



Zavarovanje osebnih podatkov

Smernice Informacijskega pooblaščenca

Namen dokumenta:	Namen smernic je tako večjim kot manjšim upravljavcem podrobneje obrazložiti zahteve ZVOP-1 glede zavarovanja osebnih podatkov (informacijske varnosti), podati usmeritve in opozoriti na primere kršitev iz inšpekcijske prakse Informacijskega pooblaščenca.
Ciljne javnosti:	Upravljalci zbirk osebnih podatkov v javnem in zasebnem sektorju ter njihovi pogodbeni obdelovalci.
Status:	Javno
Verzija:	1.0
Datum verzije:	22.9.2015
Avtorji:	Informacijski pooblaščenec
Ključne besede:	Smernice, zavarovanje osebnih podatkov, ISO/IEC 27001, ISO/IEC 27002, informacijska varnost, občutljivi osebni podatki, upravljanje tveganj.

Kazalo

O SMERNICAH INFORMACIJSKEGA POOBLAŠČENCA	4
1. UVOD	5
2. ZAKONSKE ZAHTEVE GLEDE ZAVAROVANJA OSEBNIH PODATKOV	6
2.1 DOBRE PRAKSE	9
3. SMERNICE ZA MANJŠE UPRAVLJAVCE	11
3.1 PODROBNEJŠA OBRAZLOŽITEV ZAKONSKIH ZAHTEV GLEDE ZAVAROVANJA OSEBNIH PODATKOV	12
3.2 HITRI VODIČ	15
3.3 KAKO DOBRO PRI NAS SKRBJIMO ZA VARNOST OSEBNIH PODATKOV?	17
4. SMERNICE ZA VEČJE UPRAVLJAVCE	18
4.1 CELOVIT PRISTOP K ZAVAROVANJU OSEBNIH PODATKOV	19
4.2. PODROBNEJŠA OBRAZLOŽITEV ZAKONSKIH ZAHTEV GLEDE ZAVAROVANJA OSEBNIH PODATKOV	21
4.2.1. Dostopne pravice	21
4.2.2. Beleženje dostopov do podatkov (sledljivost)	21
4.2.3. Rok hrambe sledljivosti	23
4.2.4. Zavarovanje občutljivih osebnih podatkov	24
4.2.5. Nadzor nadzornikov (Quis custodiet ipsos custodes?)	25
4.2.6. Zahteve glede varnosti osebnih podatkov pri pogodbeni obdelavi	26
4.3. PRIMERI IZ INŠPEKCIJSKE PRAKSE	27
4.4. NAJPOGOSTEJŠE KRŠITVE	31
5. ZAKLJUČEK	32

O smernicah Informacijskega pooblaščenja

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

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

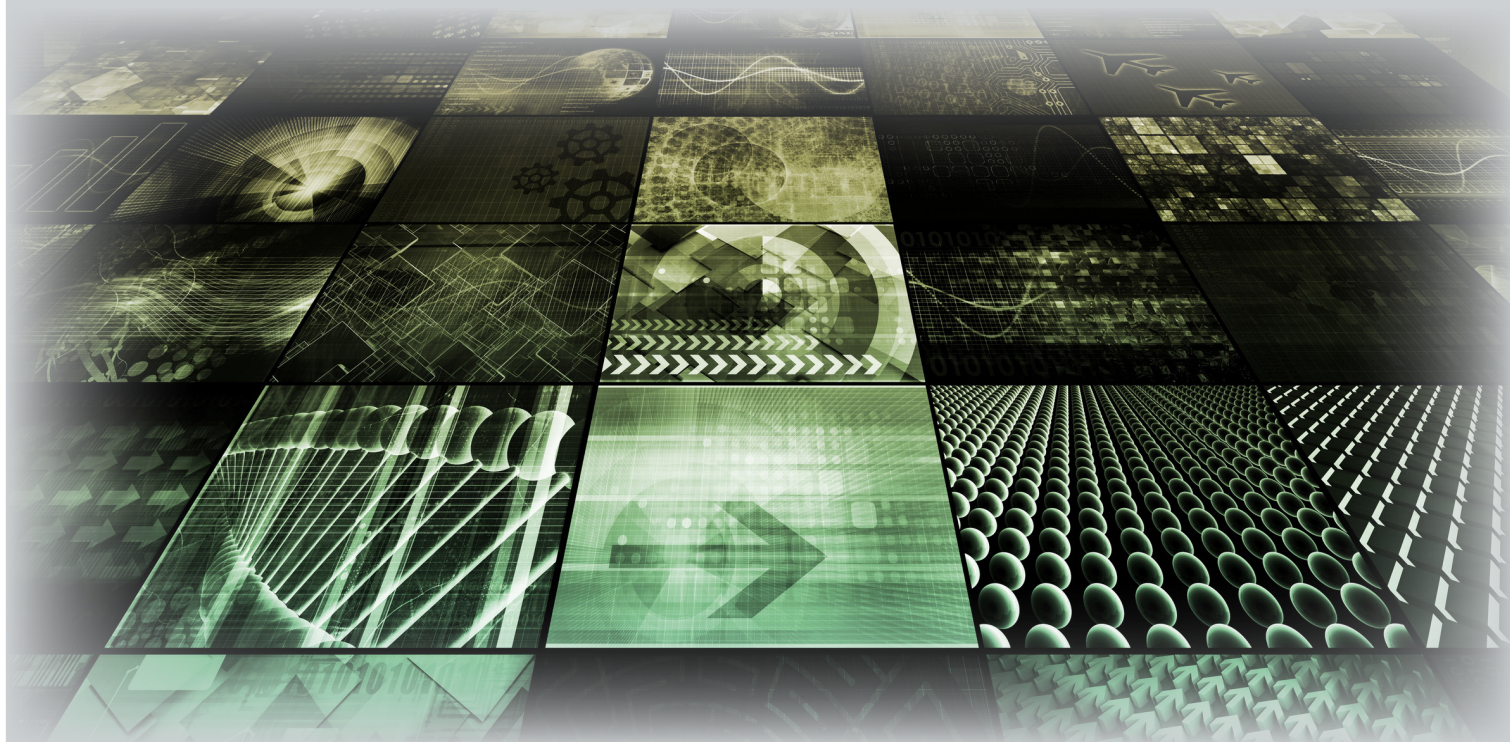
Oglejte si tudi:

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

Brošure IP: <http://www.ip-rs.si/publikacije/prirocniki/>

Smernice IP so objavljene na spletni strani:

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



Uvod

»Spoštovani, žal je zaradi varnostnega incidenta prišlo do javne objave osebnih podatkov naših strank. Svetujemo vam, da si čim prej zamenjate gesla, ki jih uporabljate za dostop do naših storitev«.

Tovrstnega obvestila si najbrž ne želi poslati oziroma podpisati noben predstojnik organizacije, a spremembe zakonodajnega okvira za varstvo osebnih podatkov v EU prinašajo tudi tovrstne ukrepe, s katerimi naj bi zagotovili večjo odgovornost za ustrezno ravnanje s podatki. Neustrezna skrb za varnost podatkov ima lahko kritične posledice za vsako podjetje in organizacijo. Ustrezno zavarovanje pa tudi širša varnost osebnih podatkov je temeljni sestavni del varstva osebnih podatkov in organizacije bodo čedalje bolj morale proaktivno izkazovati, da za varnost podatkov učinkovito skrbijo.

Varnost osebnih podatkov temelji na istih elementih kot informacijska varnost – gre za zagotavljanje zaupnosti, celovitosti in razpoložljivosti (osebnih) podatkov. Če hočemo vse to zagotoviti, moramo najprej vedeti, kje imamo podatke, ugotoviti, kaj se jim lahko pripeti, razmisliti o primernih ukrepih in vse skupaj redno preverjati in prilagajati. Varnost osebnih podatkov žal mnogi enačijo z varnostjo informacijskih tehnologij (IT), postopki za varnost podatkov pa naj bi bili v domeni informatikov, češ bodo že uredili tiste požarne zidove in protivirusne programe. A informacijska varnost je več kot, saj nas noben protivirusni program ne more ustaviti v tem, da uporabljamo isto geslo povsod, da malce pobrskamo po bazah podatkov iz zvedavosti in da nasedemo napadalcu, ki s tehnikami socialnega inženiringa od nas izvabi zaupne podatke. Človeški faktor je še vedno najšibkejši člen in zanašanje zgolj na tehnične ukrepe je recept za neuspeh. Prav tako informacijska varnost ni nekaj, kar storiš in je narejeno – preverjanje učinkovitosti varnostnih ukrepov in posodabljanje znanj naših zaposlenih mora biti stalna skrb.

V smernicah, ki jih imate pred sabo, boste – tako vsaj upamo – nekaj novega in koristnega našli tako manjši kot večji upravljavci osebnih podatkov. Manjši upravljavci si lahko pomagata z osnovnim kontrolnim seznamom, opisom dobrih in slabih praks ter najpogostejših kršitev, večjim pa podrobneje predstavimo določene specifične zahteve ZVOP-1, da jih lahko učinkovito in celovito naslovijo z obstoječo organizacijsko strukturo in ukrepi za zagotavljanje informacijske varnosti.

Zakonske zahteve glede zavarovanja osebnih podatkov

Informacijska varnost oz. **zavarovanje osebnih podatkov** je bistveni del in eno temeljnih načel vseh pravnih aktov, ki urejajo področje **varstva osebnih podatkov**¹ in kot ožji del varstva osebnih podatkov pomeni varovanje **celovitosti, zaupnosti in razpoložljivosti** osebnih podatkov. Varstvo osebnih podatkov kot širši pojem vključuje ostala temeljna načela, kot so zakonitost, sorazmernost in namenskost, zavarovanje osebnih podatkov pa se predvsem nanaša na to, kako osebne podatke varujemo pred izgubo, nepooblaščenno obdelavo in drugimi zlorabami².

ZVOP-1 se vprašanja zavarovanja osebnih podatkov dotika v 14., 24. in 25. členu ter posredno v 11. členu.

Pri tem se trudi biti **tehnološko nevtralen**. ZVOP-1 zatorej ne določa konkretnih ukrepov, ki morajo biti izvedeni za zavarovanje določenih obdelav osebnih podatkov, ampak opisuje predvsem cilje, ki jih je pri tem potrebno zasledovati. **Prav tako ne predvideva istovrstnih ukrepov za vse obdelave osebnih podatkov**, ampak določa, da morajo biti ukrepi primerni glede na tveganja, ki jih predstavlja narava konkretno obdelovanih podatkov.



¹ Gre za razliko, ki je terminološko morda bolj očitna v angleškem jeziku: zavarovanje osebnih podatkov (angl. data security) in varstvo osebnih podatkov (angl. data protection).

² Ustrezni postopki in ukrepi za zavarovanje podatkov nam seveda še ne zagotavljajo, da ne bo prišlo do kršitev ZVOP-1.

Kaj določa ZVOP-1?

14. člen ZVOP-1 ureja zavarovanje občutljivih³ osebnih podatkov in določa:

(1) Občutljivi osebni podatki morajo biti pri obdelavi posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop do njih, razen v primeru iz 5. točke 13. člena tega zakona.

(2) Pri prenosu občutljivih osebnih podatkov preko telekomunikacijskih omrežij se šteje, da so podatki ustrezno zavarovani, če se posredujejo z uporabo kriptografskih metod in elektronskega podpisa tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom.

24. člen ZVOP1 opredeljuje zavarovanje osebnih podatkov in splošne zahteve in sicer določa:

(1) Zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščen uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščen 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.

(2) V primeru obdelave osebnih podatkov, ki so dostopni preko telekomunikacijskega sredstva ali omrežja, morajo strojna, sistemska in aplikativno programska oprema zagotavljati, da je obdelava osebnih podatkov v zbirkah osebnih podatkov v mejah pooblastil uporabnika osebnih podatkov.

(3) Postopki in ukrepi za zavarovanje osebnih podatkov morajo biti ustrezni glede na tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo.

(4) Funkcionarji, zaposleni in drugi posamezniki, ki opravljajo dela ali naloge pri osebah, ki obdelujejo osebne podatke, so dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju njihovih funkcij, del in nalog. Dolžnost varovanja tajnosti osebnih podatkov jih obvezuje tudi po prenehanju funkcije, zaposlitve, opravljanja del ali nalog ali opravljanja storitev pogodbene obdelave.

25. člen ZVOP-1 opredeljuje posebne dolžnosti glede zavarovanja osebnih podatkov in določa:



(1) Upravljalci osebnih podatkov in pogodbeni obdelovalci so dolžni zagotoviti zavarovanje osebnih podatkov na način iz 24. člena tega zakona.

(2) Upravljalci osebnih podatkov v svojih aktih predpišejo postopke in ukrepe za zavarovanje osebnih podatkov ter določijo osebe, ki so odgovorne za določene zbirke osebnih podatkov, in osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke.

³ Po določbi 6. člena ZVOP-1 so občutljivi osebni podatki podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju, spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali prekrškovne evidence; občutljivi osebni podatki so tudi biometrične značilnosti, če je z njihovo uporabo mogoče določiti posameznika v zvezi s kakšno od prej navedenih okoliščin.

Podatki morajo biti ustrezno zavarovani s tehničnimi in organizacijskimi ukrepi, s katerimi se zagotavlja zaupnost, celovitost in razpoložljivost podatkov. Preprečena mora biti nepooblaščen seznanev, brisanje, spreminjanje, posredovanje, objavljanje ali uničevanje podatkov, pristop k varovanju informacij pa mora biti celovit in proaktiven – upravljavci bi morali izkazati zavezanost k proaktivnemu in odgovornemu ravnanju z osebniimi podatki (angl. accountability).

ZVOP-1 v grobem sledi mednarodno uveljavljenim standardom s področja informacijske varnosti in v prvem odstavku 25. člena povzema (nekatera) temeljna področja informacijske varnosti, kot so npr. fizična varnost, varnost omrežij, zagotavljanje zaupnosti podatkov med prenosom in beleženje uporabe podatkov. Prav tako jim sledi v delu, ki se nanaša na ustreznost ukrepov - ukrepi za zavarovanje morajo biti **ustrezni glede na naravo in tveganje**, ki jih prinaša obdelava osebnih podatkov.

**Kako zavarovati podatke videonadzornega sistema?**

1. Določite osebe, ki lahko pridejo do posnetkov.
2. Vsaka od teh oseb mora imeti svoje geslo in se držati politike gesel.
3. Vsak dostop do posnetkov mora biti zabeležen (kdo, kdaj zakaj, kaj).

Ključni poudarki so naslednji:

1. TEHNIČNI IN ORGANIZACIJSKI UKREPI. 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. **Informacijska varnost ni samo varnost informacijskih tehnologij (varnost IT) in ni samo stvar informatikov in IT-ja.**

2. UKREPI PRILAGOJENI TVEGANJEM. Ukrepi za zavarovanje morajo biti **ustrezni glede na naravo in tveganje**, ki jih prinaša obdelava osebnih podatkov. V tem oziru je izjemnega pomena **analiza tveganja**, katere rezultat je glavni vhodni podatek za sprejem ukrepov, s katerimi bomo upravljali s tveganji.

3. STALNA SKRIB ZA VARNOST. Informacijska varnost je **proces**, ki vključuje analizo tveganj, obravnavo tveganj, sprejem ukrepov za upravljanje tveganj, nadzor učinkovitosti sprejetih ukrepov in prilagajanje ukrepov.

Dobre prakse

Zakonodaja izrecno ne določa (konkretizira) postopkov in ukrepov, ki pa so lahko izrednega pomena za zagotavljanje informacijske varnosti, zato jih želimo na tem mestu predstaviti.

Odgovorne osebe za varstvo osebnih podatkov.

Odgovorne osebe za varstvo osebnih podatkov (angl. Data Protection Officer) so uveljavljen ukrep, s katerim želimo skrb za varnost in varstvo osebnih podatkov skoncentrirati v posamezni osebi ali službi. Pri večjih upravljavcih, kot so banke in zavarovalnice, podobne institute že poznajo na drugih področjih in sicer gre za osebe, ki skrbijo za (celovito) skladnost poslovanja (angl. compliance). Na področju varstva osebnih podatkov lahko njihove naloge vključujejo tudi naloge s področja varnosti osebnih podatkov, kot so:

- izvajanje internih izobraževanje za zaposlene,
- sodelovanje pri preiskovanju varnostnih incidentov,
- sodelovanje pri uvajanju ali spreminjanju informacijskih rešitev, ki vključujejo obdelave osebnih podatkov,
- sodelovanje v postopkih nadzora ustreznosti in učinkovitosti varnostnih postopkov in ukrepov,
- sodelovanje pri pripravi internih aktov, pravilnikov in varnostnih politik,
- drugo preventivno delovanje.



Presoje vplivov na zasebnost.

Pri uvajanju novih informacijskih sistemov, aplikacij in rešitev je pravočasno obravnavanje vidikov varnosti v smislu presoje vplivov na zasebnost ključnega pomena za ustrezno raven varnosti. Z zmanjšanjem obsega podatkov lahko bistveno zmanjšamo varnostna tveganja, zmanjšamo obremenitve informacijskega sistema glede zahteve po beleženju dostopov in pravočasno ugotovimo, katere tveganja so nesprejemljiva in terjajo odziv.

Stalno izobraževanje zaposlenih. Informacijska varnost se s hitrim napredkom informacijskih tehnologij hitro spreminja – zaposleni se pri svojem delu srečujejo z novimi napravami, aplikacijami in zmogljivostmi obdelave osebnih podatkov. Samo s tehničnimi ukrepi je nemogoče preprečiti nepooblaščen obdelave osebnih podatkov, zato je zelo pomembno – kakor tudi kaže inšpekcijska praksa Informacijskega pooblaščenca – da tehnične ukrepe kombiniramo z organizacijskimi, med katere ne prvo mesto sodi ustrezna ozaveščenost zaposlenih. Že samo poznavanje problematike (kaj sploh so osebni podatki in katera so (ne)dopustna ravnanja z njimi) je včasih na nizkem nivoju. Med obvezne teme rednih izobraževanje pa vsekakor sodijo še napotki glede varne izbire gesel, pomena politik čiste mize in čistega zaslona in prepoznavanje socialnega inženiringa. Včasih je namreč za varnost možno storiti ogromno že z zelo majhnimi ukrepi.

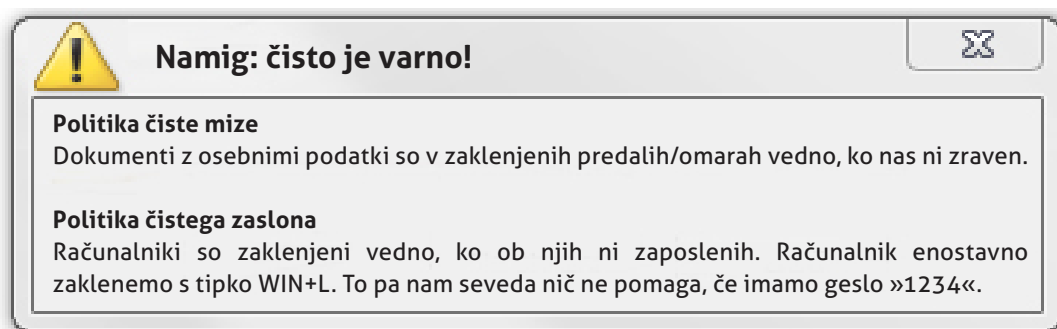


Promoviranje pomena informacijske varnosti znotraj organizacije. Prednosti informacijske varnosti niso vedno neposredno vidne, medtem ko njeni stroški so. Prav tako izvajanje ukrepov in politik informacijske varnosti pogosto naleti na negodovanje in odpor s strani zaposlenih, ki morda niso seznanjeni z razlogi za njimi oz. posledicami, ki utegnejo nastopiti zavoljo njihove opustitve. Posledično se ukrepi dostikrat površno izvajajo, ali pa se sploh ne. Da bi se organizacija zoperstavila temu trendu, morajo imeti odgovorne osebe jasno podporo vodstva, zadostno financiranje, ter skrbeti za stalno izobraževanje, kot že zgoraj. Skrb za varovanje osebnih podatkov ter informacijsko varnost morata postati integralni del vseh poslovnih procesov.

Smernice za manjše upravljavce

ZVOP-1 določa, da morajo biti ukrepi za zavarovanje **ustrezni glede na naravo in tveganje**, ki jih prinaša obdelava osebnih podatkov. Če torej hranite in uporabljate:

- manjše število osebnih podatkov (npr. samo o vaših kupcih, strankah in zaposlenih),
- ne obdelujete občutljivih osebnih podatkov (kot so npr. zdravstveni podatki),
- obdelujete osebne podatke, katerih zloraba ne bi imela hujših posledic za posameznika,



...potem tudi vaši ukrepi za varnost podatkov niso nujno takšni, kot jih pričakujemo od tistih, ki:

- obdelujejo veliko število osebnih podatkov (npr. banke, zavarovalnice, državni registri, operaterji telekomunikacij),
- obdelujejo občutljive osebne podatke (npr. izvajalci zdravstvenih storitev, upravljavci kazenskih in prekrškovnih evidenc, centri za socialno delo ipd.),
- obdelujejo osebne podatke, katerih zlorabe imajo lahko hujše posledice za posameznika.

Še vedno pa morate poskrbeti za to, da bodo podatki **varni**, kar pomeni:

- da ne smejo biti na voljo nepooblaščenim osebam (**zaupnost**),
- da se jih ne sme izgubiti, javno objaviti ali nepooblaščno spreminjati (**celovitost**),
- da morajo biti na voljo takrat, ko so res potrebni (**razpoložljivost**).

Podrobnejša obrazložitev zakonskih zahtev glede zavarovanja osebnih podatkov

Kaj torej od nas zahteva ZVOP-1?

1. Da v vsakem trenutku vemo, katere osebne podatke sploh imamo, kje in kdo ima do njih dostop.

2. Da zagotavljamo varnost osebnih podatkov, t.j. da preprečujemo slučajno ali namerno:

- nepooblaščno uničevanje podatkov,
- nepooblaščno spremembo,
- seznanitev nepooblaščenih oseb s podatki,
- izgubo podatkov.



3. Da varnost podatkov zagotavljamo s kombinacijo:

- **tehničnih ukrepov, kot so:**
 - zaklepanje prostorov, omar, predalov,
 - učinkovito uničevanje podatkov na papirnih in elektronskih nosilcih,
 - uporaba protivirusnih programov, požarnega zidu, redno nameščanje varnostnih popravkov strojne in programske opreme ter
- **organizacijskih ukrepov, kot so:**
 - pravilno izbrana gesla,
 - redno izobraževanje zaposlenih,
 - interni akti, ki določajo, kaj se sme delati z osebnimi podatki, kdo je odgovoren za posamezne zbirke osebnih podatkov ter katere osebe lahko zaradi narave svojega dela obdelujejo določene osebne podatke.



Namig: kdaj zaupati zunanjim izvajalcem?



1. Z vsakim moramo imeti sklenjeno pisno pogodbo.
2. Jasno navedimo, kaj smejo početi s podatki in česa ne (podatkov npr. ne smejo uporabljati za lastne namene).
3. Konkretno naj bo določeno kako bodo varovali naše podatke (samo »skladno z ZVOP« ni dovolj)!
4. Lahko smo tudi mi odgovorni, če bodo podatke slabo varovali!

4. Da razumemo, da:

- **varnost** podatkov še ne pomeni **varstva** osebnih podatkov. Podatki so lahko odlično zaklenjeni, a kaj ko nimamo pravne podlage, da jih sploh smemo imeti ali pa jih uporabljamo za namene, za katere niso bili zbrani.
- varnost podatkov ni samo IT varnost in da to ni nekaj, kar uredijo informatiki,
- je skrb za varnost podatkov **proces** in ne nekaj, kar narediš in je končano (npr. zgolj sprejem pravilnika),
- je **človeški faktor** pogosto največje tveganje za zlorabe.

ZASEBNOST

VARSTVO OSEBNIH PODATKOV

VARNOST OSEBNIH PODATKOV

VARNOST IT

VARSTVO OSEBNIH PODATKOV

ZAKONITOST

NAMENSKOST

SORAZMERNOST

INFORMIRANOST
POSAMEZNIKA

PRAVICE
POSAMEZNIKA

TOČNOST IN
AŽURNOST



Namig: sledljivost!

Ste vedeli, da lahko osnovno sledljivost zagotovite tudi v programih kot so Word, Excel, Writer in Calc?
Omogočite sledenje sprememb (track changes) in zabeleženo bo kdo, kaj in kdaj je spreminjal!

Zakaj poskrbeti za varnost podatkov?

1. Ker lahko izguba osebnih podatkov, njihova javna objava ali druga zloraba pomembno **okrni ugled vašega podjetja, zaupanje strank** in celo **obstoje** vašega podjetja.
2. Ker ustrezno varovanje podatkov lahko izboljša **zaupanje vaših strank, poslovnih partnerjev** in **ugled vašega podjetja**.
3. Ker gre lahko tudi za **vaše lastne osebne podatke**.
4. **In nenazadnje zato**, ker tako nalaga **zakon** in ste lahko zaradi slabega zavarovanja podatkov **odgovorni za kršitev** ter vam je lahko izrečena **globa**:
 - pravni osebi v višini **od 4.170 do 12.510 eurov**,
 - odgovorni osebi pravne osebe v višini **od 830 do 1.250 eurov**.



Hitri vodič

Smo manjše podjetje in zbiramo tudi osebne podatke. Kaj moramo storiti?

IDENTIFICIRAJ ZBIRKE OSEBNIH PODATKOV

1

Osebni podatki se lahko nahajajo:

- v kadrovskih mapah zaposlenih,
- v excelovih tabelah imamo kontaktne podatke strank,
- na spletni strani imamo podatke o nakupih,
- v posnetkih videonadzornega sistema,
- v računovodskih podatkih...

Manj osebnih podatkov – manj odgovornosti!
Premislite, katerih osebnih podatkov ne potrebujete in jih ne zbirajte na zalogo!

DOLOČI UKREPE

3

Uvedemo lahko različne ukrepe za zmanjšanje tveganj:

- sprejmemo interni pravilnik, kjer določimo postopke za varnost,
- določimo politiko gesel,
- poskrbimo za fizično varnost in varnost pred okoljskimi težavami (npr. vlom, požar, poplava),
- redno izobražujemo zaposlene o varnosti,
- pri pogodbenih izvajalcih vztrajamo na pisnih pogodbah in dogovorih o tem, kako konkretno bodo varovali naše podatke...

PRILAGODI UKREPE

5

Če pride do sprememb, ki lahko bistveno vplivajo na osebne podatke in njihovo varnost, npr. da:

- začnemo zbirati nove osebne podatke (npr. nova nagradna igra, trženja akcija, nova storitev, nova aplikacija...),
- se preselimo, razširimo dejavnost, zaposlimo nove sodelavce, spremenimo organizacijsko strukturo,
- najamemo nove zunanje izvajalce (npr. vzdrževalce spletnih strani, računovodski servis, klicni center...),
- ugotovimo, da obstoječi ukrepi za varnost podatkov ne zadostujejo, ker:
- je bila dokumentacija in oprema uničena v požaru,
- smo izgubili osebne podatke zaradi okvare diska,
- smo odkrili slabe prakse glede varnosti (npr. listke z gesli),

...potem moramo uvesti nove ukrepe ali prilagoditi obstoječe.

ANALIZIRAJ TVEGANJA

2

Kaj se lahko osebnim podatkom zgodi, katere grožnje oz. tveganja jim pretijo, npr.:

- vdor v spletno stran,
- e-naslova stranke ne izbrišemo in ponovno dobi naš oglas,
- izguba podatkov zaradi okvare diska, požara, nezaklepanja prostorov, slabo izbranih gesel,
- naši zaposleni ne poznajo zakonodaje in iz radovednosti brskajo po podatkih naših strank,
- podatke v obdelavo zaupamo drugemu podjetju, to pa ne poskrbi za njihovo varnost,
- osebni podatki ostanejo na računalnikih, ki jih zavržemo.

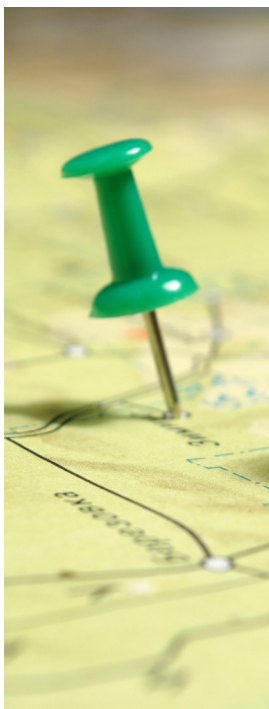
Ugotoviti moramo, kako verjetno je, da se določene grožnje uresničijo in kakšne bodo v tem primeru posledice za nas. Tveganj, ki jih ne moremo sprejeti, moramo obravnavati.

PREVERI USPEŠNOST UKREPOV

4

Vsaj enkrat na leto je priporočljivo, da ponovimo korake 1 do 3 in ugotovimo:

- ali smo na kakšno tveganje pozabili oziroma se je pojavilo novo tveganje,
- ali so obstoječi postopki in ukrepi (še) primerni ali ne.



DOBRE PRAKSE

- Naše varnostne ukrepe preverimo na polletni ravni.
- Zaposlene smo izobrazili o nevarnosti [socialnega inženiringa](#).
- Beležimo vnose, spremembe in izbrise osebnih podatkov.
- Naši zaposleni so prebrali [ABC spletne varnosti](#).
- Pravilnik o varnosti odraža dejansko stanje.
- Prednastavljena gesla smo zamenjali (npr. na wifi usmerjevalniku).
- Vsak dostop do videoposnetkov zabeležimo.
- Ko zaposleni odide od računalnika, ga zaklene, če tega ne stori, pa se računalnik po določenem času zaklene sam.
- Posodabljammo operacijske sisteme, protivirusne programe, brskalnike in dodatke v brskalnikih.
- Redno izdelujemo varnostne kopije podatkov.

SLABE PRAKSE

- Računalniki niso zaklenjeni z gesli.
- Uporabili smo vzorec pravilnika o zavarovanju OP brez prilagoditve dejanskemu stanju.
- Nikoli nismo opravili pregleda, kje vse se hranijo OP.
- Nimamo pisnih pogodb s pogodbenimi obdelovalci OP.
- Zbirka posnetkov videonadzornega sistema ni zavarovana.
- Ne posodabljammo protivirusne opreme.
- Sistem za upravljanje vsebin na spletni strani ni posodobljen na zadnjo varno verzijo.
- Zaposleni poznajo gesla drugih.
- Uporabniki imajo administratorske pravice.
- Pri odpisu stare opreme ne izbrišemo dokončno podatkov.



Kako dobro pri nas poskrbimo za varnost osebnih podatkov?

V nadaljevanju podajmo praktičen kontrolni seznam, s katerim lahko hitro in učinkovito preverite, ali imate vpeljene vsaj **osnovne varnostne kontrole**.

1. Poznavanje okolja, v katerem imamo osebne podatke

- Vemo, kje (vse) se pri nas nahajajo osebni podatki in kdo ima do njih dostop.
- Sprejeli smo politiko varovanja informacij (interni akt).

☐
☐

2. Dostop do sistema

- Določeno imamo politiko gesel.
- Posojanje gesel in uporaba skupinskih gesel je prepovedana.
- Vsak zaposlen ima svoje geslo za posamezne sisteme, aplikacije.
- Zaposlene smo podučili, kako si izbrati varna gesla.
- Vsa gesla se redno menjujejo, najmanj na tri mesece.
- Gesla niso krajša od 6 znakov.
- Določeno je, kdo je odgovoren za posamezno zbirko osebnih podatkov.
- Določeni so uporabniki, ki imajo pravico dostopa do posamezne zbirke osebnih podatkov.
- Zagotavljamo osnovno sledljivost obdelave osebnih podatkov (vnosi, brisanje, spremembe podatkov).

GLEJ [NAMIG](#) (str. 14)

☐
☐
☐
☐
☐
☐
☐
☐
☐
☐

3. Fizično in tehnično varovanje prostorov ter varovanje pred vplivi okolja

- Dostop do poslovnih prostorov je nadzorovan.
- Nepooblaščen osebe ne morejo nenadzorovano priti do osebnih podatkov.
- Računalniki so zaklenjeni, ko ob njih niso prisotni zaposleni.
- Omare in predali se zaklepajo, ko zaposleni niso prisotni.
- Uporabljamo zaščito pred vplivi okolja (npr. protipožarni sistemi, javljalniki dima, povečane temperature, vdora vode).

☐
☐
☐
☐
☐

4. Varovanje podatkov

- Uporabljamo posodobljen protivirusni program.
- Operacijski sistemi so posodobljeni.
- Podatke redno varnostno kopiramo.
- Preverili smo, ali iz varnostnih kopij lahko obnovimo izgubljene podatke.
- Nosilce podatkov pred odpisom popolno izbrišemo. GLEJ [NAMIG](#) (str. 12)
- Po e-pošti ne pošiljamo zdravstvenih in drugih občutljivih osebnih podatkov.

☐
☐
☐
☐
☐
☐

5. Človeški viri

- Zaposleni poznajo določbe pravilnika o varnosti podatkov.
- Zaposleni znajo prepoznati socialni inženiring. [NAMIG – GLEJ SMERNICE](#)
- Zaposleni se držijo politike gesel.
- Zaposleni se držijo politike čistega zaslona in čiste mize. GLEJ [NAMIG](#) (str. 11)
- Z vsemi pogodbenimi obdelovalci imamo sklenjene pisne pogodbe.
- Pisne pogodbe vsebujejo konkretne ukrepe, kako bodo varovali naše podatke GLEJ [NAMIG](#) (str. 13)

☐
☐
☐
☐
☐
☐

6. Stalno skrbimo za informacijsko varnost

- Enkrat letno preverjamo naše varnostne ukrepe.
- Ob pomanjkljivostih uvajamo nove ukrepe oz. prilagajamo obstoječe ukrepe.

☐
☐

Smernice za večje upravljavce

Večji upravljavci osebnih podatkov običajno razpolagajo z širšim naborom kadrovskih, finančnih in informacijskih resursov in tudi zahteve po informacijski varnosti ne izvirajo zgolj iz zakonodaje o varstvu osebnih podatkov, temveč tudi iz zakonodaje, ki ureja finančne vidike, ravnanje z dokumentarnim in arhivskim gradivom⁴, ravnanjem s tajnimi podatki⁵ in poslovnimi skrivnostmi... Teh zahtev je lahko veliko in so medsebojno lahko bolj ali manj usklajene, zato terjajo **celovite in integralne pristope k informacijski varnosti**. Okviri za takšen pristope so bili že razviti s strani kompetentnih organizacij in nobenega smisla nima te okvire kopirati, podvajati ali po nepotrebnem komplicirati. Namen smernic Informacijskega pooblaščenca zato **ni podajati novih zahtev ali kontrol**, temveč predvsem pojasniti, katere **specifične zahteve** pred večje upravljavce postavlja zakonodaja o varstvu osebnih podatkov in kako se določene zahteve ZVOP-1 tolmačijo v praksi. Na upravljavcih je, da se sami odločijo, katere že razvite okvire za informacijsko varnost uporabiti in kako jih najustrezneje uskladiti ter izvajati v skladu s svojo organizacijsko strukturo.



⁴ Zahteve Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA), Uredbe o varstvu dokumentarnega in arhivskega gradiva ter arhivih ter Enotnih tehnoloških zahtev (ETZ).

⁵ Zakon o tajnih podatkih (ZTP), Uredba o tajnih podatkih (UTP).

Celovit pristop k zavarovanju osebnih podatkov

Zahteve poslovnega in zakonodajnega okolja za večje upravljavce terjajo **celovite in integralne pristope** z zagotavljanju informacijske varnosti.

Informacijski pooblaščenec zato priporoča, da upravljavci pri zagotavljanju informacijske varnosti sledijo mednarodno uveljavljenim standardom, dobrim praksam in priporočilom glede informacijske varnosti, kot so zlasti:

- Standardi družine **ISO /IEC 27001:2013**⁶,
- Standard informacijske varnosti na področju poslovanja s plačilnimi karticami (Payment Card Industry Data Security Standard - **PCI DSS**⁷),
- Standardi ameriškega zveznega urada za standarde in tehnologijo - **NIST**⁸,
- Poslovni okvir za upravljanje IT (Control Objectives for Information and Related Technology - **COBIT**⁹),
- Priporočila Evropske agencije za varnost omrežij in informacij (European Union Agency for Network and Information Security - **ENISA**¹⁰),
- Poročila projekta Open Web Application Security Project (**OWASP**¹¹),
- Priporočila Ministrstva za javno upravo - Informacijska varnostna politika javne uprave (**IVPJU**¹²),
- opozorila in poročila **SI-CERT**¹³ – nacionalnega odzivnega centra za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij.



Glede na to, da morajo biti postopki in ukrepi za zavarovanje osebnih podatkov ustrezni glede na tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo, se v inšpekcijskem postopku »ustreznost« postopkov ugotavlja zlasti s primerjavo zahtev navedenih varnostnih standardov, smernic, priporočil in dobrih praks.

⁶ <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>

⁷ https://www.pcisecuritystandards.org/security_standards/

⁸ <http://www.nist.gov/information-technology-portal.cfm>

⁹ <https://cobitonline.isaca.org/>

¹⁰ https://www.enisa.europa.eu/publications#c2=publicationDate&reversed=on&c5=all&c0=10&b_start=0

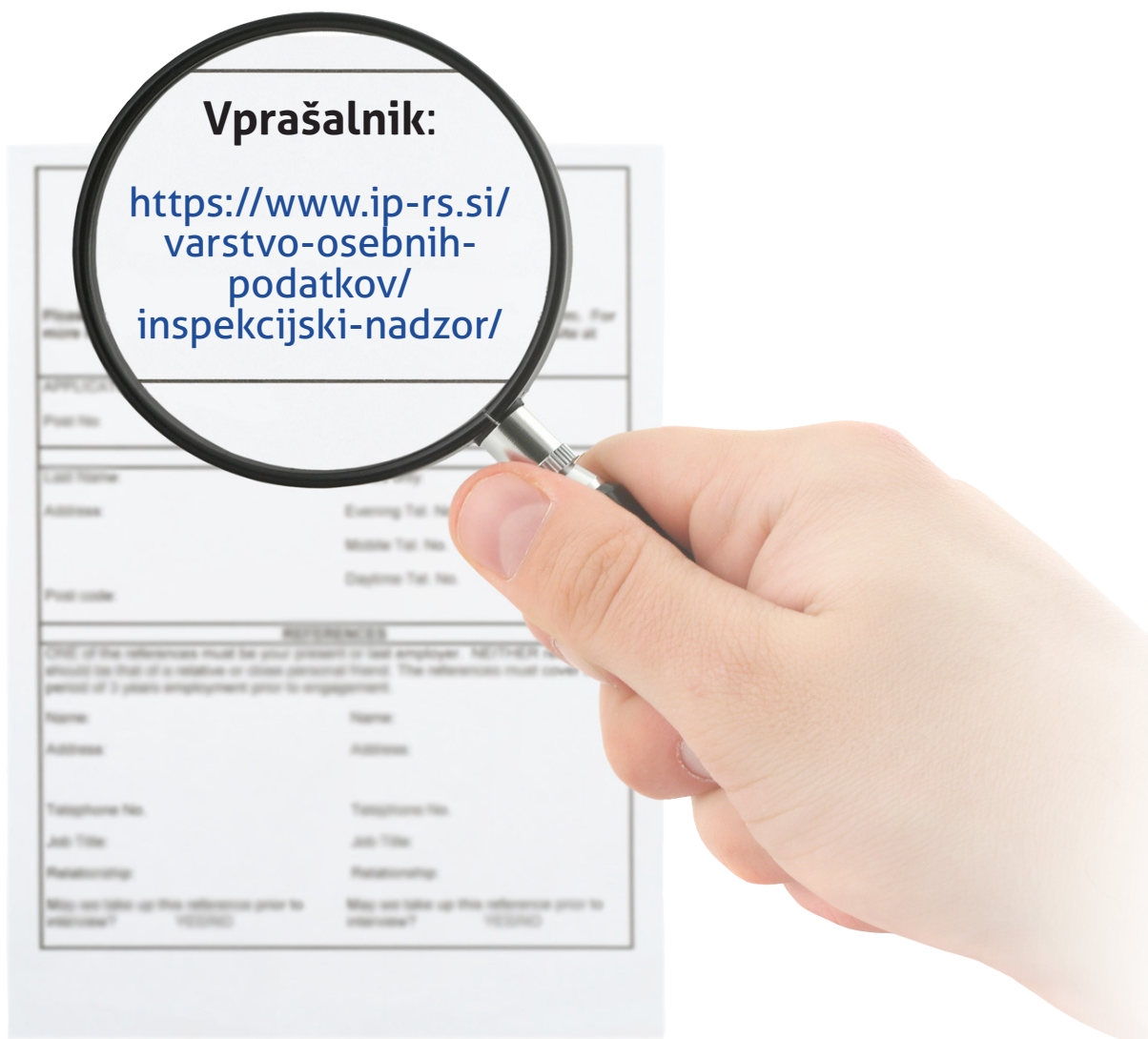
¹¹ https://www.owasp.org/index.php/Main_Page

¹² <http://nio.gov.si/nio/asset/informacijska+varnostna+politika>

¹³ <https://www.cert.si/>

Informacijski pooblaščenec zaradi njegove celovitosti in prilagodljivosti posebej priporoča mednarodni standard varovanja informacij **ISO/IEC 27001**, ki temelji na vzpostavitvi in upravljanju **sistema za upravljanje varovanja informacij** (SUVI oz. ISMS¹⁴).

V pomoč upravljavcem glede zahtevane ravni varnosti osebnih podatkov in obsega preverjanja s strani državnih nadzornikov za varstvo osebnih podatkov je Informacijski pooblaščenec pripravil poseben **vprašalnik o informacijski varnosti**, ki ga Informacijski pooblaščenec uporablja pri postopkih, ki jih sproži po uradni dolžnosti (t.i. ex offo postopki), gre pa običajno za večje upravljavce oziroma za celovitejše inšpekcijske preglede.



Vprašalnik je namenjen predhodni pridobitvi informacij o postopkih in ukrepih, ki jih zavezanec izvaja za zavarovanje osebnih podatkov. Pri oblikovanju vprašalnika smo se v veliki meri naslonili na zahteve standarda ISO/IEC 27001, pri čemer smo dodali določena specifična vprašanja, ki izhajajo iz zahtev Zakona o varstvu osebnih podatkov (ZVOP-1). Kjer je bilo možno, je dodana oznaka na ustrezno kontrolo po standardu ISO/IEC 27001. S pomočjo vprašalnika lahko upravljavci lažje ugotovijo, kakšne so v praksi zahteve glede varnosti osebnih podatkov in kaj je predmet inšpekcijskega nadzora.

¹⁴ Information Security Management System.

Podrobnejša obrazložitev zakonskih zahtev glede zavarovanja osebnih podatkov

V nadaljevanju podrobneje pojasnjujemo nekatera področja, na katerih se v praksi tudi pri večjih upravljavcih pojavljajo vprašanje glede zahtev ZVOP-1.

Dostopne pravice

Dostopne pravice uporabnikov morajo biti jasne in skladne z nalogami, ki jih opravljajo uporabniki, predvsem pa 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 ali medsebojna izmenjava sredstev za avtentikacijo in avtorizacijo uporabnikov, kot so uporabniška imena in gesla, kartice ipd., razen izjemoma, iz razloga nujnosti.

Beleženje dostopov do podatkov (sledljivost)

Upravljalci 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**. Takšno raven sledljivosti morajo zagotoviti upravljavci, ki:

- **obdelujejo večje število osebnih podatkov** (npr. večji klubi zvestobe, državni registri, zbirke transakcijskih in demografskih podatkov o komitentih, zavarovancih, naročnikih elektronskih komunikacij ipd.),
- obdelujejo **občutljive osebne podatke** (kot so npr. zdravstveni podatki),
- obdelujejo osebne podatke, katerih zloraba bi lahko imela **hujše posledice za posameznika**.

Odstopanje od tega načela je možno le na podlagi ustrezne analize in obravnave tveganj. ZVOP-1 po mnenju Informacijskega pooblaščenca po drugi strani **ne zahteva takšne ravni sledljivosti, ki bi beležila celotni življenjski cikel podatkov** (torej stare in nove vrednosti podatkov), saj bi tovrstna zahteva lahko pomenila nesorazmerno obremenitev za informacijski sistem upravljavca.

24. člen ZVOP-1 prav tako formalno ne zahteva **beleženja namena dostopa do osebnih podatkov**.

Kot preventivni ukrep posebej poudarjamo, da naj bodo osebe, ki obdelujejo osebne podatke, **obveščene o tem, da se njihovi dostopi beležijo**¹⁵. S tem ukrepom se lahko bistveno pripomore k večji ozaveščenosti uporabnikov in k preprečevanju nezakonitih vpogledov v osebne podatke.

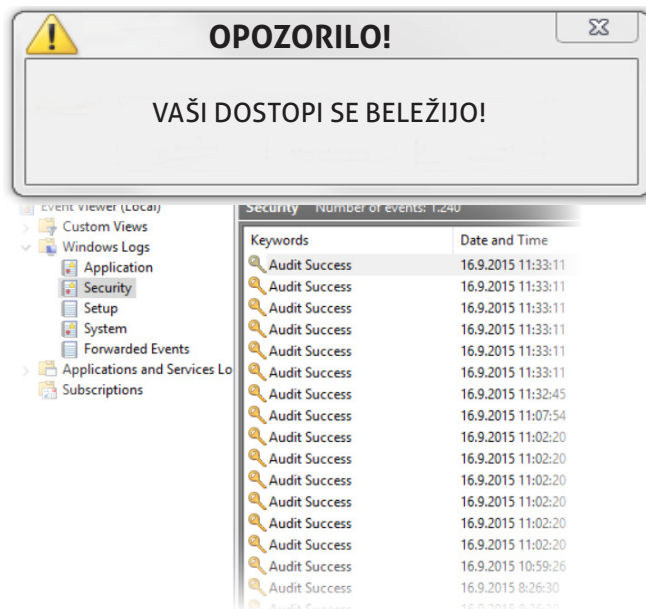
Beleženje dostopov mora biti takšno, da omogoča naknadno preverjanje, kdo je, kdaj in do katerih osebnih podatkov dostopal; **identifikacija osebe, ki je stopila v stik s podatki, mora biti enolična**, torej se mora nanašati na posamezno konkretno osebo (uporabnika, zaposlenega ali osebe pri zunanjem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

Sledljivost obdelave osebnih podatkov se nanaša tako na **notranjo** kot na **zunanjo 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 upravljavca 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.

Zagotavljanje sledljivosti je lahko pri pogodbeni obdelavi osebnih podatkov predmet dogovora med upravljavcem (naročnikom) in pogodbenim obdelovalcem (zunanjim izvajalcem). Če se npr. upravljavca odloči uporabljati oblako rešitev za obdelavo osebnih podatkov (npr. oblako rešitev za upravljanje odnosov s strankami), lahko sledljivost obdelave osebnih podatkov za upravljavca zagotavlja ponudnik storitve, torej pogodbeni obdelovalec. Upravljavca se mora o tem vnaprej prepričati in dogovoriti s pogodbenim obdelovalcem.

Zahteve glede sledljivosti so manjše, če je bilo pri postavljanju določene informacijske rešitve striktno upoštevano **načelo sorazmernosti** oziroma pristop **vgrajene zasebnosti** (angl. privacy by design). Že pri oblikovanju poizvedb in iskalnikov (kakšni so možni iskalni kriteriji, kaj se izpiše pri rezultatih iskanja – več prikazanih podatkov na zaslonu

¹⁵ Npr. s pojavnim okno, izpisom opozorila ali na drug ustrezen način ob vstopu v informacijski sistema ali aplikacijo. Opozorilo je lahko implementirano tudi tako, da ga mora uporabnik aktivno zapreti, da lahko nadaljuje z dostopom do podatkov.



namreč 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, se lahko z **omejitvijo obdelave na nujno potrebno** bistveno zmanjšajo obremenitve z vidika zagotavljanja sledljivosti.

Sledljivost dostopov se lahko hrani ločeno od izvornih baz podatkov in ni nujno, da je dostopna »na klik«, temveč mora biti dostopna v razumnem roku. Zagotovljena mora biti celovitost in avtentičnost zapisov.

Rok hrambe sledljivosti

5. točka 1. odstavka 24. člena ZVOP-1 upravljavca oz. pogodbenega obdelovalca osebnih podatkov obvezuje k vzpostavitvi sistema sledljivosti oz. revizijske sledi obdelave osebnih podatkov, točneje, da povzameta »organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščen uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščen obdelava teh podatkov tako, da se [...] 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.**

Obdobje, ko je še mogoče zakonsko varstvo pravic posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov, določa materialno pravo.

Splošni zastaralni rok za uveljavljanje terjatev določa Obligacijski zakonik (Uradni list RS, št. 97/07-UPB1, v nadaljevanju OZ) v 346. členu, in sicer pet let, ki v skladu z določbo 1. odstavka 336. člena OZ začne teči »prvi dan po dnevu, ko je upnik imel pravico terjati izpolnitev obveznosti, če za posamezne primere ni z zakonom določeno kaj drugega«, kar bo prvi dan po nedopustni obdelavi ali posredovanju osebnih podatkov.

V primeru, da je bilo s takšno nedopustno obdelavo storjeno tudi kaznivo dejanje, je pri določitvi zastaralnega roka potrebno upoštevati določbe 353. člena OZ, kjer je v prvem odstavku določeno: »Če je škoda povzročena s kaznivim dejanjem, za kazenski pregon pa je predpisan daljši zastaralni rok, zastara odškodninski zahtevek proti odgovorni osebi, ko izteče čas, ki je določen za zastaranje kazenskega pregona.« V tem primeru torej velja rok, predpisan za zastaranje kazenskega pregona. Ta rok določa 90. člen KZ-1 in je odvisen od dolžine zagrožene kazni zapor. Za najpogostejši oblik kaznivega dejanja zlorabe osebnih podatkov po 1. in 2. odstavku 143. členu KZ-1 je zagrožena denarna kazen ali zapor do enega leta, zato je kazenski pregon v skladu s 5. točko 1. odstavka 90. člena KZ-1 zastara po poteku šest let od storitve kaznivega dejanja.

Za kvalificirane oblike po sledečih odstavkih ter za nekatera druga kazniva dejanja je to obdobje seveda tudi ustrezno daljše.

Informacijski pooblaščenec ocenjuje, da je **glede večine obdelav osebnih podatkov sprejemljivo revizijsko sled** obdelave osebnih podatkov po 5. točki 1. odstavka 24. člena **hraniti za obdobje šestih (6) let od dne, ko se je zadevna obdelava osebnih podatkov tudi zgodila**. Upošteva določeno sektorsko zakonodajo (zlasti glede nekaterih računovodskih listin oz. uradnega poslovanja) pa je lahko ta rok tudi ustrezno daljši.



Namig: Vas zanima javni oblak?



S pomočjo [Smernic glede računalništva v oblaku](#) in kontrolnega seznama preverite, katere zahteve ZVOP-1 morate izpolniti.

Zavarovanje občutljivih osebnih podatkov

14. člen ZVOP-1 določa posebne zahteve glede zavarovanja občutljivih osebnih podatkov, kot so npr. podatki zdravstvenem stanju. Žal se omenjene določbe ZVOP-1 pri tem osredotočajo samo na določena in specifična tveganja in ne predvidevajo celovitejših ukrepov za zavarovanje občutljivih podatkov, kot bi bila npr. zahteva po uvedbi **sistema za upravljanje informacijske varnosti**, kot je to zahtevano na področju elektronskih komunikacij in elektronske hrambe dokumentarnega in arhivskega gradiva.

Dileme glede implementacije v praksi povzroča predvsem določba 2. odstavka 14. člen ZVOP-1, ki določa:

(2) Pri prenosu občutljivih osebnih podatkov preko telekomunikacijskih omrežij se šteje, da so podatki ustrezno zavarovani, če se posredujejo z uporabo kriptografskih metod in elektronskega podpisa tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom.

Določba namreč ne opredeljuje natančneje elektronskega podpisa, saj obstajajo različne vrste elektronskega podpisa (navadni, varni itd.), prav tako pa se postavlja vprašanje učinkovitosti in uporabe elektronskega podpisa za zagotavljanje »nečitljivost oziroma neprepoznavnost med prenosom«, saj se to zahtevo zagotavlja (že) s šifriranjem podatkov. Iz prakse Informacijskega pooblaščenca glede na navedeno izhajajo naslednja priporočila:

- Pošiljanje občutljivih osebnih podatkov po elektronski pošti le z uporabo uveljavljenih kriptografskih metod (npr. PGP¹⁶), s šifrirnimi ključi ustreznih dolžin.
- Rešitve z uporabo kvalificiranih digitalnih potrdil (na obeh straneh komunikacijske poti), uporaba https protokola ter dodatna zaščita z uporabniškim imenom in geslom.
- Uporaba VPN dostopa.
- Uporaba elektronskega podpisa, kjer je to smiselno za zagotovitev verodostojnosti in celovitosti (npr. pri podpisovanju dokumentov, ki vsebujejo občutljive osebne podatke in se prenašajo prek telekomunikacijskih omrežij).

¹⁶ https://en.wikipedia.org/wiki/Pretty_Good_Privacy

Nadzor nadzornikov (Quis custodiet ipsos custodes?)

Administratorji oziroma privilegirani uporabniki imajo oziroma celo morajo imeti širok obseg pooblastil, saj njihove naloge vključujejo različna opravila, ki terjajo dostop do večje količine podatkov (npr. vzdrževanje podatkovnih baz). Kot taki predstavljajo posebna tveganja, saj so lahko zlorabe z njihove strani kritične, težko zaznavne in se lahko nanašajo na celotne baze (osebnih) podatkov. Nadzor administratorjev zato terja poseben premislek in ukrepe, s katerimi lahko upravljamo tveganja, ki jih predstavljajo njihova široka pooblastila. Revizijska sled obdelave osebnih podatkov mora 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. 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. Med možne ukrepe, odvisno od konkretnih okoliščin, sodijo:

- redno pregledovanje obsega administratorskih pravic in njihovo omejevanje po načelu nujnosti in minimizacije,
- strogo izvajanje politike upravljanja administratorskih gesel,
- sistem »štirih oči«, kjer posamezna oseba ne more pridobiti dostopa do podatkov brez dovolilnic druge osebe,
- beleženje dostopov do podatkov s strani administratorjev na mesta, ki so izven njihovega dosega in na način, da beleženja ne morejo izklopiti, naknadno popravljati ali drugače okrniti celovitosti zapisov o dostopih¹⁷.

Uporaba zunanjih nadzornikov

IP priporoča, da organizacije, če jim sredstva to omogočajo, izvajajo periodične ali priložnostne zunanje revizije svoje informacijske varnosti. Tovrstne revizije pogosto odkrijejo slabe vzorce ukrepov varovanja osebnih podatkov, ki bi sicer ostali skriti ali neopaženi.

¹⁷ Glej npr. kontrolo 12.4.3. standarda ISO 27002:2013 (oz. A.10.10.3, A.10.10.4 verzije 2005).

Zahteve glede varnosti osebnih podatkov pri pogodbeni obdelavi

Ključen pogoj za ustrezno ureditev pogodbenih odnosov je obstoj **pisne pogodbe o pogodbeni obdelavi** (ta je lahko sklenjena tudi v enakovredni elektronski obliki). Sestavni del pogodbe o pogodbeni obdelavi morajo biti **konkretizirani postopki in ukrepi za zavarovanje osebnih podatkov**, ki se jih bo držal pogodbeni obdelovalec. Zgolj sklic na zahteve ZVOP-1 ali določbe, kot so »podatki bodo varovani skladno z »ZVOP-1« ne zadostujejo. Postopke in ukrepe za varnost podatkov je treba opredeliti in konkretizirati (npr. kakšni so postopki fizične varnosti, kopiranja podatkov itd.). Dopusten je tudi sklic na obstoječe pravilnike o informacijski varnosti upravljavca ali pogodbenega obdelovalca, če so seveda ti pravilnik ustrezni.



Namig: Mnenja IP v konkretnih situacijah



Na spletni strani IP najdete več kot 30 mnenj, ki se nanašajo na konkretna vprašanja glede zavarovanja OP.

Pogodbeni obdelovalec včasih ne bo niti vedel, da nastopa v tej vlogi (npr. če ponuja storitev hrambe podatkov, naročniki pa pri njemu hranijo podatke v kriptirani obliki). Upravljavec osebnih podatkov bo praviloma vedno vedel, ali bo pogodbenemu obdelovalcu zaupal osebne podatke ali ne, zato je njegova dolžnost, da se izpolnijo pogoji iz 11. člena ZVOP-1.

Odgovornost za ustrezno varnost nosita oba, saj to izrecno zahteva 1. odstavek 25. člena ZVOP-1, ki določa, da so **upravljavci osebnih podatkov in pogodbeni obdelovalci dolžni zagotoviti zavarovanje** osebnih podatkov na način iz 24. člena ZVOP-1.

Primeri iz inšpekcijske prakse

- **NOTRANJINADZOR.** Informacijski pooblaščenec je večjemu upravljavcu na področju zdravstvene oskrbe že odredil protokoliranje in izvajanje notranjega nadzora nad zakonitostjo uporabe osebnih podatkov kot potrebnega organizacijskega ukrepa za zagotavljanje ustrezne varnosti osebnih podatkov. Notranji nadzor je – na podlagi izvedene analize tveganj – smiseln v situacijah, kjer obstajajo velika tveganja, npr. pri dostopu do velikih državnih registrov, velikih zbirkah transakcijskih podatkov, zbirkah občutljivih osebnih podatkov. Notranji nadzor, katerega namen je zaznava nezakonite obdelave osebnih podatkov in sprejem postopkov in ukrepov za preprečitev takšnih obdelav mora biti protokoliran, ne pa podvržen sprotnemu pavšalnemu odločanju o predmetu in obsegu nadzora. To pomeni, da bi moral upravljavec opredeliti **obseg, pogostost, izvajalce, cilje, način izvajanja, poročanje in ukrepanje v primeru zaznanih nezakonitih obdelav osebnih podatkov.** Notranji nadzor naj bi se izvajal z ustrezno frekvenco in obsegom¹⁸.



- **POLITIKA GESEL.** Informacijski pooblaščenec je upravljavcem že odredil, da morajo v internem aktu **določiti in začeti izvajati**



politiko upravljanja gesel za informacijski sistem, ki mora opredeljevati vsaj naslednje postopke in zahteve glede gesel: zahtevano dolžino, postopek dodeljevanja in spreminjanja, zahtevano kompleksnost, zahteve glede zgodovine (ponavljanja) gesel in trajanje veljavnosti gesel. Prav tako so bile izdane odločbe, kjer so morali upravljavci **preprečiti uporabo skupinskih uporabniških pravic, zagotoviti hrambo gesel v neberljivi obliki** in izbrisati sezname gesel v berljivi obliki, ki so jih hranili administratorji.

- **PREVERJANJE ODPORNOSTI NA ZNANE RANLJIVOSTI.** Informacijski pooblaščenec je v

¹⁸ Nesorazmernost pri tem ukrepu lahko pomeni pretirane obremenitve za zaposlene in lahko neugodno vpliva na organizacijsko klimo, zato prepogosto ali preobsežno izvajanje lahko implicira nesorazmerne obdelave osebnih podatkov in druge negativne posledice.

inšpekcijskih postopkih ugotovil zlorabo osebnih podatkov zaradi neustrezne varnosti spletnega mesta upravljavca, saj ta ni preveril, ali je spletno mesto odporno vsaj na najbolj pogoste in znane spletne ranljivosti¹⁹, kot je npr. SQL vrivanje²⁰.



- **SLEDLJIVOST.** Informacijski pooblaščenec je številnim upravljavcem, zlasti tistim, ki obdelujejo občutljive osebne podatke, odredil uvedbo sistema sledljivosti obdelave osebnih podatkov, ki omogoča beleženje vsakega dostopa do osebnih podatkov. Prav tako je bila odrejena **sledljivost izvozov oziroma paketnih poizvedb in tiskanja osebnih podatkov.**



• **POGODBENA OBDELAVA.** Informacijski pooblaščenec je kaznoval upravljavca, ki je najel pogodbenega obdelovalca za prevoz dokumentacije z osebnimi podatki na uničenje, ker z njim **ni sklenil ustrezne pogodbe** o pogodbeni obdelavi osebnih podatkov (11. člen ZVOP-1). Prav tako je bil kaznovan tudi pogodbeni obdelovalec, ker se **ni držal postopkov in ukrepov** za zavarovanje osebnih podatkov, saj morajo te zagotavljati in izvajati tudi pogodbeni obdelovalci osebnih podatkov.



¹⁹ Glej npr. OWASP Top 10: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

²⁰ <http://www.monitor.si/clanek/vrivanje-sql-od-a-do-z/123404/>



• **ZBIRANJE OBČUTLJVIH OSEBNIH PODATKOV PREK SPLETNIH STRANI.** Informacijski pooblaščenec je bolnišnici odredil, da mora pri elektronskem naročanju na svoji spletni strani zavarovati prenos osebnih podatkov z uporabo uveljavljenih kriptografskih metod, ki varujejo zaupnost in celovitost posredovanih podatkov, čeprav občutljive osebne podatke vpisujejo pacienti sami.

• **PRILAGODITEV INFORMACIJSKE VARNOSTNE POLITIKE.** Informacijski pooblaščenec je zavezancu iz javnega sektorja izdal odločbo za zagotovitev poštenosti in zakonitosti obdelave osebnih podatkov, ki se obdelujejo pri uporabi nove opreme za varovanje omrežja, in sicer je moral zavezanec **prilagoditi in začeti izvajati varnostno politiko za varovanje internega omrežja** zavezanca; varnostna politika mora med drugim vsebovati:

- omejitve uporabe omrežja zavezanca;
- popis mehanizmov, ki se izvajajo za varovanje in stabilnost delovanja omrežja z navedbo protokolov in storitev, ki se pregledujejo;
- obrazložitev postopkov, ki se izvajajo za filtriranje ali pregledovanje prometa,
- režim nadgradenj opreme za varovanje internega omrežja zavezanca,
- postopke in ukrepe za nadzor fizičnega in logičnega dostopa do systemskega prostora in opreme.



• **POENOTENJE ZBIRK OSEBNIH PODATKOV.** Informacijski pooblaščenec je zavezancu izdal odločbo, po kateri je moral zavezanec zagotoviti celovitost, točnost in ažurnost zbirk osebnih podatkov svojih strank, ki jih je uporabljal za neposredno trženje po e-pošti, saj je zaradi neposodobljenih zapisov v podatkovnih bazah (osebni podatki posameznika so bili podvojeni in neposodobljeni v različnih podatkovnih zbirkah), prihajalo do **nepopolnega brisanja osebnih podatkov** in so posamezniki prejeli oglasna sporočila kljub izrecnemu preklicu.

- **UKREPI PO VDORU NA SPLETNO STRAN.**

Informacijski pooblaščenec je upravljavcu spletnega foruma, na katerem je zaradi neposodobljenega vmesnika za administracijo spletne strani prišlo do vdora na spletno stran in javne objave osebnih podatkov uporabnikov, odredil, da mora:

- izbrisati vsa obstoječa gesla uporabnikov portala in uporabnike obvestiti, da so bila gesla, elektronski naslovi ter uporabniška imena uporabnikov portala javno objavljena;
- onemogočiti dostop do osebnih podatkov uporabnikov spletnega portala pogodbenemu obdelovalcu;
- zagotoviti, da bodo nova gesla uporabnikov portala hranjena samo v kriptirani obliki.



- **ZAVAROVANJE VIDEONADZORA.** Pri inšpekcijskih postopkih v zvezi z videonadzorom Informacijski pooblaščenec pogosto odkriva pomanjkljivo zavarovane videonadzorne sisteme. Snemalne naprave so bodisi nameščene v neprimernih prostorih, nezaklenjenih, nenadzorovanih, dostopnih številnim osebam, bodisi snemalniki niso zavarovani z dostopnim geslom ali je le-to podeljeno (pre)velikemu številu oseb. Pogosto se ne vodi evidenca izvajanja videonadzora, kar onemogoča notranjo sledljivost (vpoglede in posege v posnetke) ali zunanjo sledljivost (posredovanje posnetkov). Priporočljivo je, to pa je hkrati tudi zakonska obveznost, da so za upravljanje z videonadzornim sistemom izrecno pooblaščne točno določene osebe, in sicer čim manjši krog le-teh, pri čemer mora biti jasno določeno, kdo upravlja z videonadzorom v tehničnem pogledu ter katere osebe smejo dostopati in obdelovati osebne podatke v videonadzornih posnetkih. Priporočamo, da upravljavci osebnih podatkov in izvajalci videonadzora o tem izdelajo natančna pravila, ki so lahko zapisana bodisi v posebnem aktu o izvajanju videonadzora ali v splošnem aktu o zavarovanju osebnih podatkov.

Najpogostejše kršitve

Na področju zavarovanja osebnih podatkov gre za različna odstopanja od uveljavljenih standardov informacijske varnosti. Na takšna odstopanja morajo včasih biti pozorni že razvijalci informacijskih rešitev, določene ukrepe (zlasti organizacijske), pa morajo izvajati uporabniki takšnih rešitev (upravljavci in pogodbeni obdelovalci). Med najpogostejše napake sodijo:

- 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,
- ni ločevanja testnega, šolskega in produkcijskega okolja,
- zagotavljanje le tehničnih, ne pa tudi organizacijskih ukrepov (npr. izobraževanje uporabnikov, notranji nadzor ipd.).



Zaključek

V srednjem veku so bile knjige vredne celo bogastvo in srednjeveške knjižnice so se včasih borile proti kraji in izgubi vrednih knjig tudi tako, da so bile posamezne knjige dobesedno priklenjene na knjižne police. Od takrat je minilo veliko časa in danes so podatki tisti, ki so lahko vredni celo bogastvo oziroma jih mnogi imenujejo kar za valuto informacijske družbe. Podatkov ne moremo prikleniti na knjižne police, prav tako s priklepjanjem ne moremo zagotoviti njihove zaupnosti. Varnost podatkov zahteva, da so podatki neokrnjeni, na voljo samo tistim, ki jih smejo izvedeti in da so podatki na voljo takrat, ko so potrebni. Navedenega ne moremo zagotoviti z enim samim ukrepom, prav tako določeni ukrepi ne bodo ustrezni v vseh situacijah. K sreči je bilo na temo informacijske varnosti napisanega veliko in nam ni treba odkrivati tople vode. Mnogi so se že opekli in tako imamo veliko primerov dobrih in slabih praks, kataloge groženj, ki pretijo varnosti podatkov, in kataloge postopkov in ukrepov za njihovo varnost. Orodij nam torej ne manjka, ključno pa ostaja zavedanje, da samo tehnika ne more zagotoviti varnosti, da je vsak od nas pomemben element v zagotavljanju informacijske varnosti in da brez varnosti (osebnih) podatkov tudi ni varstva (osebnih) podatkov.

Evropski zakonodajni ovir za varstvo osebnih podatkov se spreminja in posodablja. Čedalje več poudarka bo namenjenega izkazovanju proaktivnosti na področju varnosti, sankcije za kršitelje pa ne bodo zgolj finančne narave, temveč vse bolj takšne, da bodo imele vpliv tudi na zaupanje strank in poslovnih partnerjev. Zagotavljanje informacijske varnosti bo tako pridobivalo na pomenu – v informacijski družbi nenazadnje drugače ne more biti.

