ali telo posameznika ali da se zagotovi izvajanje nalog obveščevalnih in varnostnih organov, določenih z zakonom. O tem je potrebno brez odlašanja napraviti uradni zaznamek ali drug pisni zapis.

Možnost iskanja zgolj po EMŠO je z vidika narave EMŠO kot enoličnega identifikatorja izrazito problematična, če sistem ne deluje po načelu zadetek/ni zadetka, temveč omogoča pridobitev več izhodnih podatkov. Takšno iskanje namreč omogoča nenadzorovano pridobivanje podatkov o posamezniku (angl. *harvesting*) in ustvarjanje novih zbirk osebnih podatkov.

Podobno ureditev lahko iščemo v primeru preverjanja veljavnosti identifikacijskih dokumentov, ki je možno na spletnih straneh e-uprave:

Posameznik izbere tip dokumenta, vhodni podatek pa je podatek o številki dokumenta. Rezultat iskanja je v tem primeru **zgolj podatek o tem, ali se osebni dokument z vnesenimi vhodnimi podatki nahaja v zbirki ali ne (zadetek/ni zadetka)**, ne pa več podatkov, ki so povezani z vnesenim vhodnim podatkom (npr. kdo je lastnik konkretnega dokumenta).

2. Vhodni podatek: ime in priimek ter naslov

V primeru iskanja po imenu in priimku in naslovu, lahko iskalnik vrne samo naslednje zadetke:

- da je oseba s temi podatki bazi,
- da osebe s temi podatki v bazi ni,
- da obstaja več oseb s takšnimi podatki in da je potrebno dodatno vnesti bodisi rojstni datum bodisi EMŠO.

3. Vhodni podatek: ime in priimek in EMŠO ali ime in priimek, naslov in rojstni datum[15]

Iskalnik lahko vrne **vse podatke razen EMŠO samo pri takšnem iskanju**, saj oseba, ki izvaja iskanje, že razpolaga z dovolj podatki za **enolično identifikacijo iskanega posameznika** in samo preverja neko dejstvo.

Analogijo lahko iščemo v primeru vpogleda v podatke o vozilih, kjer je potrebno vnesti registrsko številko vozila in številko prometnega dovoljenja, da lahko dobimo več podatkov, kot samo zadetek/ni zadetka. V nasprotnem primeru bi recimo že samo z registrsko številko lahko prišli do podatkov, kar se pa lahko zlorabi za nenadzorovano zbiranje in ustvarjanje novih zbirk podatkov.

Iskanja po drugih vhodnih podatkih (npr. že samo po opravilni številki) ali drugačnih kombinacijah vhodnih podatkov (npr. opravilna številka in naziv sodišča) ne bi smela biti dovoljena.

15 V RS po podatkih Statističnega urada RS ni dveh posameznikov, ki bi imela isto ime in priimek, bila rojena istega dne in ki bi živela na istem naslovu.

Zahteve z vidika zavarovanja osebnih podatkov

Zavarovanje osebnih podatkov (angl. *data security*) moramo ločiti od izraza varstvo osebnih podatkov (angl. *data protection*). Zavarovanje je le podmnožica širšega pojma varstvo osebnih podatkov. Da lahko podatke ustrezno varujemo, jih je seveda potrebno zavarovati, torej zaščititi pred nepooblaščenimi dostopi in uporabami, poleg zavarovanja pa je seveda bistveno, da za obdelavo sploh razpolagamo z ustrezno pravno podlago, da podatke uporabljamo samo za namene, za katere so bili zbrani, da spoštujemo pravice posameznika in tako dalje. Zavarovanje je tako le del varstva osebnih podatkov, gotovo pa gre za enega najpomembnejših elementov. Glede na to, da gre pri zavarovanju v osnovi za zavarovanje podatkov oz. informacij, je smiselno iskati smernice v uveljavljenih standardih varovanja informacij. Primer mednarodno uveljavljenega standarda, ki je tehnološko neodvisen, namenjen pa zavarovanju tako elektronsko kot papirno obdelovanih podatkov, je standard ISO/IEC 27001:2005[16], saj gre **za sistematičen in celovit pristop k upravljanju informacijske varnosti**. Standard ISO/IEC 27001:2005 je primeren predvsem z organizacijskega vidika, torej z vidika mehanizmov in postopkov, medtem ko se je za tehnične vidike potrebno opreti na druge, bolj tehnično naravnane standarde in dobre prakse kot so COBIT[17], ITIL[18] ipd. Podrobnejše opisovanje omenjenih dobrih praks bi preseglo obseg in namen teh smernic, vsekakor pa gre za napotitev na dobre prakse, ki jih je z vidika upravljavcev smiselno preučiti in jim slediti. Po mnenju Pooblaščenca bi moral organi javne uprave, ki povezujejo zbirke osebnih podatkov, vzpostaviti, izvajati ter vzdrževati sistem za upravljanje varovanja informacij (SUVI), kot to priporoča omenjeni ISO standard.

Ko govorimo o uveljavljenih standardih in postopkih za varnost v informacijskih sistemih imamo v mislih predvsem tako imenovani pristop AAA, ki temelji na treh temeljih varnosti, ki so v angleškem jeziku poimenovani authentication, authorization in accountability. Razlog za odločitev, da se v smernicah predstavi ta pristop, temelji predvsem na dejstvu, da se v informacijski družbi velika večina podatkov zbira, hrani in obdeluje s pomočjo sredstev informacijsko komunikacijskih tehnologij. Teorije varnosti informacijskih sistemov so torej izrednega pomena za varnost osebnih podatkov, ki se v teh sistemih nahajajo in obdelujejo. Sodobne informacijsko komunikacijske tehnologije nudijo izredne možnosti za obdelavo osebnih podatkov, saj se ti lahko obdelujejo veliko hitreje, v večjih količinah, boljša je tako časovna kot prostorska dostopnost do podatkov, s tem pa pridejo tudi nova tveganja za varnost podatkov v informacijskih sistemih. Princip AAA je tehnološko nevtralen in neodvisen od vrste informacijskega sistema ali uporabljenih tehnologij in je kot tak zelo uporaben za opredeljevanje ustreznih postopkov in ukrepov za zavarovanje osebnih podatkov.

Prvi element principa AAA je avtentikacija (angl. authentication), gre pa za postopek, v katerem ugotavljamo istovetnost identitete, ki jo izkazuje uporabnik, ki želi dostopati do informacijskega sistema oziroma do podatkov, ki se v njem hranijo. Z drugimi besedami z vidika zavarovanja osebnih podatkov – gre za to, kako preverjamo identiteto oseb, ki lahko dostopajo do osebnih podatkov.

Drugi element principa AAA je avtorizacija (angl. authorization). Postopek avtorizacije definira uporabnikom, skupinam uporabnikov, storitvam ali procesom pravice dostopa do celega ali delov informacijskega sistema, storitev, aplikacij in drugih elementov. Z vidika zavarovanja osebnih podatkov – do katerih osebnih podatkov lahko dostopajo pooblaščene (avtentificirane) osebe in kaj lahko s podatki počno (t. i. **dostopne pravice**).

Tretji ključni element varnosti po principu AAA je sledljivost oz. možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil (angl. *accountability*).

Upravljavec, ki želi in mora ustrezno zavarovati osebne podatke, mora poskrbeti, da zagotavlja vse tri AAA sorazmerno z naravo osebnih podatkov in tveganjem, ki ga predstavlja obdelava določenih osebnih podatkov.

16 ISO / IEC 27001je standard za vzpostavitev in upravljanje informacijske varnosti (ISMS) standard, ki ga je sprejela Mednarodna organizacija za standardizacijo (ISO) in Mednarodna elektrotehnična komisija (IEC).

17 COBIT je skupek najboljših praks (okvir) za informacijsko tehnologijo (IT) za upravljanje, ki jih ustvarja Information Systems Audit and Control Association (ISACA) ter IT Governance Institute (ITGI). COBIT zagotavlja upravljavcem, revizorjem in IT uporabnikom z vrsto splošno sprejetih ukrepov, indikatorjev, procesov in najboljših praks orodje za upravljanje in maksimiranje koristi, pridobljenih z uporabo informacijske tehnologije .

18 The Information Technology Infrastructure Library (ITIL) je skupek konceptov in politik za upravljanje informacijske tehnologije (IT), infrastrukturo, razvoj in delovanje. ITIL vsebuje podroben opis številnih pomembnih IT praks s seznami, nalogami in postopki, ki jih je mogoče prilagoditi za vse IT vidike organizacije.

Osnovne zahteve glede zavarovanja

1. odstavek 24. člena ZVOP-1 določa, da zavarovanje osebnih podatkov obsega **organizacijske, tehnične in logično-tehnične postopke in ukrepe**, s katerimi se varujejo osebni podatki, preprečuje **slučajno ali namerno nepooblaščeno uničevanje podatkov**, njihova **sprememba** ali **izguba** ter **nepooblaščena obdelava** teh podatkov tako, da se:

1. varujejo prostori, oprema in sistemsko programska oprema, vključno z vhodno-izhodnimi enotami;
2. varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
3. preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;
4. zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;
5. omogoča **poznejše ugotavljanje, kdaj so bili posamezni osebni podatki** vneseni v zbirko osebnih podatkov, uporabljeni ali drugače **obdelani** in **kdo** je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

1. točka 1. odstavka 24. člena ZVOP-1 narekuje varovanje prostorov, opreme in sistemsko programske opreme, vključno z vhodno-izhodnimi enotami. Če ostanemo v domeni zbirk osebnih podatkov, ki se povezujejo, mora upravljavec zagotoviti fizično varovanje prostorov, kjer se nahaja oprema, ki je vključena v povezovanje (strežniška oprema, delovne postaje ipd.), pri čemer ne gre pozabiti na zavarovanje vhodno-izhodnih enot, ki omogočajo dostop do podatkov.

Sama aplikativna programska oprema mora glede na zahteve 2. točke 1. odstavka 24. člena ZVOP-1 zagotavljati, da je dostop do podatkov skladen s pooblastili določenega uporabnika, že omenjene dostopne pravice pa morajo biti dokumentirane. Mehanizmi za varovanje logičnega dostopa, kot so gesla, morajo biti opredeljeni v ustrezni politiki, ki določa pravila glede dolžine, veljavnosti, menjave in ostalih relevantnih vidikov. Upravljavec mora izvajati t.i. politiko čistega zaslona, o čemer morajo biti zaposleni primerno podučeni.

3. točka 1. odstavka 24. člena ZVOP-1 zahteva avtentikacijo in avtorizacijo vira in ponora podatkov pred pridobivanjem podatkov, prav tako pa je pri povezovanju zbirk osebnih podatkov zelo pomembno zavarovanje pred nepooblaščenim prestrezanjem, prisluškovanjem ali potvarjanjem podatkov med samim prenosom – uporabljene morajo biti rešitve za varovanje med prenosom in zagotavljanje nečitljivosti nepooblaščenim osebam, ki preprečujejo navedene zlorabe (npr. kriptirni postopki in varni protokoli, npr. SSL, VPN, IPSEC, digitalni certifikati …). Podatki, ki se pridobijo iz poveznih zbirk osebnih podatkov, morajo biti tudi po pridobitvi ustrezno zavarovani – določiti je potrebno varno lokacijo shranjevanja.

Po preteku roka hrambe osebnih podatkov je potrebno glede na zahteve 21. člena ter 4. točke 1. odstavka 24. člena ZVOP-1 onemogočiti nadaljnjo obdelavo osebnih podatkov. Tu bi opozorili predvsem na varen oz. dejanski izbris podatkov z nosilcev podatkov kot so trdi diski (npr. z večkratnim prepisovanjem z naključnim nizom podatkov) oziroma na varno uničenje podatkov na trajno zapisnih prenosnih medijih. Slednji morajo biti fizično uničeni, pri oddaji v uničenje zunanjemu izvajalcu pa je nujno poskrbeti za komisijsko uničenje z ustreznim zapisnikom.

5. točka 1. odstavka 24. člena ZVOP-1 od upravljavcev zbirk osebnih podatkov zahteva t. i. **sledljivost obdelave osebnih podatkov**. Gre za izjemno pomemben vidik zavarovanja, ki je ključen pri odkrivanju nepooblaščenih vstopov v zbirke osebnih podatkov in posledično zlorabe tako pridobljenih osebnih podatkov (npr. javno razkritje, nenamenska uporaba). Izvajanje sledljivosti je namreč tisti ukrep, s katerim naj bi se dalo ugotoviti, kdo je zlorabil določene osebne podatke. Kot primer scenarija v praksi si lahko predstavljamo, da se javno objavijo podatki o zdravstvenem stanju neke medijsko izpostavljene osebnosti, npr., da je določena politična osebnost okužena s HIV. Ali bomo lahko ugotovili, kdo je odgovoren za nepooblaščeno razkritje takšnih podatkov? Potrebno se je zavedati, da stoodstotne varnosti ni in da je nemogoče stoodstotno preprečiti nepooblaščeno seznanitev in zlorabo osebnih podatkov, vendar pa je potrebno sprejeti vse razumne mere in ukrepe, ki lahko možnost zlorabe minimizirajo ali vsaj omogočijo naknadno ugotavljanje odgovornosti. Povezovanje zbirk osebnih podatkov, s katerimi upravlja javna uprava, pomen sledljivosti obdelave še dodatno izpostavi. Sledljivost je pomembna tudi s preventivnega vidika, zaradi česar je potrebno **zaposlene seznaniti z dejstvom, da se izvaja sledljivost obdelave osebnih podatkov**. V nekaterih primerih lahko že to dejstvo odvrne posameznika, da bi se odločil za neupravičen dostop do osebnih podatkov, saj se bo zavedal, da bodo njegova dejanja evidentirana in da bo v primeru zlorabe

na seznamu osumljenih.

Ne pozabimo, da je obdelava osebnih podatkov zelo širok pojem, ki vključuje praktično vsakršno ravnanje z osebnimi podatki, vključno z vpogledom in seznanitvijo. Pri tem pa se v praksi porajajo določena vprašanja, saj izvajanje sledljivosti, kljub sodobnim informacijskim tehnologijam, s katerimi se v sodobni družbi v čedalje večji meri obdeluje (osebne) podatke, ni enostavno in lahko za upravljavca predstavlja velike vložke v sredstva, ljudi in ostale vire, zato je toliko pomembneje, da se ta vidik obravnava že v prvih fazah projekta (Privacy by design).

Nadzor nadzornikov ter avtentičnost in celovitost revizijske sledi

Poleg beleženja dostopov do podatkov na nivoju storitve je potrebno poskrbeti tudi za beleženje dostopov do podatkov v sami bazi podatkov. 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 potrebno poskrbeti za primerne tehnične in organizacijske ukrepe, s katerimi se uvaja **nadzor oziroma omejevanje pooblastil tudi administratorjem z najvišjimi pooblastili**. Sistem mora delovati tako, da beleženja dostopov ni možno za določen čas izključiti, prav tako pa tudi najvišjim administratorjem ne sme biti dana možnost naknadnega popravljanja, spreminjanja ali brisanja dela ali celotne revizijske sledi.

Zavarovanje osebnih podatkov kot proces

Varovanja informacija ali osebnih podatkov ne smemo obravnavati kot enkratno aktivnost, temveč kot proces. Standard ISO 27001:2005 temelji na tako imenovanem PDCA krogu, ki je predstavljen na spodnji sliki:

Določitev ukrepov in postopkov za zavarovanje osebnih podatkov v internih aktih izrecno zahteva 25. člen ZVOP-1, vsekakor pa je za ustrezno raven zagotavljanja zavarovanja osebnih podatkov potrebno poskrbeti tudi za to, da se interni akt ažurira ob vseh pomembnejših spremembah v okolju upravljavca, da se izvajanje internega akta redno nadzoruje in ukrepa s predlogi izboljšav in odpravo ugotovljenih pomanjkljivosti. Kot smo že izpostavili, bi po mnenju Pooblaščenca moral organi javne uprave, ki povezujejo zbirke osebnih podatkov, vzpostaviti, izvajati ter vzdrževati sistem za upravljanje varovanja informacij (SUVI), kot to priporoča omenjeni ISO standard.

Upravljavci zbirk osebnih podatkov morajo v internih aktih po določbi 2. odstavka 25. člena ZVOP-1 **določiti osebe, ki so odgovorne za določene zbirke osebnih podatkov**, in osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke.

Napotki za izpolnitev vloge za izdajo predhodnega dovoljenja za povezavo zbirk osebnih podatkov

Kot že navedeno, morajo upravljavci za povezovanje zbirk pridobiti dovoljenje (odločbo) **Informacijskega pooblaščenca**, če:

- vsaj ena zbirka osebnih podatkov, ki naj bi se jo povezalo, vsebuje občutljive podatke, ali
- bi povezovanje imelo za posledico razkritje občutljivih podatkov, ali
- je za izvedbo povezovanja potrebna uporaba istega povezovalnega znaka.

Zaradi ekonomičnosti in hitrosti izvedbe postopka Pooblaščenec v nadaljevanju podaja nekaj napotkov za izpolnitev vloge za pridobitev navedenega dovoljenja:

- Obrazec vloge za izdajo dovoljenja za povezavo zbirk osebnih podatkov je dostopen na spletnih straneh Informacijskega Pooblaščenca[19].
- Pred vložitvijo zahtevka za dovoljenje, **preverite ali se s povezovanjem zbirk strinja tudi upravljavec druge zbirke** – torej zbirke, s katero želite povezati svojo zbirko. Najbolj smotrno je vlogo za **dovoljenje podati skupaj z upravljavcem druge zbirke**.
- V vlogi navedite **točen naziv zbirk osebnih podatkov**, ki naj bi se povezovale ter **naziv in sedež upravljavca posamezne zbirke**.
- V vlogi morate utemeljiti **namen** in **pravno podlago** za povezovanje zbirk.
- V vlogi **izrecno navedite, zaradi katerega od razlogov vlagate zahtevek** – torej ali zaradi vsebovanja oz. možnosti razkritja občutljivih podatkov ali zaradi uporabe istega povezovalnega znaka.
- Z vidika določb 24. člena ZVOP-1 obvezno **opišite način zavarovanja zbirk, ki naj bi se povezovale ter k vlogi priložite notranje akte, v katerih imate predpisane postopke in ukrepe za zavarovanje osebnih podatkov**, saj lahko Pooblaščenec izda odločbo le, če ugotovi, da je zagotovljeno ustrezno zavarovanje osebnih podatkov.
- Navedite in na kratko **opišite informacijsko komunikacijske tehnologije**, ki se uporabljajo za vodenje zbirk, ki naj bi se povezovale in bodo uporabljene za nameravano povezovanje zbirk osebnih podatkov ter **opišite s tem povezane komunikacijske protokole, aplikacije in servise**.

Predvsem pred odločitvijo za povezovanje zbirk preverite, ali obstaja pravna podlaga za takšno povezovanje. Pravno podlago mora namreč **izrecno določati zakon**. Pogosto namreč upravljavci interpretirajo veljavno zakonodajo tako, kot da jim omogoča povezovanje zbirk, vendar Pooblaščenec ugotovi, da dejansko ni tako. Zato je smotrno **pregledati seznam odločb**, ki jih je Pooblaščenec **že izdal** upravljavcem zbirk, iz katerega je razvidno, kdaj je bila v veljavni zakonodaji podana pravna podlaga za povezovanje zbirk in kdaj ne. Seznam odločb je dostopen na spletnih straneh Pooblaščenca[20].

Primeri zakonskih pravnih podlag za povezovanje zbirk:

Zakon	Člen
Zakon o sodnem registru	2.b člen (3) V sodni register se vpiše enotna identifikacijska številka osebe iz prvega odstavka tega člena, drugi identifikacijski podatki te osebe pa se avtomatično na podlagi povezanosti matične evidence s sodnim registrom prevzamejo iz matične evidence in so s tem vpisani v sodni register. (4) Če se v matični evidenci spremenijo identifikacijski podatki osebe iz prvega odstavka tega člena, se te spremembe avtomatično na podlagi povezanosti z matično evidenco prevzamejo tudi v sodni register.

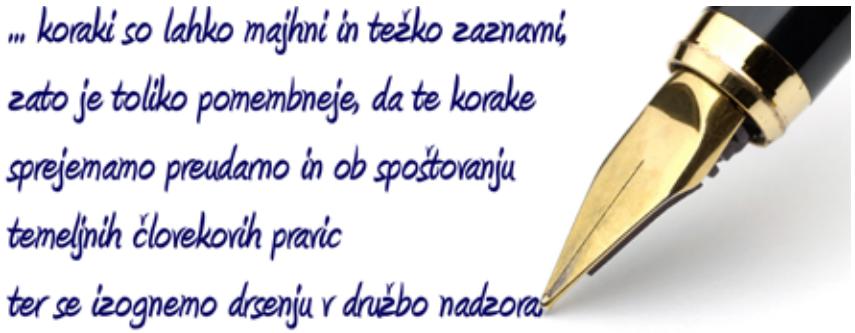
19 Dostopno na povezavi: http://www.ip-rs.si/fileadmin/user_upload/doc/obrazci/Zahtevek_za_odlocbo_povezljivost-1.doc

20 Dostopno na: http://www.ip-rs.si/varstvo-osebnih-podatkov/register-zbirk/povezava-zbirk-osebnih-podatkov/seznam-izdanih-odlocb-o-povezljivosti-zbirk-osebnih-podatkov/

Zakon	Člen
Zakon o finančnem poslovanju, postopkih zaradi insolventnosti in prisilnem prenehanju	113. člen (vodenje seznama upraviteljev) (2) V seznam upraviteljev se vpiše upraviteljeva identifikacijska številka, drugi identifikacijski podatki upravitelja pa se avtomatično na podlagi povezanosti centralnega registra prebivalstva, davčnega registra in poslovnega registra (v nadaljnjem besedilu: matične evidence) s seznamom upraviteljev prevzamejo iz teh evidenc in so s tem vpisani v seznam upraviteljev.
Zakon o kmetijstvu	140. člen (evidenca subjektov) (2) Prevzemanje podatkov iz prve, tretje in četrte alineje prejšnjega odstavka v evidenco subjektov poteka s samodejnim povezovanjem s centralnim registrom prebivalstva, evidenco gospodinjstev, poslovnim registrom Slovenije in registrom prostorskih enot. Prevzemanje osebnih podatkov poteka z uporabo EMŠO ali matične številka poslovnega subjekta ali davčne številke. 167. člen (povezovanje zbirk podatkov) (1) Za izvajanje nalog z delovnega področja ministrstva se evidence z delovnega področja ministrstva lahko povezujejo med seboj in z evidencami iz prvega in drugega odstavka prejšnjega člena. (3) Za povezovanje evidenc z delovnega področja ministrstva z evidencami iz prvega in drugega odstavka prejšnjega člena se za osebne podatke uporablja davčna številka ali EMŠO ali matična številka poslovnega subjekta.

Zaključek

Želimo si, da bi bile pričujoče smernice Informacijskega pooblaščenca upravljavcem zbirk osebnih podatkov v javnem sektorju v premislek in napotek o tem, ali je povezovanje zbirk res rešitev, in ko je, kako ga izvesti zakonito in sorazmerno s posegom v pravice posameznika. Znani izrek iz 18. stoletja, ki ga pripisujejo Benjaminu Franklinu, pravi, da si tisti, ki bi se odrekli temeljnim svoboščinam za nekaj začasne varnosti, ne zaslužijo ne svobode in ne varnosti[21]. Vsi podatki o nas na enem mestu se verjetno ne bodo znašli medsebojno povezani kar čez noč ...



21 V izvirniku: "*Those who would give up Essential Liberty to purchase a little Temporary Safety deserve neither Liberty nor Safety*"