

Viri podatkov

7. srečanje:

- **Pravni in etični vidiki varstva osebnih podatkov**
- **Statistična zaščita podatkov**

Mojca Bavdaž (mojca.bavdaz@ef.uni-lj.si)

Varstvo osebnih podatkov



Pravica do zasebnosti

Prvi krog zasebnosti.

Drugi krog zasebnosti.

absolutne javne osebnosti

relativne javne osebnosti

Tretji krog zasebnosti.



Pravna podlaga v Sloveniji

Ustava RS

Zakon o varstvu osebnih podatkov (uradno prečiščeno besedilo) (ZVOP-1-UPB1), 27.7.2007

Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES

Začetek veljavnosti 25.5.2018 neposredno

ZVOP-2 ???



Osebni podatek

6.čl.ZVOP:

katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen. Posameznik je **določena ali določljiva** fizična oseba, na katero se nanaša osebni podatek; fizična oseba je določljiva, če se jo lahko **neposredno ali posredno** identificira, predvsem s sklicevanjem na **identifikacijsko številko ali na enega ali več dejavnikov**, ki so značilni za njeno fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto, pri čemer način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa.

4.čl.GDPR:

katero koli informacijo v zvezi z **določenim ali določljivim** posameznikom; določljiv posameznik je tisti, ki ga je mogoče **neposredno ali posredno** določiti, zlasti z navedbo identifikatorja, kot je ime, **identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov**, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika

Občutljivi osebni podatki

6.čl.ZVOP:

Občutljivi osebni podatki so 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 evidenc, ki se vodijo na podlagi zakona, ki ureja prekrške;
- tudi biometrične značilnosti, če je z njihovo uporabo mogoče določiti posameznika v zvezi s kakšno od prej navedenih okoliščin.

9.čl.GDPR (posebne vrste OP):

Prepovedani sta obdelava osebnih podatkov, ki razkrivajo

rasno ali etnično poreklo,

politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in

obdelava genetskih podatkov,

biometričnih podatkov za namene edinstvene identifikacije posameznika,

podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.

10.čl: kazenski...



Inšpekcijski nadzor v letu 2018



	2017 (celo leto)	2018 (celo leto)	+
Število odprtih inšpekcijskih zadev	655	1029	+ 57%
Število rešenih zadev	594	722	+ 22%
Število dodeljenih zadev na nadzornika	61	92	+ 51%
Uradna obvestila o kršitvi varnosti	0	68	

- 12 državnih nadzornikov za varstvo OP

Prijavljene kršitve: izguba/kraja nosilcev OP (računalnikov in službenih gsm-jev), nepooblaščen dostop do OP zaradi: *programske napake, *zlorabe pooblastil zaposlenih, *hekerskega napada na informacijski sistem, onemogočanja dostopa do OP zaradi kriptiranja z zlonamerno programsko kodo



Uporaba GDPR

1. Obdelava v celoti ali delno avtomatizirana ali zbirka OP.
2. GDPR se **NE** uporablja (**LE**) za obdelavo OP:
 - (a) če dejavnost izven uporabe prava EU (nacionalna varnost);
 - (b) ko DČ izvajajo skupno zunanjo in varnostno politiko;
 - (c) če fiz. oseba za popolnoma (izključno) osebno/domačo rabo;
 - (d) organi za preprečevanje/preiskovanje/odkrivanje/pregon KD ali izvrševanje kaz. sankcij, varovanje grožnjam javne varnosti
 - (e) sodišča v „dejavnosti sojenja“.



Ozemeljska veljavnost GDPR

1. **po sedežu upravljavca ali obdelovalca v EU**, ne glede ali obdelava poteka v EU ali ne. (=čtetudi obdelave sploh ni v EU)
2. **posameznikov ki so v EU**, upravljavec/obdelovalec **pa nima sedeža v EU**, če so dejavnosti obdelave **povezane z**:
 - (a) nudenjem B/S posameznikom v EU, ne glede na (ne) plačilo (*(*nudenje = uporaba jezika ali valute, ki se uporablja v 1 ali več DČ, možnost naročanja B/S v tem drugem jeziku, navedba strank ali uporabnikov, ki so v EU -- → vse to jasno pokaže, da želi upravljavec nuditi B/S posameznikom v EU)*)
 - (b) spremljanjem njihovega vedenja v EU (*(*npr. se mu sledi na internetu, profiliranje – Google; vedenje/obnašanje mora biti v EU, ne glede na to, od kje poteka spremljanje)*)
3. če upravljavec nima sedeža v EU, ampak v kraju, kjer se pravo DČ **uporablja na podlagi MJP** (npr. v DKP DČ)

Obdelava osebnih podatkov

= kakršnokoli „rokovanje“ z OP, vključno z vpogledom, obvezna pravna podlaga

Izključno za osebno uporabo, družinsko življenje \Rightarrow x

V javnem sektorju \Rightarrow ključna osnova **zakon** itd.

V zasebnem sektorju \Rightarrow ključna osnova **osebna privolitev** itd.



Sodbe sodišča EU – kaj vse je zbirka OP?

1.) Bodil Linquist v. EK: ga. Bodil Linquist je za potrebe svoje cerkve (Švedska) naredila spisek sodelavcev z njihovimi OP (ime, tel. št., podatke o zdravstvenem stanju sodelavca) in ga dala na internet.

Avtomatska obdelava OP + posredovanje OP v 3. države, četudi švedski strežnik, saj pri uporabi interneta obstaja možnost, da OP dobi oseba iz 3. države.



2.) Člani skupnosti Jehovih prič (C-25/17, 10.7.2018)

Finski DPA je leta 2013 članom skupnosti Jehovih prič prepovedala zbiranje in obdelavo OP med oznanjevanjem od vrat do vrat, saj niso bili spoštovani zakonski pogoji za obdelavo OP. Delali so zapiske o osebah, beležili imena+priimke, podatke o njihovem verskem prepričanju in družinskih razmerah, posledično naj bi župnije izdelale seznam oseb, ki so izrazile željo, da jih člani Jehovih prič ne bi več obiskovali na domu →> **pritožba**→ **Finsko upravno sodišče**: odpravilo odločbo DPA, ker da verska skupnost ni upravljavec OP →> DPA izpodbija na **vrhovnem upravnem sodišču** →> to na SEU naslovi predlog za predhodno odločanje.

SEU: ne gre za popolnoma domačo ali osebno rabo, gre za zbirko OP, verska skupnost je upravljavec OP.



Pravne podlage za javni sektor
člen 6 (1) Splošne uredbe

Primeri:

ZAKON
točka (c)



Podatki pacientov pri
zdravstveni obravnavi.

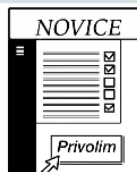
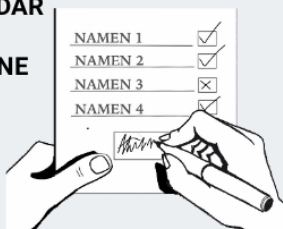


Podatki strank upravnih postop-
kov pri CSD.



Podatki o obsojencih iz kazenskih
evidenc pri MNZ.

**PRIVOLITEV, KADAR
NE GRE ZA
IZVAJANJE JAVNE
OBLASTI**
točka (a)



Prijava na e-novice.

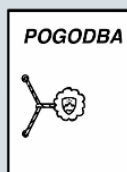


Sodelovanje v nagradni igri.



Objava fotografij učencev na
spletu.

**POTREBNA ZA
IZVAJANJE ALI
ZA SKLENITEV
POGODBE**
točka (b)



Izvajanje pogodb na podlagi
javnega naročila.



Izvajanje pogodb o najemu
prostorov.

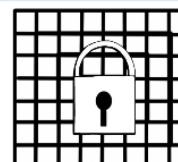


Delo po pogodbi zunaj delovnega
razmerja.

**POTREBNO ZA
IZVAJANJE
JAVNE NALOGE**
točka (e) v povezavi s
9/IV členom ZVOP-1



Pošiljanje obvestil za javnost
na službene e-naslove
novinarjev.



Varovanje omrežja.



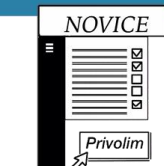
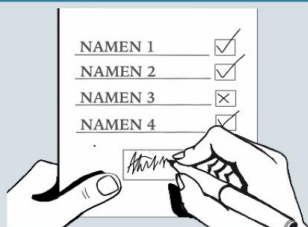
Preprečevanje goljufij.



Pravne podlage za zasebni sektor, ko obdeluje običajne osebne podatke
člen 6 (1) Splošne uredbe

Primeri:

PRIVOLITEV
točka (a)



Prijava na prejemanje e-novic.

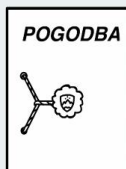


Sodelovanje v nagradni igri.

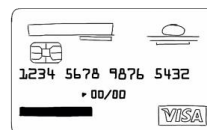


Objava osebnih podatkov na spletu.

OBDELAVA JE POTREBNA ZA SKLENITEV ALI ZA IZVAJANJE POGODBE
točka (b)



Posameznik izvede spletni nakup.



Nakup v veleblagovnici z bančno kartico.



Delo po pogodbi zunaj delovnega razmerja.

ZAKON ALI IZVAJANJE JAVNIH NALOG
točki (c) ali (e)



Podatki zaposlenih na podlagi Zakona o delovnih razmerjih.

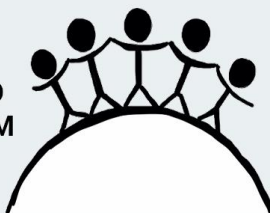


Podatki komitentov bank na podlagi Zakona o bančništvu.

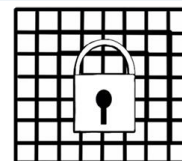


Podatki zavarovancev na podlagi Zakona o zavarovalništvu.

ZAKONITI INTERESI, KI PREVLAĐAJO NAD INTERESOM POSAMEZNIKA
točka (f)



Pošiljanje obvestil za javnost na službene e-naslove novinarjev.



Varovanje omrežja.







Preprečevanje goljufij.



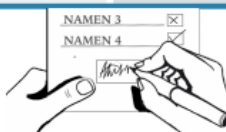
OBDELAVA OSEBNIH PODATKOV PRI NEPOSREDNEM TRŽENJU FIZIČNIM OSEBAM

Obdelava dopustna BREZ PRIVOLITVE

POT OBVEŠČANJA	PODATKI	POGOJI	PRAVNA PODLAGA	POSEBNI POGOJI
Navadna pošta 	Ime, priimek, stalno in začasno prebivališče	<p>Če so podatki javno objavljeni (imenik, profilna spletna stran, itd.).</p> <p>Če so bili podatki pridobljeni v okviru zakonitega opravljanja dejavnosti (vizitke, dogodki, sejmi, nakup, itd.).</p>	<p>72/I ZVOP-1</p> <p>72/I ZVOP-1</p>	<p>Jasna možnost, da lahko zahteva prenehanje pošiljanja obvestil (obvestilo o pravici do ugovora po 73. čl. ZVOP-1).</p> <p>Če posameznik že ob zbiranju ali kadarkoli kasneje ne dovoli uporabe njegovih podatkov za neposredno trženje, upravljavec njegovih podatkov ne sme uporabiti za ta namen.</p>
Elektronska pošta 	E-naslov	<p>Če podjetje od kupca svojih izdelkov/storitev pridobi njegov elektronski naslov, ga lahko uporablja tudi za trženje svojih podobnih izdelkov/storitev.</p> <p>Če so e-naslovi posameznikov javno objavljeni na spletnih omrežjih in pri drugih ponudnikih spletnih storitev, kjer je posameznik sprejel politiko zasebnosti, ki predvideva neposredno trženje na te e-naslove.</p>	<p>158/II ZEKom-1</p> <p>Pogodba med ponudnikom spletne storitve in posameznikom v povezavi s 6(1f) Splošne uredbe</p>	<p>Jasna možnost, da brezplačno in enostavno zahteva prenehanje uporabe naslova za ta namen (pravica po drugem odst. 158 ZEKom-1).</p> <p>Možnost, da lahko zahteva prenehanje pošiljanja obvestil (obvestilo o pravici do ugovora po čl. 21 Splošne uredbe).</p>
Telefon 	Tel. številka iz imenika	Za namen ponujanja izdelkov ali storitev po telefonu na številke iz Telefonskega imenika Slovenije.	150 ZEKom-1	<p>Če v imeniku ni označbe, da posameznik NE želi prejemati klicev s komercialnim namenom (označba po tretjem odstavku 150. čl. ZEKom-1).</p>
UPORABA OBJAVLJENIH KONTAKTOV ZAPOSLENIH ZA TRŽENJE PODJETJU ALI DRUGI ORGANIZACIJI				
Navadna pošta/telefon elektronska pošta 	Naslov, e-naslov, telefon	Če podjetje trži na kontakt zaposlenega, ko je kontakt javno objavljen v skladu s 106. členom ZVOP-1.	48/I ZDR, 106/II ZVOP-1 v povezavi s 6(1f) Splošne uredbe	Možnost, da lahko zahteva prenehanje pošiljanja obvestil (obvestilo o pravici do ugovora po čl. 21 Splošne uredbe).

UPOŠTEVAJTE PREKLIČE

V drugih primerih je obdelava dopustna
le na podlagi PRIVOLITVE



INFORMACIJSKI
POOBLAŠČENEC





Veljavna PRIVOLITEV po Splošni uredbi



DOKAZLJIVA

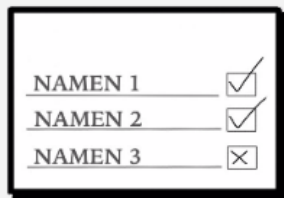
Dokazljiva je privolitev, ki omogoča, da jo lahko upravljavec kadarkoli izkaže na zahtevo nadzornega organa.



PROSTOVOLJNA

Prostovoljna je privolitev, ki:

- zagotavlja resnično izbiro in nadzor,
- NE izhaja iz razmerja nesorazmerne moči med upravljavcem in posameznikom (delovno razmerje, javna oblast itd.),
- NI pogoj za sklenitev pogodbe,
- jo lahko posameznik kadarkoli umakne,
- ne prinaša škodljivih posledic za posameznika, če je ne poda ali če jo umakne.



SPECIFIČNA

Specifična je privolitev, ki je podana za konkretno opredeljen namen.



INFORMIRANA

Informirana je privolitev, ki jasno pove:

- kdo je upravljavec,
- za kakšen namen se bodo podatki obdelovali,
- kateri podatki se bodo obdelovali,
- da lahko posameznik privolitev kadarkoli umakne,
- da ima pravico, da zanj ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov,
- o morebitnih tveganjih pri prenosu osebnih podatkov v tretjo državo ali mednarodno organizacijo.



NEDVOUMNA

Nedvoumna je privolitev, ki je podana z izkazljivim in aktivnim dejanjem posameznika, ni domnevna.



Ne preohlapni, presplošni pojmi, ker so nepošteni, (saj posameznik ne more dati informirane privolitve) npr.:

- „Vaše OP uporabljamo za izboljšanje kvalitete te storitve.“
- „Vaše OP lahko posredujemo tretjim za namen izboljšanja storitve.“
- „OP pošiljamo le našim skrbno izbranim poslovnim partnerjem.“
- „Z nadaljnjim koriščenjem te spletne strani izražate privolitev za obdelavo vaših OP.“
- „Zbiramo OP kot npr. ime, naslov, starost, in druge relevantne OP.“
- „Ta spletna stran uporablja cookieje, da vam zagotovimo najboljšo uporabniško izkušnjo.“

OPT-IN princip, ne opt-out.



Enostaven umik privolitve

Upravljavec zagotoviti umik privolitve enako enostavno kot dajanje in to kadarkoli – v isti obliki: klik, preko spletne strani, aplikacije, log-on račun, e-mail, vmesnik pri IoT) + brez škode: „po možnosti“ (?) brezplačno ali brez zniževanja nivoja storitve.

Primer slabe prakse: Prodaja kart po internetu in dajanje privolitev tudi za uporabo OP v marketinške namene, umik pa le po telefonu v času uradnih ur.

Obvestiti o pravici do umika + kako uresničevati to pravico in to oboje pred dajanjem privolitve (člen 7(3))!

Če umik privolitve, upravljavec ne more le enostavno „zamenjati pravno podlago“, pač pa mora biti vsaka sprememba pravne podlage posamezniku sporočena po členu 13 in 14 ter generalno zahtevo po transparentnosti.



**(2., 4. odst. 9. čl.) – prepoved obdelave posebnih OP
ne velja, če:**

- a) posameznik izrecno privoli v obdelavo za določen namen, razen če pravo EU/DČ prepoveduje ta odstop
- b) P in D iz del. prava, soc. varnosti in soc. varstva (če to dovoljuje pravo EU ali DČ ali kolektivna pogodba)
- c) za zaščito življenjskih interesov, če fizično ali pravno ni sposoben dati privolitve
- d) **znotraj neprofitnih subjektov s političnim, filozofskim, verskim ali sindikalnim ciljem o svojih sedanjih ali bivših članih ali oseb v rednem stiku**
- e) posameznik OP sam objavi
- f) za pravne zahteve ali ko sodišča izvajajo sodno pristojnost
- g) bistveni javni interes po pravu EU ali DČ, sorazmerno s ciljem in spoštovanjem VOP ----- >>>>



h.) **potrebno za preventivno medicino ali medicino dela, oceno delovne sposobnosti, zdravstveno diagnozo**, zdravstveno ali socialno oskrbo, **zdravljenje, upravljanje sistemov in storitev zdravstvenega** ali socialnega varstva po pravu EU ali DČ, po pogodbi z zdravstvenim delavcem - le strokovnjaki z obveznostjo varovanja poklicne skrivnosti

i.) zaradi javnega interesa na področju **javnega zdravja** po pravu EU ali DČ (npr. zaščita pred epidemijami, zagotovitev visokega standarda zdravstvenega varstva, zdravil, medicinskih pripomočkov!)

j.) za **namene** arhiviranja v javnem interesu, znanstveno- ali zgodovinsko-raziskovalne ali statistične namene po pravu EU/DČ

Ključne novosti GDPR (1)

Veljavnost za vse upravljavce ne glede na sedež, če obdelujejo osebne podatke prebivalcev EU (nudenje blaga in storitev v EU, spremljanje vedenja v EU)

Bistveno strožje sankcije: do 20 000 000 EUR ali 4 % skupnega svetovnega letnega prometa v preteklem proračunskem letu, upošteva se višji znesek

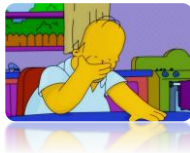
Imenovanje pooblaščenih oseb za varstvo podatkov: pri obdelavi obsežnejših osebnih podatkov, ki se jih redno in sistematično spremlja

Uradno obvestilo nadzornemu organu o kršitvi varstva osebnih podatkov (vdori, odtujitve): brez nepotrebnega odlašanja, max 72h



Dejavnosti, ki so lahko **redno in sistematično spremljanje**:

- upravljanje **telekomunikacijskega omrežja**,
- zagotavljanje **telekomunikacijskih storitev**,
- **dejavnosti trženja**, ki temeljijo na *(več kot le kontaktnih) OP*,
- **oblikovanje profilov** in točkovanje za namene ocene tveganja (npr. zaradi kreditnega točkovanja, določitve zavarovalnih premij, preprečevanja goljufij, odkrivanja pranja denarja),
- **sledenje** geografskemu položaju, npr. z mobilnimi napravami,
- **programi zvestobe**,
- oglaševanje na podlagi **vedenjskih vzorcev**,
- spremljanje podatkov o **počutju, telesni pripravljenosti in zdravju** prek nosljivih naprav („wearables“),
- **(obsežni) videonadzorni sistemi**, povezane naprave, **npr. pametni števc**i, pametni avtomobili, povezani sistemi za avtomatizacijo doma itd.



Pravice posameznika po ZVOP-1

Pravica do seznanitve z lastnimi osebnimi podatki!

Pravica do dopolnitve, popravka, blokiranja, izbrisa in ugovora od upravljalca zahtevati dopolnitev, popravek, blokiranje ali izpis, če posameznik dokaže, da so nepopolni, netočni ali neažurni ali da so bili zbrani ali obdelani v nasprotju z zakonom;

posameznik ima kadarkoli z ugovorom pravico zahtevati prenehanje njihove obdelave;

brezplačno za posameznika.

Rok: 15 dni.



Pravice posameznika (12. čl. in nasl.)

Upravljavec mora **zagotoviti posamezniku informacije o njegovih pravicah in sprejetih ukrepih** (glede potrditve obdelave, popravka, RTBF, omejitve obdelave, Data portability, ugovora, ugovora zoper avtomatizirano odločitev) v jedrnati, pregledni, razumljivi in lahko dostopni obliki + jasnem in preprostem **jeziku**, pisno ali v e-obliki. Na zahtevo posameznika lahko ustno, a le če se identiteta posameznika izkaže kako drugače.

Zahteve glede pravic uresničuje brez odlašanja v 1 mesecu.

+ dodatno **največ 2 meseca** ob upoštevanju kompleksnosti in števila zahtev, a ga mora v 1 mesecu obvestiti o podaljšanju in razlogih.

Če zahtevo predloži z **e-sredstvi**, **zagotovi** odgovor, če je mogoče, tudi z e-sredstvi. Možnosti vložitve **pritožbe pri IP** in **možnosti uveljavljanja pravnih sredstev**.



Vse informacije se zagotovijo **brezplačno!** (ne več zaračunavanja po Pravilniku o materialnih stroških!) -> vendar:

Če pa so **zahteve očitno neutemeljene ali pretirane** zlasti **ponavljajoče, lahko upravljavec (=šikanoznost):**

- a) **zaračuna razumno pristojbino**, pri čemer upošteva upravne stroške posredovanja informacij ali sporočila ali izvajanja zahtevanega ukrepa,
- b) **zavrne ukrepanje** v zvezi z zahtevo.

Upravljavec nosi dokazno breme!

Ključne novosti GDPR (2)

Pravica do pozabe: pravico doseči, da upravljavec brez nepotrebnega odlašanja izbriše osebne podatke v zvezi z njim

Pravica do prenosljivosti podatkov: od enega k drugemu ponudniku storitev

Privolitev: dokazljivo, prostovoljno, specifično, informirano in nedvoumno izrazil soglasje k obdelavi

Obveznost upravljavcev glede zagotavljanja preglednih in lahko dostopnih informacij posameznikom, na katere se nanašajo osebni podatki, o obdelavi njihovih podatkov.

Obdelava za zgodovinsko, statistično in znanstveno-raziskovalne namene

17.čl.ZVOP:

Ne glede na prvotni namen zbiranja se lahko osebni podatki nadalje obdelujejo za zgodovinske, statistične in znanstveno-raziskovalne namene.

Uporabniku se posredujejo v anonimizirani obliki.

Uporabnik mora ob zaključku obdelave uničiti te podatke in upravljalca brez odlašanja po njihovem uničenju pisno obvestiti, kdaj in na kakšen način jih je uničil.

Rezultati obdelave se objavijo v anonimizirani obliki.

Izjema: zakon, pisna privolitev



Ocena učinka v zvezi z varstvom podatkov *PIA* (35. čl)

1. Če je možno, da bi lahko obdelava, zlasti z novimi tehnologijami, ob upoštevanju narave/obsega/okoliščin/namenov obdelave povzročila veliko tveganje za TČP, upravljavec pred obdelavo opravi **PIA-o** predvidenih dejanj obdelave na VOP.
2. Upravljavec pri izvedbi ocene **za mnenje zaprosi DPO**.
3. Ocena učinka se zahteva zlasti v primeru:
 - a) **sistematičnega in obsežnega vrednotenja osebnih vidikov**, ki temelji na **avtomatizirani obdelavi**, vključno s **profiliranjem**, in je osnova za odločitve, ki imajo pravne učinke na posameznika ali nanj znatno vplivajo;
 - b) **obsežne obdelave posebnih vrst podatkov** ali OP v zvezi s KE/PE;
 - c) **obsežnega sistematičnega spremljanja javno dostopnega območja**. --→>



PIA zajema vsaj:

- a) sistematičen opis dejanj + namenov obdelave,
- b) oceno **potrebnosti** in **sorazmernosti** obdelave glede na namen,
- c) oceno tveganj za TČP,
- d) ukrepe za obravnavanje tveganj, zaščitne in varnostne ukrepe ter mehanizme za zagotavljanje VOP in za **dokazovanje skladnosti** s to uredbo, ob upoštevanju pravic in zakonitih interesov posameznikov ter drugih oseb, ki jih to zadeva.

(analiza tveganj na področju VOP)



Predhodno posvetovanje z IP (36. čl.)

Če iz ocene učinka izhaja, da bo obdelava OP veliko tveganje, se upravljavec predhodno posvetuje z IP.

Pri posvetovanju mora upravljavec IP **predložiti**:

- dolžnosti upravljavca, skupnih upravljavcev in obdelovalcev,
- namene in sredstva predvidene obdelave,
- ukrepe in zaščitne ukrepe za zaščito TČP posameznikov,
- kontaktne podatke pooblaščen osebe za VOP,
- oceno učinka v zvezi z varstvom podatkov,
- vsakršne druge informacije, ki jih zahteva IP.

Sta varnost in zasebnost lahko na istem imenovalcu?

„Kdor je pripravljen žrtvovati svojo svobodo zato, da si bo zagotovil delček varnosti, bo na koncu izgubil oboje.“

(Benjamin Franklin)

Presečišče interesov:

Zasebnost - posameznik želi, da se ga pusti pri miru.

Varnost – posameznik potrebuje občutek varnosti.

Nadzor - oblast želi učinkovito dosežati svoje cilje.

OP - osnovna “valuta” zasebnosti in nadzora.

Iskanje prave mere med različnimi interesi!

Ni vprašanje: **varnost v. zasebnost**, pač pa: **nadzor v. svoboda**
--→> problem ni varnost, ampak nadzor.

Napačno predočenje držav, zato napačna percepcija in sploh odločanje ljudi med dvema vrednotama = zloraba državljanov
→ ankete: 51% izbere varnost, 29% pa zasebnost.

„False dichotomy“ – sploh če se ljudi prej prestraši!

Zasebnost in varnost nista nasprotnika, nismo dolžni sprejeti manj ene za dosego več druge vrednote – gre tudi brez posegov v zasebnost. Varnost prizadene zasebnost le, ko/če temelji na identifikaciji - ta pristop terja omejitve (policija)!

Ni varnosti brez zasebnosti – svoboda pa terja obe! (B. Franklin)

Predvsem v boju proti terorizmu, države sprejemajo **vrsto „anti-privacy“ varnostnih ukrepov**, ki niso učinkoviti, kot se želi predstaviti (zbiranje OP brez pravne podlage, množičen nadzor, neobstoj pravne podlage za uporabo novih tehnologij: IMSI lovilci, droni, posegi v komunikacijsko zasebnost brez sodne odredbe, podatkovno rudarjenje,...) velikokrat pa celo škodijo varnosti.

Napačno dojemanje, da je *varnost „nujnost“*, zasebnost pa „bonus“ – resnica: **če se odpovemo zasebnosti, bomo vsekakor manj varni in manj svobodni – to prenesemo na državo!**

So v GB bolj varni, ker imajo 20x več videonadzornih kamer na prebivalca kot večina drugih EU-držav? Ne, celo več uličnega kriminala z uporabo orožja.

Posegi v zasebnost morajo biti sorazmerni in preiščeni – policija

lahko dobi nova pooblastila (=posege v zasebnost), če so ta:

- Nujna
- Učinkovita za dosego ustavno-dopustnega cilja
- Sorazmerna s posegi v TČP (tehtamo s posegom prizadete pravice v primerjavi s pravico, ki se jo želi zavarovati) --→ tehtanje: splošna varnost vseh prebivalcev in človekova pravico do zasebnosti.

Problemi: nesorazmernost pooblastil (zajeti nedolžni), ni PIA, ni javne in strokovne razprave, ni zadostnega družbenega konsenza.

Se cilj res ne da doseči z milejšimi posegi, ali je sorazmerno poseči v zasebnost vseh posameznikov – ki so se npr. znašli na AC (avtomatska prepoznavna tablic)?

Kako dosežemo win-win situacijo, torej varnost in zasebnost (in ne nadzor) ? - GDPR

Razvijati: **PIA** (Privacy Impact Assessment) naslovimo cilje in tveganja pred uvedbo vsakega posega v zasebnost (zlasti ob novem tehničnem sredstvu: DRON-i, IMSI lovilci....) +

RIA (Regulatory Impact Assessment) – analize učinkov predpisov na družbo: predhodne in že sprejetih predpisov

Razvoj in evalvacija novih varnostnih tehnologij:

a.) **SIA** = Surveillance Impact Assessment (impacts: privacy, legal, psychological, ethical, financial)

b.) **DESSI** = Decision Support System on security Investments (kaj je problem, učinkovite rešitve zanj, varnost + in -, družbena sprejemljivost, socialna implikacija, etični vidik, stroški, pravni vidik)

c.) **STEFI** = Security, Trust, Efficiency, Freedom infringement

Pravica do prenosljivosti OP - Data portability (20. čl.)

Posameznik ima pravico, da od upravljavca prejme svoje OP **v strukturirani, splošno uporabljani in strojno berljivi obliki**, in **pravico, da jih posreduje drugemu upravljavcu**, če:

- a) obdelava temelji na privolitvi (ali pogodbi) **IN**,
- b) se obdelava izvaja z avtomatiziranimi sredstvi.

Posameznik ima **pravico, da se OP neposredno prenesejo od enega upravljavca k drugemu, (le) kadar je to tehnično izvedljivo**.

Ta pravica velja le za zasebni sektor + le za avtomatizirano obdelavo!



Kaj je profiliranje? (4.čl. GDPR)

„Oblikovanje profilov“ = vsaka avtomatizirana obdelava OP, ki vključuje uporabo OP za ocenjevanje osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje: uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja posameznika.

Pomaga pri odločanju v bankah, zavarovalnicah, zdravstvu, davčnih postopkih, zavarovalništvu, v marketingu, pri oglaševanju

Avtomatizirano odločanje **povečuje učinkovitost**, varčevanje z resursi, povečuje prihranke, omogoča posamezniku prilagojeno-targetirano oglaševanje... odločajo algoritmi.

Pravilo VOP: „If you don't pay for the product, you are the product.“ – Ugodnosti vedno plačuješ, največkrat z OP.



Avtomatizirano odločanje – profiliranje, 22. čl.

Posameznik ima pravico, da zanj **ne velja** odločitev, ki temelji **zgolj (*solely*)** na avtomatizirani obdelavi, vključno z oblikovanjem profilov, ki ima zanj pravne učinke ali nanj znatno vpliva.

Dopustno pa je, če je odločitev (3 primeri):

- a) **nujna za sklenitev ali izvajanje pogodbe** posameznik - upravljavec;
- b) **dovoljena v pravu EU ali pravu DČ** upravljavca + določa ustrezne ukrepe za zaščito TČP in zakonitih interesov posameznika, ali
- c) **utemeljena z izrecno privolitvijo posameznika**

... + v primerih a.) in c.) mora upravljavec izvesti ustrezne ukrepe za zaščito TČP ter zakonitih interesov posameznika, **vsaj pravice do:**

- ***osebnega posredovanja** (**human intervention*) upravljavca,
- ***izražanja lastnega stališča,**
- ***izpodbijanja odločitve (=pravna sredstva).**

----->>>>



Avtomatizirane odločitve NE smejo temeljiti na

.... posebnih vrstah OP iz 1. odst. 9. člena:

- OP ki razkrivajo rasno ali etnični poreklo,
- politično mnenje
- versko ali filozofsko prepričanje
- članstvo v sindikatu
- genetski podatki
- biometrični podatki za namene identifikacije
- zdravstveni podatki
- spolno življenje in spolna usmerjenost,

.... **razen če** izrecna osebna privolitev (v 1 ali več namenov) + obenem tudi pravo EU/DČ ne prepoveduje dajanja soglasja (ker posameznik šibkejša stranka) ali je obdelava potreba zaradi bistvenega javnega interesa na podlagi prava EU/DČ + se obenem izvajajo ustrezni ukrepi za zaščito TČP in zakonitih interesov tega posameznika.



Kaj povedati posamezniku

.... če gre za avtomatsko odločanje, ki temelji **zgolj** na avtomatski obdelavi (torej tudi profiliranje), ki ustvarja pravne ali podobno pomembne učinke:

- 1.) Jasno in razumljivo povedati posamezniku, da je vključen v aktivnost profiliranja.
- 2.) Dati povedno informacijo o uporabljeni logiki odločanja.
- 3.) Razložiti pomen in posledice take obdelave.

Kaj pa razkritje algoritmov – „odločevalcev“? Recital št. 63 vseeno daje nekaj zaščite upravljavcem glede (ne)razkritja njihovih poslovnih skrivnosti.

„Posameznik ima pravico do seznanitve z: lastnimi OP, namenu obdelave, roku hrambe, uporabnikih OP, razlogih za avtomatsko obdelavo OP, o posledicah profiliranja. Te pravice pa ne smejo negativno vplivati na pravice drugih, vključno s poslovnimi skrivnostmi ali intelektualno lastnino, ter predvsem avtorske pravice, ki ščitijo programsko opremo, a obenem to za posameznika seveda ne sme pomeniti zavrnitev dostopa do vseh informacij.



ŠE NEKAJ MITOV IN NERESNIC O GDPR



1. mit: “NA ZAHTEVO POSAMEZNIKA BOMO SEDAJ MORALI IZBRISATI VSE NJEGOVE OP”

Člen 17

- **Ni** pravica do izbrisa zgodovine, do cenzure!
- **Umik podatkov oz. povezav do nepotrebnih, zastarelih, izrazito škodljivih podatkov o posamezniku**
 - npr. nepremišljene izjave/objave v mladosti
 - javne osebe
- **Tehtanje pravic!**
- **Druge pravne podlage!**
- **Številne izjeme:** svoboda izražanja in obveščanja, pravna obveznost, javni interes, arhiviranje v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene...





2. mit: „VEDNO BOM LAHKO DOBIL E-VERZIJO SVOJIH OP”

Člen 20

Posameznik ima pravico, da prejme OP, ki jih je posredoval upravljavcu, **v strukturirani, splošno uporabljani in strojno berljivi obliki**, in pravico, da te OP posreduje drugemu upravljavcu, ko:

- a) obdelava temelji **na privolitvi** (ali pogodbi),
 - b) se obdelava izvaja **z avtomatiziranimi sredstvi**.
- Posameznik ima **pravico**, da se OP neposredno prenesejo od enega upravljavca k drugemu, ***kadar je to tehnično izvedljivo***.
 - Uresničevanje pravice ne posega v druge pravice – dobiš **kopijo lastnih OP** in ne **podatkov drugih** (npr. intelektualno lastnino).
 - Ta pravica se **NE** uporablja za obdelavo, potrebno za opravljanje **naloge v javnem interesu** ali izvajanju **javne oblasti upravljavca**.



Bomo tako (počasi)
spoznali pravo
vrednost naših OP?



3. mit: „**PROFILIRANJE** **NE BO DOVOLJENO**“

Člen 22

Posameznik ima pravico, da zanj **ne velja odločitev**, ki temelji **zgolj na avtomatizirani obdelavi, vključno z oblikovanjem profilov**, ki ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva.

Avtomatizirano odločanje in profiliranje **bo dopustno, če** je odločitev:

- a) **nujna za sklenitev/izvajanje pogodbe** med posameznikom in upravljavcem;
- b) **dovoljena v pravu EU ali DČ + zaščitni ukrepi**, ali
- c) **utemeljena z izrecno privolitvijo posameznika**.

Pravica do :

- osebnega posredovanja upravljavca,
- do izražanja lastnega stališča in
- izpodbijanja odločitve.



Avtomatiziranih odločitev načeloma **NI na posebnih vrstah OP** (so možne izjeme)

- npr. da računalnik samostojno odloča o vaši diagnozi in zdravljenju.

(uspešna umetna inteligenca: AI-zdravniki, odvetniki)



4. mit: „VSI UPRAVLJAVCI BODO MORALI IMETI DPO“

Upravljavec in obdelovalec imenujeta DPO, kadar:

- a) **javni organ** ali telo, razen sodišč, kadar delujejo kot sodni organ;
- b) temeljne dejavnosti zajemajo dejanja **obdelave**, pri katerih je treba **zaradi njihove narave, obsega in/ali namenov posameznike redno in sistematično obsežno spremljati, ali**
- c) temeljne dejavnosti upravljavca ali obdelovalca zajemajo obsežno obdelavo posebnih vrst podatkov in OP v zvezi s KD in prekrški.



5. mit: „ZA VSE KRŠITVE BOMO DOBILI 20 MILIONSKO KAZEN“

Sankcije bodo učinkovite, sorazmerne in odvračilne.

Upravne globe do 10 mio EUR ali 2 % skupnega svetovnega letnega prometa oz. do 20 mio EUR ali 4% skupnega svetovnega letnega prometa - kateri znesek je višji.



Upoštevalo se bo **11 kriterijev**:

- a) narava, teža in trajanje kršitve, število posameznikov, raven škode, ki so jo utrpeli;
- b) ali je kršitev namerna ali posledica malomarnosti;
- c) vsi ukrepi, ki jih je sprejel upravljavec ali obdelovalec, da bi ublažil škodo, ki so jo utrpeli posamezniki;
- d) stopnja odgovornosti upravljavca/obdelovalca, pri čemer se upoštevajo tehnični in organizacijski ukrepi;
- e) vse zadevne predhodne kršitve upravljavca ali obdelovalca;
- f) stopnja sodelovanja z IP pri odpravljanju kršitve in blažitvi škodljivih učinkov kršitve;
- g) vrste OP, ki jih zadeva kršitev,
- h) kako je IP izvedel za kršitev, ali je bil uradno obveščen o kršitvi;
- i) če so bili ukrepi že prej odrejeni zoper upravljavca/obdelovalca z enako vsebino, skladnost s temi ukrepi;
- j) upoštevanje odobrenih kodeksov ravnanja ali odobrenih mehanizmov potrjevanja, in
- k) morebitni drugi oteževalni ali olajševalni dejavniki (npr. pridobljene finančne koristi).

Informacije javnega značaja



Pravna podlaga v Sloveniji

Zakon o dostopu do informacij javnega značaja (ZDIJZ),
osnovni zakon iz 2003, vrsta sprememb in dopolnitev,
trenutno neuradno prečiščeno besedilo št. 11



Informacije javnega značaja

Definicija:

informacija, ki izvira iz delovnega področja organa

se nahaja v obliki dokumenta (materializirana oblika)

organ z njo razpolaga

Zgolj veliko dela ni razlog za zavrnitev. Možna pa je zaradi zlorabe pravice (obsežne in pogoste zahteve).

V roku 20 delovnih dni od dneva prejema popolne zahteve. Organ je dolžan prosilca tudi opozoriti na plačilo stroškov.

Informacije javnega značaja: zgodovina

1766:

finski duhovnik (v takratni kraljevini Švedski) v Zakon o svobodi tiska in o dostopu do javnih dokumentov napiše, da mora biti uradni dokument dostopen vsakomur, ki ga zahteva, in to takoj ter brezplačno.

1966 ZDA

1949 na Švedskem in Danskem

1970 na Norveškem

2003 v Sloveniji

2005 v Veliki Britaniji

2006 v Nemčiji ...



Vir: Bakan Toplak, M. (2010). Seminar aktualna praksa s področja informacij javnega značaja, *Organizacija znanja* 15(1-2). Najdeno na http://home.izum.si/cobiss/oz/2010_1-2/html/clanek_16.html

Informacije javnega značaja: zavezanci

državni organi, organi lokalnih skupnosti, javne agencije, javni skladi in druge osebe javnega prava, nosilci javnih pooblastil in izvajalci javnih služb

gospodarske družbe in druge pravne osebe zasebnega prava pod neposrednim ali posrednim prevladujočim vplivom, posamično ali skupaj, Republike Slovenije, samoupravnih lokalnih skupnosti in drugih oseb javnega prava

Informacije javnega značaja: izjeme (6.čl.)

Tajni podatki (ZTP)

Poslovna skrivnost (ZGD)

Osebni podatki (ZVOP)

Podatki državne statistike (ZDS)

Davčna tajnost (absolutna izjema)

Podatki o naravni/kulturni vrednoti

Kazenski, upravni, sodni postopki pred zaključkom; podatki o
notranjem delovanju organa; dokumenti v postopku izdelave
⇒ škodni test

Statistična zaščita podatkov



Osnovni pojmi

Zaupnost (*angl. confidentiality*)

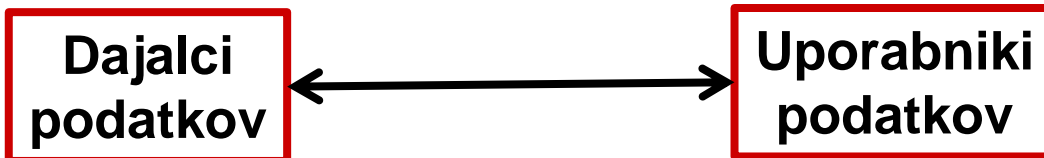
Zaupnost je status podatkov, za katerega sta se dogovorila oseba/organizacija, ki je podatke priskrbela, in organizacijo, ki je te podatke dobila, opisuje pa stopnjo nudene zaščite. (Dalenius, 1988)

Zasebnost (*angl. privacy*)

Pravica odločati, katere informacije o sebi bomo delili z drugimi. (Fellegi, 1972)

Razkritje (*angl. disclosure*)

Ko oseba/organizacija iz objavljenih podatkov izve o drugi osebi/organizaciji nekaj novega, česar brez teh podatkov ne bi vedela.



Statistična zaščita podatkov

Statistična zaščita podatkov

(*angl.* statistical disclosure control/limitation)

⇒ Uporaba metod za znižanje tveganja razkritja.

Področja uporabe:

Uradna statistika (zaupanje respondentov)

Zdravstveni podatki

Elektronsko poslovanje

...

Vrste rezultatov, ki naj se jih ščiti:

(Statične) statistične tabele

Dinamične poizvedbe po bazah

Mikropodatki (*Netflix!*)

Tipologija podatkov glede na stopnjo razkritja

Mikro podatki

- neanonimizirani mikro podatki (data enclaves),
- anonimizirani mikro podatki,
- statistično zaščiteni mikro podatki,
- public use microdata/files

Agregirani podatki

- v tabelah/bazah
- v grafičnih prikazih

Vrste spremenljivk glede na vlogo v statistični zaščiti podatkov

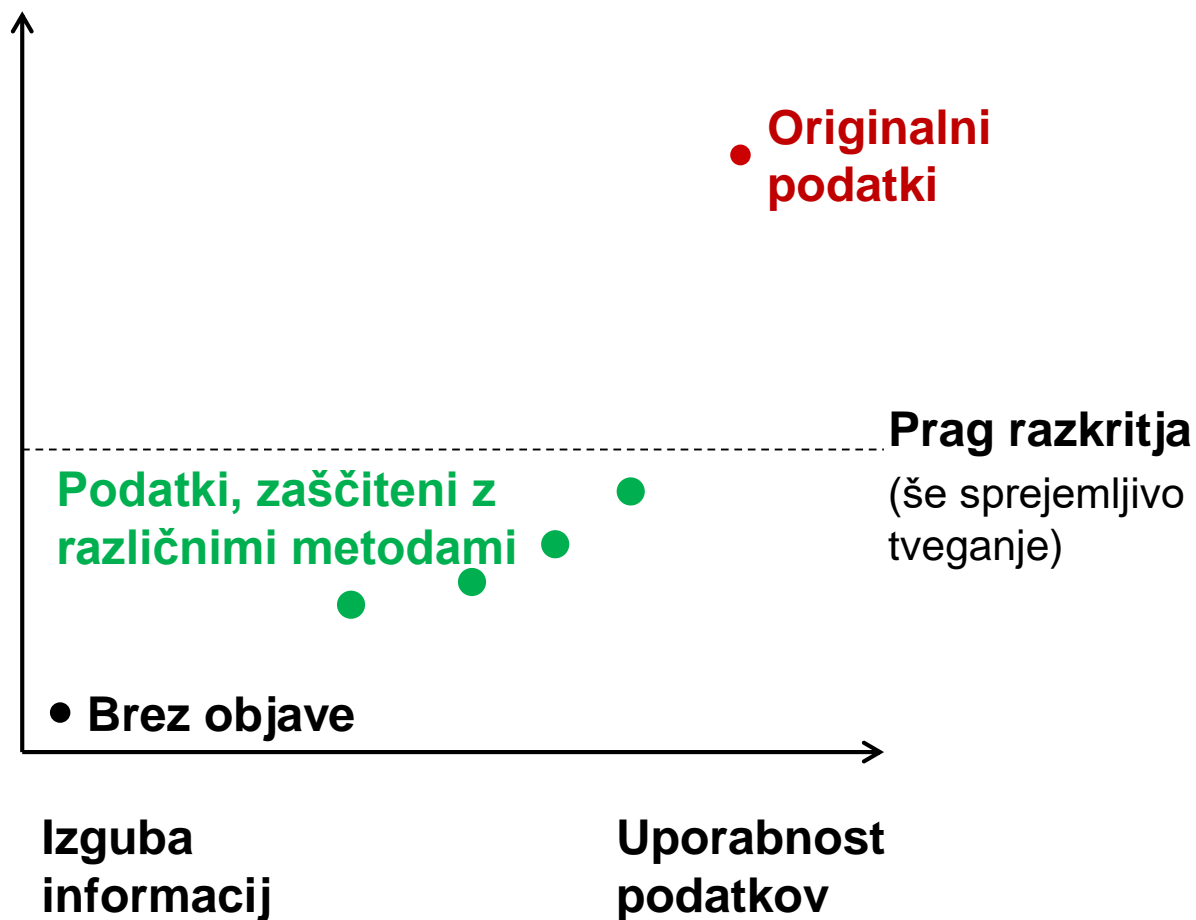
- Identifikatorji
 - spremenljivke, ki natančno določijo enoto
 - npr. EMŠO, davčna številka, matična številka podjetja
 - večinoma kategorialne spremenljivke (nominalke)
- Kvazi identifikatorji ali ključne spremenljivke
 - spremenljivke, ki pri določitvi enote dopuščajo dvom, a njihovo povezovanje lahko določi enoto
 - npr. ime, naslov, spol, starost, telefonska številka
- Zaupne spremenljivke
 - spremenljivke z občutljivo vsebino
 - nacionalnost, dohodek, zdravstveno stanje, veroizpoved
- Neobčutljive spremenljivke



Kompromisi

Tveganje
razkritja

- enostavnost sklepa
- posledice (ne)točnosti sklepa za “vohljača”
- posledice teh sklepov za organizacijo/ponudnika podatkov



Metode statistične zaščite

- Metode so lahko namenjene:
 - mikropodatkom / tabelam / obojemu
 - kategorialnim spr. / zveznim spr./ obojim
- Glede na pristop ločimo:
 - deterministične metode
 - verjetnostne metode
- Glede na rezultat ločimo:
 - metode, ki ustvarijo sintetične podatke, tako da ohranijo določene statistične značilnosti originalnih podatkov
 - metode, ki zakrivajo originalne podatke:
 - zakrivanje z vnosom motenj (*angl.* perturbative masking)
 - zakrivanje brez vnosa motenj (*angl.* non-perturbative masking; podatkov ne spreminjajo, ampak jih izpuščajo, prekodirajo, agregirajo, vzorčijo ipd.)

Mikropodatki: zakrivanje z vnosom motenj

Metoda	Zvezne spremenljivke	Kategorialne spremenljivke	
Dodajanje šuma	X		⇒
Zaokroževanje	X		
Ponovno vzorčenje	X		
Mikroagregacija	X	(X)	⇒
Menjava rangov/podatkov	X	X	⇒
PRAM		X	⇒

Dodajanje šuma

cilj: zaščita pred povezovanjem z zunanjimi podatki z
dodajanjem stohastičnega šuma
različne metode dodajanja šuma (več šuma na osamelce,
ohranjanje povprečij, ohranjanje korelacij)

Mikroagregacija

cilj: vse enote porazdeliti po skupinah in znotraj vsake skupine posamične vrednosti spremenljivke nadomestiti z aritmetično sredino ali kako drugo vrednostjo

upoštevanje načela k-anonymity, minimalnega števila enot v skupini, ki še zagotavlja anonimnost (običajno $k=3$)

Menjava rangov/podatkov

osnovna ideja: zamenjati vrednosti neke spremenljivke na delu enot

postopek pri upoštevanju rangov: razvrstitev po velikosti določene spremenljivke, zamenjava podatkov znotraj določenega intervala, ponovitev postopka na naslednji spremenljivki. Tak pristop se je izkazal kot dober kompromis

Post-randomizacija

(*angl.* Post Randomization Method, PRAM)

namerna napačna klasifikacija

cilj: spremeniti del vrednosti kategorialne spremenljivke na osnovi vnaprej določenih verjetnosti prehoda iz ene v drugo kategorijo

Mikropodatki: zakrivanje brez vnosa motenj

Metoda	Zvezne spremenljivke	Kategorialne spremenljivke	
Prekodiranje	X	X	⇒
Vzorčenje		X	
Delno izpuščanje		X	⇒

Prekodiranje (*angl.* recoding):

cilj: zmanjšati število možnih vrednosti spremenljivke;

slabost: čeprav je problem navadno v specifični kombinaciji (npr. redek poklic+manjši kraj), se prekodiranje izvede na vseh podatkih (zato imenovano tudi globalno prekodiranje)

kategorialne spremenljivke: združevanje več kategorij v eno, manj informativno

zvezne spremenljivke: iz zveznih v diskretne vrednosti (manj običajno)

prekodiranje najnižjih/najvišjih vrednosti (*angl.* bottom/top coding): združevanje vrednosti pod/nad pragom

Delno izpuščanje (*angl.* local suppression)

cilj: izpustiti določene vrednosti iz spremenljivke, ki bi omogočila razkritje

običajno se je potrebno odločiti, katera v kombinaciji vrednosti kategorialnih spremenljivk naj bo manjkajoča (npr. kraj ali poklic)

Tveganje razkritja v tabelah

Frekvenčne tabele

Vrednostne tabele (*angl.* magnitude tables) \Rightarrow vsote

Povezane tabele



Primer problematične frekvenčne tabele

Zakonski stan	Polni delovni čas	Krajši delovni čas	Skupaj
Poročen	6	0	6
Razvezan	5	1	6
Samski	2	2	4
Skupaj	13	3	16

Hundepool, A. et al. (2010). *Handbook on Statistical Disclosure Control. Version 1.2.*
ESSNet SDC. Najdeno na http://neon.vb.cbs.nl/casc/SDC_Handbook.pdf

Katera polja so problematična?

Določanje občutljivosti polj v tabeli

Pravila	Polje v tabeli je občutljivo, ko...
Pravilo najmanjše frekvence	je frekvenca manjša od vnaprej definiranega minimuma n (običajno $n=3$)
(n, k) - pravilo dominantnosti	je vsota n največjih vrednosti večja od $k\%$ vsote v polju
Pravilo $p\%$	je vsota v polju minus dve največji vrednosti manjša od $p\%$ največje vrednosti

Hundepool, A. et al. (2010). *Handbook on Statistical Disclosure Control. Version 1.2.*
ESSNet SDC. Najdeno na http://neon.vb.cbs.nl/casc/SDC_Handbook.pdf

Metode za zaščito tabel

- Predhodna zaščita mikropodatkov
- Preoblikovanje tabele
 - Združevanje kategorij, uporaba višje hierarhične ravni
 - Uporaba praga, najmanjše frekvence
- Spremembe po pripravi tabele
 - Uporaba manjkajočih vrednosti
 - Primarna
 - Sekundarna
 - Zaokrožitev vrednosti po vseh poljih
 - Motnja polja, npr. 'barnardisation', ki vsako polje z neničelno vrednostjo spremeni za +1, 0 ali -1 v skladu z verjetnostjo
- *Paziti na povezane tabele, nerazkrivanje pravil za zaščito, število dimenzij v tabeli*

Primer objavljenih pravil

EHIS Wave 1 variables: ANONYMISATION RULES

[Povezava na primer](#)

http://ec.europa.eu/eurostat/documents/203647/203710/EHIS_wave_1_anonymisation_rules.pdf



Uporaba manjkajočih vrednosti

Primarna

	Regija				
	A	B	C	D	Skupaj
Squash	58	47	36	89	230
Fitness	71	124	24	31	250
Odbojka	92	157	59	28	454
Ostalo	800	934	651	742	3127
Skupaj	1021	1262	770	890	4061

Sekundarna

	Regija				
	A	B	C	D	Skupaj
Squash	58	X	36	89	230
Fitness	71	124	24	31	250
Odbojka	92	157	59	X	454
Ostalo	800	934	651	742	3127
Skupaj	1021	1262	770	890	4061

	Regija				
	A	B	C	D	Skupaj
Squash					
Fitness					
Odbojka					
Ostalo					
Skupaj					4061