844/14/SL
WP 217

Mnenje št. 6/2014 o pojmu zakonitih interesov upravljavca podatkov iz člena 7 Direktive 95/46/ES

Sprejeto 9. aprila 2014

Kazalo

Povzetek

To mnenje vsebuje analizo meril za zakonitost obdelave podatkov, ki so določena v členu 7 Direktive 95/46/ES. Osredotoča se na zakonite interese upravljavca ter vsebuje smernice za uporabo člena 7(f) v sedanjem pravnem okviru in priporočila za prihodnje izboljšave.

Člen 7(f) je zadnja od šestih podlag za zakonito obdelavo osebnih podatkov. Zahteva namreč tehtanje zakonitih interesov, za katere si prizadeva upravljavec ali katera koli tretja oseba, ki so ji osebni podatki posredovani, ter interesov ali temeljnih pravic posameznika, na katerega se osebni podatki nanašajo. Rezultat tega testa tehtanja bo pokazal, ali je člen 7(f) mogoče uporabiti kot pravno podlago za obdelavo.

Delovna skupina iz člena 29 priznava pomen in uporabnost merila iz člena 7(f), ki lahko v pravih okoliščinah in ob ustreznih zaščitnih ukrepih pomaga preprečevati pretirano opiranje na druge pravne podlage. Člen 7(f) se ne bi smel obravnavati kot „zadnja možnost“ v redkih ali nepričakovanih okoliščinah, v katerih se šteje, da se druge podlage za zakonito obdelavo ne uporabljajo. Vendar ne bi smel biti izbran samodejno oziroma se njegova uporaba ne bi smela preveč razširiti zaradi mnenja, da je manj omejevalen kot druge podlage.

Prava ocena iz člena 7(f) ni preprost test tehtanja, ki zajema le tehtanje dveh zlahka opredeljivih in primerljivih „uteži“. Nasprotno, test zahteva popolno upoštevanje številnih dejavnikov, da se zagotovi ustrezno upoštevanje interesov in temeljnih pravic posameznikov, na katere se osebni podatki nanašajo. Hkrati se lahko stopnjuje, kar pomeni, da lahko sega od preprostega do vsestranskega ter da ni treba, da je pretirano težaven. Pri izvajanju testa tehtanja je treba upoštevati te dejavnike:

– naravo in vir zakonitega interesa ter ali je obdelava podatkov potrebna za uveljavljanje temeljne pravice, ali je sicer v javnem interesu in ali jo zadevna skupnost priznava;

– učinek na posameznike, na katere se osebni podatki nanašajo, in njihova razumna pričakovanja, kaj se bo zgodilo z njihovimi podatki, ter naravo podatkov in način njihove obdelave;

– dodatne zaščitne ukrepe, ki lahko omejijo pretiran učinek na posameznika, na katerega se osebni podatki nanašajo, kot so zmanjšanje količine podatkov, tehnologije za boljše varovanje zasebnosti, večja preglednost, splošna in brezpogojna pravica do zavrnitve ter prenosljivost podatkov.

Delovna skupina iz člena 29 za naprej priporoča, naj se v predlagano uredbo vstavi uvodna izjava o ključnih dejavnikih, ki se upoštevajo pri izvajanju testa tehtanja. Priporoča še, naj se doda uvodna izjava, s katero se bo od upravljavca zahtevalo, da, kadar je primerno, dokumentira svojo oceno zaradi večje odgovornosti. Nazadnje, delovna skupina iz člena 29 podpira tudi vsebinsko določbo, da morajo upravljavci posameznikom, na katere se osebni podatki nanašajo, pojasniti, zakaj menijo, da njihovi interesi ne bodo podrejeni interesom, temeljnim pravicam in svoboščinam teh posameznikov.

DELOVNA SKUPINA ZA VARSTVO POSAMEZNIKOV PRI OBDELAVI OSEBNIH PODATKOV,

ustanovljena z Direktivo Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995, JE –

ob upoštevanju člena 29 ter člena 30(1)(a) in (3) navedene direktive,

ob upoštevanju svojega poslovnika –

SPREJELA NASLEDNJE MNENJE:

I. Uvod

To mnenje vsebuje analizo meril za zakonitost obdelave podatkov, ki so določena v členu 7 Direktive 95/46/ES[1] (v nadaljnjem besedilu: Direktiva). Osredotoča se predvsem na zakonite interese upravljavca iz člena 7(f).

Merila iz člena 7 se nanašajo na širše načelo „zakonitosti“, določeno v členu 6(1)(a), po katerem morajo biti osebni podatki obdelani „pošteno in zakonito“.

Člen 7 določa, da se osebni podatki obdelujejo le, če se uporablja vsaj ena izmed šestih pravnih podlag, naštetih v tem členu. Osebni podatki obdelujejo le (a) na podlagi nedvoumne privolitve posameznika, na katerega se osebni podatki nanašajo,[2] ali če je obdelava – na kratko[3] – potrebna za:

(b) izvajanje pogodbe, katere stranka je posameznik, na katerega se nanašajo osebni podatki;
(c) skladnost z zakonsko obveznostjo, ki velja za upravljavca;
(d) varstvo življenjskih interesov posameznikov, na katere se osebni podatki nanašajo;
(e) izvajanje naloge, ki se opravlja v javnem interesu, ali
(f) zakonite interese, za katere si prizadeva upravljavec, ki so predmet dodatnega testa tehtanja s pravicami in interesi posameznika, na katerega se osebni podatki nanašajo.

V skladu z zadnjo pravno podlago „je obdelava potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja stranka ali stranke, ki so jim osebni podatki posredovani, razen kadar nad takimi interesi prevladajo temeljne pravice in[4] svoboščine posameznika, na katerega se osebni podatki nanašajo, ki se varujejo na podlagi člena 1(1)“. Z drugimi besedami, člen 7(f) dovoljuje obdelavo, ki je predmet tehtanja, pri katerem se tehtajo zakoniti interesi, za katere si prizadeva upravljavec – ali tretja oseba ali osebe, ki so jim osebni podatki

[1] Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, str. 31).
[2] Glej Mnenje št. 15/2011 o opredelitvi privolitve, ki ga je delovna skupina iz člena 29 sprejela 13. julija 2011 (WP 187).
[3] Te določbe bodo podrobneje obravnavane v nadaljevanju.
[4] Kot je pojasnjeno v oddelku III.3.2, angleška različica Direktive vsebuje tipkarsko napako: pisati bi moralo „interesi ali temeljne pravice“ („interests or fundamental rights“) namesto „interesi za temeljne pravice“ („interests for fundamental rights“).

posredovani –, in interesi ali temeljne pravice posameznikov, na katere se osebni podatki nanašajo.[5]

Potreba po doslednejšem in bolj usklajenem pristopu v Evropi

Študije, ki jih je Komisija opravila v okviru pregleda Direktive[6], ter sodelovanje in izmenjava mnenj med nacionalnimi organi za varstvo podatkov so pokazali pomanjkljivo usklajenost razlage člena 7(f) Direktive, zaradi česar ga države članice uporabljajo različno. Čeprav se izvajanje pravega testa tehtanja zahteva v več državah članicah, se člen 7(f) včasih napačno obravnava kot „odprta vrata“ za upravičenje vsake obdelave podatkov, ki je ne pokriva ena od drugih pravnih podlag.

Nedosledni pristop lahko povzroči pomanjkanje pravne gotovosti in predvidljivosti, oslabi položaj posameznikov, na katere se osebni podatki nanašajo, in naloži nepotrebna regulativna bremena za podjetja in druge organizacije, ki poslujejo čezmejno. Take nedoslednosti so že privedle do postopka pred Sodiščem Evropske unije (v nadaljnjem besedilu: Sodišče EU).[7]

Zato je še zlasti pravi čas, da zdaj, ko se delo za novo splošno uredbo o varstvu podatkov nadaljuje, jasneje razumemo šesto podlago za obdelavo (ki se nanaša na „zakonite interese“) in njeno razmerje z drugimi podlagami za obdelavo. Zlasti dejstvo, da gre za temeljne pravice posameznikov, na katere se osebni podatki nanašajo, zahteva, da se pri uporabi vseh šestih podlag – ustrezno in enako – upošteva spoštovanje teh pravic. Člen 7(f) ne sme postati preprost način za izogibanje upoštevanju zakonodaje o varstvu podatkov.

Zato se je delovna skupina za varstvo podatkov iz člena 29 (v nadaljnjem besedilu: delovna skupina) v okviru delovnega programa za obdobje 2012–2013 odločila skrbno pregledati to vprašanje in se zavezala, da pripravi to mnenje zaradi izvajanja delovnega programa.[8]

Izvajanje veljavnega pravnega okvira in priprave na prihodnost

V delovnem programu sta jasno določena dva cilja: „zagotavljanje pravilnega izvajanja veljavnega pravnega okvira“ in „priprave na prihodnost“.

Skladno s tem je prvi cilj tega mnenja zagotoviti splošno razumevanje obstoječega pravnega okvira. Ta cilj sledi starejšim mnenjem o drugih ključnih določbah Direktive.[9] V nadaljevanju

[5] Sklicevanje na člen 1(1) se ne sme razlagati tako, da omejuje obseg interesov ter temeljnih pravic in svoboščin posameznika, na katerega se osebni podatki nanašajo. Nasprotno, namen tega sklicevanja je poudariti splošen cilj zakonodaje o varstvu podatkov in same direktive. Člen 1(1) se namreč ne sklicuje le na varstvo zasebnosti, ampak tudi na varstvo vseh drugih „pravic in svoboščin fizičnih oseb“, saj je zasebnost le ena od njih.

[6] Evropska komisija je 25. januarja 2012 sprejela sveženj za reformo evropskega okvira varstva podatkov. Sveženj zajema (i) Sporočilo (COM(2012) 9 final), (ii) predlog splošne uredbe o varstvu podatkov (v nadaljnjem besedilu: predlagana uredba) (COM(2012) 11 final) in (iii) predlog direktive o varstvu podatkov na področju kazenskega pregona (COM(2012) 10 final). Spremljajoča ocena učinka, ki vsebuje 10 prilog, je v delovnem dokumentu Komisije (SEC(2012) 72 final). Glej zlasti študijo z naslovom „Ocena izvajanja direktive o varstvu podatkov“ v Prilogi 2 k Oceni učinka, priloženi svežnju Evropske komisije za reformo varstva podatkov.

[7] Glej na strani 7 v poglavju II.1 Kratka zgodovina podpoglavje z naslovom *Izvajanje Direktive; sodba ASNEF in FECEMD*.

[8] Glej Delovni program 2012–2013 delovne skupine za varstvo podatkov iz člena 29, sprejet 1. februarja 2012 (WP 190).

[9] Kot so Mnenje št. 3/2013 o omejitvi namena, sprejeto 3. aprila 2013 (WP 203), Mnenje št. 15/2011 o opredelitvi privolitve (navedeno v opombi 2), Mnenje 8/2010 o pravu, ki se uporablja, sprejeto

bodo na podlagi analize predstavljena tudi priporočila glede politike, ki jih je treba upoštevati pri pregledu pravnega okvira varstva podatkov.

Struktura tega mnenja

Po kratkem pregledu zgodovine in vloge zakonitih interesov in drugih podlag za obdelavo v poglavju II, bodo v poglavju III preučene in razložene pomembne določbe Direktive ob upoštevanju splošnega temelja pri njihovi uporabi v nacionalni zakonodaji. Analiza za ponazoritev vsebuje praktične primere na podlagi nacionalnih izkušenj. Analiza podpira priporočila v poglavju IV tako glede uporabe veljavnega regulativnega okvira kot v okviru pregleda Direktive.

II. Splošne ugotovitve in izzivi politike

II.1 Kratka zgodovina

Ta pregled se osredotoča na to, kako sta se razvila koncepta zakonitosti in pravnih podlag za obdelavo, skupaj z zakonitimi interesi. V njem je predvsem pojasnjeno, kako se je potreba po pravni podlagi prvič uporabila kot zahteva v okviru odstopanj od pravice do zasebnosti in se posledično razvila v ločeno zahtevo na področju varstva podatkov.

Evropska konvencija o človekovih pravicah (EKČP)

Člen 8 Evropske konvencije o človekovih pravicah, sprejete leta 1950, določa pravico do zasebnosti, to je pravico vsakogar do spoštovanja njegovega zasebnega in družinskega življenja, doma in dopisovanja. Prepoveduje vsakršno poseganje v pravico do zasebnosti, razen če je to „določeno z zakonom“ in „nujno v demokratični družbi“ zaradi nekaterih vrst posebej naštetih nujnih javnih interesov.

Člen 8 EKČP se osredotoča na varstvo zasebnega življenja in zahteva utemeljitev za vsako poseganje v zasebnost. Ta pristop temelji na splošni prepovedi poseganja v pravico do zasebnosti in dovoljuje izjeme le pod strogo opredeljenimi pogoji. V primerih „poseganja v zasebnost“ se zahtevata pravna podlaga in navedba zakonitega namena kot pogoja za presojo potrebe po takem poseganju. Ta pristop kaže, da EKČP ne vsebuje seznama možnih pravnih podlag, ampak le poudarja potrebo po pravni podlagi in pogoje, ki jih mora ta pravna podlaga izpolnjevati.

Konvencija 108

S Konvencijo 108 Sveta Evrope[10], ki je na voljo za podpis od leta 1981, je bilo varstvo osebnih podatkov uvedeno kot ločen koncept. Takratna temeljna ideja ni bila, da je treba obdelavo osebnih podatkov vedno šteti za „*poseganje* v zasebnost“, ampak bolj, da mora obdelava osebnih podatkov zaradi *varstva* temeljnih pravic in svoboščin vsakogar, zlasti pravice do zasebnosti, izpolnjevati nekatere pogoje. Člen 5 tako določa temeljna načela zakonodaje o varstvu podatkov, vključno z zahtevo, da morajo biti „[o]sebni podatki, ki se

16. decembra 2010 (WP 179), in Mnenje 1/2010 o pojmih „upravljavec“ in „obdelovalec“, sprejeto 16. februarja 2010 (WP 169).

[10] Konvencija 108 o varstvu posameznika glede na avtomatsko obdelavo osebnih podatkov.

avtomatsko obdelujejo: (a) […] pridobljeni in obdelani pošteno in zakonito“. Vendar Konvencija ne določa podrobnih podlag za obravnavo.[11]

Smernice OECD[12]

Smernice OECD, pripravljene vzporedno s Konvencijo 108 in sprejete leta 1980, vsebujejo podobne ideje o „zakonitosti“, čeprav je koncept izražen drugače. Posodobljene so bile leta 2013, ne da bi se načelo zakonitosti pomembno spremenilo. Člen 7 Smernic OECD zlasti določa, da morajo „obstajati omejitve za zbiranje osebnih podatkov in vse take podatke je treba pridobiti zakonito in pošteno ter po potrebi z vednostjo ali privolitvijo posameznika, na katerega se osebni podatki nanašajo“. Tu je pravna podlaga, ki se nanaša na privolitev, izrecno omenjena kot možnost, ki se uporablja „po potrebi“. To bo zahtevalo presojo zadevnih interesov in pravic ter tega, kako intruziven je postopek. V tem smislu ima pristop OECD nekatere podobnosti s precej bolj razvitimi merili, določenimi v Direktivi 95/46/ES.

Direktiva 95/46/ES

Direktiva je ob sprejetju leta 1995 temeljila na zgodnjih instrumentih varstva podatkov, skupaj s Konvencijo 108 in Smernicami OECD. Upoštevale so se tudi zgodnje izkušnje z varstvom podatkov v nekaterih državah članicah.

Poleg širše zahteve, določene v njenem členu 6(1)(a), da je treba osebne podatke obdelovati „pošteno in zakonito“, so bile v Direktivi dodane še posebne zahteve, ki kot take še niso bile navedene v Konvenciji 108 in Smernicah OECD: obdelava osebnih podatkov mora temeljiti na eni od šestih pravnih podlag iz člena 7.

Izvajanje Direktive; sodba ASNEF in FECEMD[13]

Komisija v poročilu z naslovom Ocena izvajanja direktive o varstvu podatkov[14] poudarja, da je bilo izvajanje določb Direktive v nacionalni zakonodaji včasih nezadovoljivo. Komisija v tehnični analizi prenosa Direktive v državah članicah[15] navaja dodatne podrobnosti o izvajanju člena 7. Pojasnjuje, da čeprav je šest pravnih podlag v zakonodaji večine držav članic določenih razmeroma podobno kot v Direktivi, je prožnost teh načel v resnici privedla do različne uporabe.

Glede na te okoliščine je posebej pomembno, da je Sodišče v sodbi z dne 24. novembra 2011 v združenih zadevah ASNEF in FECEMD odločilo, da Španija ni pravilno prenesla člena 7(f) Direktive, ker je zahtevala, da morajo biti upoštevni podatki – kadar ni privolitve posameznika, na katerega se osebni podatki nanašajo – navedeni v javno dostopnih virih. Razsodilo je tudi, da ima člen 7(f) neposredni učinek. S to sodbo se omejuje diskrecijska

[11] V osnutku posodobljene konvencije, ki je bil novembra 2012 sprejet na plenarnem zasedanju T-PD, je navedeno, da se podatki lahko obdelujejo na podlagi privolitve posameznika, na katerega se osebni podatki nanašajo, ali na „drugi legitimni podlagi, določeni z zakonom“, podobno kot v Listini Evropske unije o temeljnih pravicah, omenjeni na strani 8.

[12] Smernice OECD o varstvu zasebnosti in čezmejnem prenosu osebnih podatkov, 11. julij 2013.

[13] Sodba Sodišča z dne 24. novembra 2011 v združenih zadevah C-468/10 in C-469/10, *ASNEF in FECEMD*.

[14] Glej Prilogo 2 k Oceni učinka, priloženi svežnju Evropske komisije za reformo varstva podatkov, navedenemu v opombi 6.

[15] Analiza in ocena učinka izvajanja Direktive 95/46/ES v državah članicah. Glej http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf.

pravica držav članic pri izvajanju člena 7(f). Predvsem ne smejo preseči ozke ločnice med natančnejšim pojasnilom na eni strani in določitvijo dodatnih zahtev, s katerimi bi se spremenilo področje uporabe člena 7(f), na drugi strani.

Sodba, s katero se jasno določa, da države članice v svoji zakonodaji ne smejo določiti dodatnih enostranskih omejitev in zahtev v zvezi s pravnimi podlagami za zakonito obdelavo podatkov, ima pomembne posledice. Nacionalna sodišča in drugi ustrezni organi morajo nacionalne določbe razlagati z vidika te sodbe in po potrebi razveljaviti vsa sporna nacionalna pravila in opustiti tovrstne prakse.

Glede na to sodbo je še toliko bolj pomembno, da nacionalni organi za varstvo podatkov in/ali evropski zakonodajalci dosežejo jasen in splošen dogovor glede uporabe člena 7(f). To je treba doseči na uravnotežen način brez neupravičenega omejevanja ali neupravičenega širjenja področja uporabe te določbe.

Listina o temeljnih pravicah

Listina Evropske unije o temeljnih pravicah (v nadaljnjem besedilu: Listina) ima od začetka veljavnosti Lizbonske pogodbe 1. decembra 2009 „enako pravno veljavnost kot Pogodbi“.[16] Listina v členu 8 kot temeljno pravico določa varstvo osebnih podatkov, ki je ločeno od spoštovanja zasebnega in družinskega življenja, določenega v členu 7. S členom 8 se zahteva legitimna podlaga za obdelavo. Predvsem pa je določeno, da se morajo osebni podatki obdelovati „na podlagi privolitve prizadete osebe ali na drugi legitimni podlagi, določeni z zakonom“.[17] Te določbe krepijo pomen načela zakonitosti in potrebe po ustrezni pravni podlagi za obdelavo osebnih podatkov.

Predlagana uredba o varstvu podatkov

V okviru postopka pregleda varstva podatkov se zdaj obravnava področje uporabe podlag za zakonitost iz člena 7 in zlasti področje uporabe člena 7(f).

Člen 6 predlagane uredbe vsebuje seznam podlag za zakonito obdelavo osebnih podatkov. Šest razpoložljivih podlag – z nekaj izjemami (kot bo opisano v nadaljevanju) – se ne razlikuje pomembno od podlag, ki so zdaj določene v členu 7 Direktive. Vendar je Komisija predlagala, da se določijo dodatna navodila v obliki delegiranih aktov.

Zanimivo je, da se je v okviru dela ustreznega odbora Evropskega parlamenta[18] poskušalo koncept zakonitih interesov pojasniti v sami predlagani uredbi. Pripravljena sta bila seznam primerov, v katerih bi zakoniti interesi upravljavca podatkov praviloma prevladali nad zakonitimi interesi ter temeljnimi pravicami in svoboščinami posameznika, na katerega se osebni podatki nanašajo, in seznam primerov, v katerih bi bilo ravno obratno. Ta seznama –

[16] Glej člen 6(1) PEU.
[17] Glej člen 8(2) Listine.
[18] Osnutek poročila Odbora za državljanske svoboščine, pravosodje in notranje zadeve (LIBE) o predlogu uredbe Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Splošna uredba o varstvu podatkov) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) z dne 16. januarja 2013 (v nadaljnjem besedilu: osnutek poročila odbora LIBE). Glej zlasti predloga sprememb 101 in 102. Glej tudi predloge sprememb, ki jih je odbor sprejel 21. oktobra 2013 v končnem poročilu (v nadaljnjem besedilu: končno poročilo odbora LIBE).

določena bodisi v določbah bodisi v uvodnih izjavah – sta pomemben prispevek k oceni ravnovesja med pravicami in interesi upravljavca in posameznika, na katerega se osebni podatki nanašajo, in se upoštevata v tem mnenju.[19]

II.2 Naloga koncepta

Zakoniti interesi upravljavca: test tehtanja kot zadnja možnost?

Člen 7(f) je naveden kot zadnja možnost med šestimi podlagami, ki dovoljujejo zakonito obdelavo osebnih podatkov. Zahteva test tehtanja: to, kaj je potrebno z vidika zakonitih interesov upravljavca (ali tretjih oseb), se mora tehtati glede na interese ali temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo. Rezultat testa tehtanja bo pokazal, ali je člen 7(f) mogoče uporabiti kot pravno podlago za obdelavo.

Odprtost te določbe postavlja številna pomembna vprašanja o njenem točnem obsegu in uporabi, ki bosta analizirana v tem mnenju. Kot bo pojasnjeno v nadaljevanju, to ne pomeni nujno, da je treba to možnost obravnavati, kot da se lahko uporablja le zmerno kot „zadnja možnost“ ali kot zadnja priložnost, če se ne uporabi druga podlaga, za zapolnitev vrzeli v redkih in nepredvidenih okoliščinah. Niti se ne sme šteti za prednostno možnost in njena uporaba se ne sme neupravičeno razširiti, ker bi se ta podlaga štela za manj zavezujočo od drugih.

Namesto tega je mogoče, da ima člen 7(f) svoje naravno področje uporabe ter zelo koristno vlogo kot podlaga za zakonito obravnavo, če so izpolnjeni nekateri ključni pogoji.

Ustrezna uporaba člena 7(f) v pravih okoliščinah in ob ustreznih zaščitnih ukrepih pomaga preprečevati zlorabo drugih pravnih podlag in pretirano opiranje nanje.

Prvih pet podlag iz člena 7 temelji na privolitvi posameznika, na katerega se osebni podatki nanašajo, pogodbenem dogovoru, zakonski obveznosti ali drugih posebej opredeljenih razlogih kot podlagi za zakonitost. Kadar obdelava temelji na eni izmed teh petih podlag, se šteje, da je *a priori* zakonita in mora biti zato skladna le z drugimi veljavnimi zakonodajnimi določbami. Povedano drugače, domneva se, da obstaja ravnovesje med različnimi zadevnimi pravicami in interesi – skupaj s pravicami in interesi upravljavca in posameznika, na katerega se osebni podatki nanašajo –, če so seveda izpolnjene vse druge določbe zakonodaje o varstvu podatkov. Člen 7(f) pa, nasprotno, zahteva *poseben* test v primerih, ki ne spadajo v katerega izmed scenarijev, ki so vnaprej opredeljeni v točkah (a) do (e). Zagotavlja, da mora vsaka obdelava, ki ne spada med te scenarije, izpolnjevati zahtevo po testu tehtanja, pri čemer se ustrezno upoštevajo interesi in temeljne pravice posameznika, na katerega se osebni podatki nanašajo.

V nekaterih primerih lahko ta test pokaže, da je tehtnica na strani interesov in temeljnih pravic posameznika, na katerega se osebni podatki nanašajo, ter da zato obdelava ni mogoča. Nasprotno pa je lahko primerna ocena ravnovesja iz člena 7(f), pogosto z možnostjo zavrnitve obdelave, v drugih primerih ustrezna alternativa za, na primer, neprimerno uporabo „privolitve“ ali „potrebe po izvajanju pogodbe“ kot podlage. Če člen 7(f) pogledamo tako,

[19] Glej oddelek III.3.1, zlasti alinee na straneh 24 in 25, ki vsebujejo neizčrpen seznam nekaterih najobičajnejših okoliščin, v katerih se lahko postavi vprašanje zakonitih interesov iz člena 7(f).

zagotavlja dodatne zaščitne ukrepe – ki zahtevajo ustrezne ukrepe – v primerjavi z drugimi predhodno opredeljenimi podlagami. Zato se ne sme šteti za najšibkejši člen ali odprta vrata za upravičenje vseh postopkov obdelave podatkov, za katere se ne more uporabiti nobena druga pravna podlaga.

Delovna skupina ponavlja, da si pri razlagi področja uporabe člena 7(f) prizadeva za uravnotežen pristop, ki upravljavcem podatkov zagotavlja potrebno prožnost v primerih, v katerih ni pretiranega učinka na posameznike, na katere se osebni podatki nanašajo, tem posameznikom pa zagotavlja zadostno pravno gotovost in jamstva, da se ta odprta določba ne bo zlorabila.

II.3 Povezani koncepti

Razmerje med členom 7(f) in drugimi podlagami za zakonitost

V členu 7 je naprej navedena privolitev, za katero so naštete druge podlage za zakonitost, skupaj s pogodbami in zakonskimi obveznostmi, in nazadnje test zakonitega interesa, ki je naveden kot zadnji med šestimi možnimi podlagami. Vrstni red, v katerem so navedene pravne podlage v členu 7, se je včasih razlagal kot pokazatelj izrecnega pomena drugih podlag. Kot je delovna skupina že poudarila v mnenju o pojmu privolitve[20], pa besedilo Direktive ne določa pravnega razlikovanja med šestimi podlagami in ne namiguje, da med njimi obstaja hierarhija. Prav tako nič ne kaže, da se mora člen 7(f) uporabljati le v izjemnih primerih, in besedilo tudi sicer ne opredeljuje, da bi poseben vrstni red šestih pravnih podlag imel pravno relevanten učinek. Hkrati sta bila točen pomen člena 7(f) in njegovo razmerje z drugimi podlagami za zakonitost dolgo precej nejasna.

Glede na to ozadje ter ob upoštevanju zgodovinskih in kulturnih razlik in ubeseditve Direktive, ki omogoča različne razlage, se je razvilo več pristopov: nekatere države članice so v členu 7(f) videle vsaj prednostno podlago, ki naj bi zapolnila vrzeli le v redkih izjemnih primerih, v katerih se nobena od drugih petih podlag ne more ali ne bi mogla uporabiti.[21] Druge države članice pa v njem vidijo le eno od šestih možnosti, in to tako, ki ni ne bolj ne manj pomembna od drugih ter se lahko uporablja v številnih in zelo različnih položajih, če so izpolnjeni potrebni pogoji.

Ob upoštevanju teh razlik in tudi z vidika sodbe ASNEF in FECEMD je treba pojasniti razmerje med podlago, ki se nanaša na „zakonite interese“, in drugimi podlagami za zakonitost – na primer v zvezi s privolitvijo, pogodbami, nalogami v javnem interesu – ter v zvezi s pravico posameznika, na katerega se osebni podatki nanašajo, do ugovora. To bo lahko omogočilo boljšo opredelitev vloge in naloge podlage, ki se nanaša na zakonite interese, in tako prispevalo k pravni gotovosti.

Treba je še ugotoviti, da podlaga, ki zadeva zakonite interese, skupaj z drugimi podlagami, razen privolitve, zahteva test „nujnosti“. To strogo omejuje okoliščine, v katerih se lahko vsaka izmed njih uporablja. Sodišče Evropske unije je presodilo, da je „nujnost“ koncept, ki

[20] Glej opombo 2.

[21] Poudariti je treba še, da je odbor LIBE v predlogu spremembe 100 v osnutku poročila predlagal ločitev člena 7(f) od drugih pravnih podlag ter dodatne zahteve v primeru opiranja na to pravno podlago, skupaj z večjo preglednostjo in večjo odgovornostjo, kot bo predstavljeno v nadaljevanju.

ima v pravu Skupnosti svoj neodvisni pomen.[22] Evropsko sodišče za človekove pravice pa je zagotovilo tudi koristne smernice.[23]

Poleg tega upravljavca podatkov to, da ima primerno pravno podlago, ne odvezuje obveznosti, ki so mu naložene s členom 6 v zvezi s poštenostjo, zakonitostjo, nujnostjo, sorazmernostjo in kakovostjo podatkov. Na primer, tudi če bi obdelava osebnih podatkov temeljila na zakonitih interesih ali izpolnjevanju pogodbe, to ne bi dovoljevalo, da zbiranje podatkov presega to, kar je potrebno za neki namen.

Zakoniti interesi in druge podlage iz člena 7 so alternativne podlage, zato zadostuje, da se uporabi le ena izmed njih. Vseeno ne dopolnjujejo le zahtev iz člena 6, ampak tudi vsa druga načela in zahteve glede varstva podatkov, ki se lahko uporabljajo.

Drugi testi tehtanja

Člen 7(f) ni edini test tehtanja, predviden v Direktivi. Na primer, člen 9 zahteva tehtanje pravice do varstva osebnih podatkov in svobode izražanja. S tem členom je državam članicam dovoljeno, da določijo potrebne izjeme in odstopanja za obdelavo osebnih podatkov, „ki se izvaja zgolj v novinarske namene ali zaradi umetniškega ali literarnega izražanja samo, če so potrebna za uskladitev pravice do zasebnosti s predpisi, ki urejajo svobodo izražanja“.

Poleg tega tudi številne druge določbe Direktive zahtevajo analizo vsakega posameznega primera, uravnoteženje zadevnih interesov in pravic ter prožno oceno na podlagi več dejavnikov. Med njimi so določbe o nujnosti, sorazmernosti in omejitvi namena, izjeme iz člena 13 ter znanstvene raziskave, če naštejemo le nekatere.

Pravzaprav se zdi, da je bila Direktiva oblikovana tako, da omogoča prosto razlago in tehtanje interesov. Namen tega je bil seveda vsaj delno pustiti državam članicam še več prostora za prenos v nacionalno zakonodajo. Vendar poleg tega potreba po delni prožnosti izhaja tudi iz narave pravice do varstva osebnih podatkov in pravice do zasebnosti. Ti pravici se skupaj z večino (a ne vsemi) drugih temeljnih pravic štejeta za relativni ali kvalificirani človekovi pravici.[24] Take pravice je treba vedno razlagati v kontekstu. Ob upoštevanju ustreznih zaščitnih ukrepov se lahko uravnotežijo s pravicami drugih. V nekaterih primerih – in ob upoštevanju ustreznih zaščitnih ukrepov – so lahko tudi omejene z razlogi v javnem interesu.

[22] Sodba Sodišča z dne 16. decembra 2008 v zadevi Heinz Huber proti Zvezni republiki Nemčiji (C-524/06), točka 52: „Zato se vsebina pojma nujnosti – kot izhaja iz člena 7(e) Direktive 95/46, katerega namen je natančno določiti primere, v katerih je obdelava osebnih podatkov dopustna – ob upoštevanju cilja zagotovitve enakovredne ravni varstva v vseh državah članicah ne more spreminjati glede na posamezno državo članico. Gre torej za samostojen pojem prava Skupnosti, ki ga je treba razlagati tako, da popolnoma ustreza namenu te direktive, kot je opredeljen v njenem členu 1(1).“

[23] Evropsko sodišče za človekove pravice je v točki 97 sodbe z dne 25. marca 1983 v zadevi Silver in drugi proti Združenemu kraljestvu obravnavalo izraz „nujno v demokratični družbi“: „pridevnik ‚nujen‘ ne pomeni isto kot ‚nujno potreben‘ in njegov pomen tudi ni tako prilagodljiv kot pomen izrazov ‚dopusten‘, ‚običajen‘, ‚koristen‘, ‚razumen‘ ali ‚želen‘ […]“.

[24] Le nekaterih človekovih pravic ni mogoče uravnotežiti s pravicami drugih ali interesi širše skupnosti. To so absolutne pravice. Teh ni mogoče nikoli omejiti ne glede na okoliščine – celo v primeru vojne ali izrednih razmer. En primer je pravica vsakogar, da ni podvržen mučenju ali nečloveškemu ali ponižujočemu ravnanju ali kaznovanju. Ne glede na okoliščine ni nikoli dopustno mučiti osebo ali nečloveško ali ponižujoče ravnati z njo. Med neabsolutnimi človekovimi pravicami so spoštovanje zasebnega in družinskega življenja, pravica do svobode izražanja in pravica do svobode misli, vesti in vere.

II.4 Kontekst in strateške posledice

Zagotavljanje zakonitosti in prožnosti: sredstva za pojasnitev člena 7(f)

Trenutno besedilo člena 7(f) Direktive je mogoče razlagati na različne načine. To pomeni, da se je nanj mogoče opreti v številnih primerih, če so le njegove zahteve, skupaj s testom tehtanja, izpolnjene. Vendar ima lahko taka prožnost tudi negativne posledice. Da to ne bi privedlo do nedosledne uporabe v nacionalni zakonodaji ali pomanjkanja pravne gotovosti, bodo imela pomembno vlogo dodatna navodila.

Komisija v predlagani uredbi predvideva taka navodila v obliki delegiranih aktov. Druga možnost je, da se pojasnila in podrobne določbe zagotovijo v besedilu predlagane uredbe[25] ali/in da se Evropskemu odboru za varstvo podatkov dodeli naloga, da zagotovi smernice na tem področju.

Vsaka izmed teh možnosti ima prednosti in pomanjkljivosti. Če bi bilo treba vsak posamezni primer presojati brez dodatnih navodil, bi to lahko povzročilo nedosledno uporabo in pomanjkljivo predvidljivost, kot se je že zgodilo v preteklosti.

Nasprotno pa bi določitev podrobnih in izčrpnih seznamov primerov, v katerih bi zakoniti interesi upravljavca praviloma prevladali nad temeljnimi pravicami posameznika, na katerega se osebni podatki nanašajo, ali obratno, v besedilu predlagane uredbe lahko povzročilo zavajanje ali nepotrebne predpise ali oboje.

Ta pristopa bi vseeno lahko bila zgled za uravnoteženo rešitev, saj bi se v predlagani uredbi določile dodatne podrobnosti, dodatna navodila pa bi bila določena v delegiranih aktih ali smernicah Evropskega odbora za varstvo podatkov.[26]

Namen analize v poglavju III je določiti temelj za iskanje tega pristopa, ki ne bi bil niti preveč splošen, da ne bi bil nepomemben, niti preveč specifičen, da ne bi bil preveč tog.

[25] Glej oddelek II.1 Kratka zgodovina pod naslovom *Predlagana uredba o varstvu podatkov*, strani 8 in 9.
[26] Kar zadeve delegirane akte in smernice Evropskega odbora za varstvo podatkov, je delovna skupina v Mnenju št. 8/2012 kot dodatni prispevek k razpravam o reformi varstva podatkov, sprejetem 5. oktobra 2012 (WP 199), izrazila večjo naklonjenost prav smernicam (glej strani 13 in 14).

III. Analiza določb

III.1 Pregled člena 7

Člen 7 določa, da se osebni podatki obdelujejo le, če se uporablja vsaj ena izmed šestih pravnih podlag, naštetih v tem členu. Pred analizo vsake od teh podlag bo v oddelku III.1 predstavljen pregled člena 7 in njegovega razmerja s členom 8 o posebnih vrstah podatkov.

III.1.1 Privolitev ali „potrebna za […]“

Razlikovati je mogoče med primerom, v katerem se osebni podatki obdelujejo na podlagi nedvoumne privolitve posameznika, na katerega se osebni podatki nanašajo (člen 7(a)), in drugimi petimi primeri (člen 7(b) do (f)). Skratka, v teh petih primerih so opisani scenariji, ko je lahko obdelava potrebna v posebnih okoliščinah, kot so izpolnjevanje pogodbe, sklenjene s posameznikom, na katerega se osebni podatki nanašajo, skladnost z zakonsko obveznostjo, ki velja za upravljavca, itd.

V prvem primeru iz člena 7(a) posamezniki, na katere se osebni podatki nanašajo, sami dovolijo obdelavo svojih osebnih podatkov. Sami se odločijo, ali bodo dovolili obdelavo svojih podatkov. Hkrati privolitev ne pomeni, da ni treba upoštevati načel iz člena 6.[27] Poleg tega mora privolitev še vedno izpolnjevati nekatere poglavitne pogoje, da je zakonita, kot je pojasnjeno v Mnenju delovne skupine št. 15/2011.[28] Glede na to, da se uporabnik ne nazadnje lahko sam odloči glede obdelave svojih osebnih podatkov, je poudarek na veljavnosti in obsegu privolitve posameznika, na katerega se osebni podatki nanašajo.

Z drugimi besedami, prva podlaga iz člena 7(a) se osredotoča na samoodločanje posameznika, na katerega se osebni podatki nanašajo, kot podlago za zakonitost. Vse druge podlage, nasprotno, dovoljujejo obdelavo – ob upoštevanju zaščitnih in drugih ukrepov – v primerih, v katerih je ne glede na privolitev primerno in nujno obdelati podatke v nekem kontekstu v prizadevanju za poseben zakoniti interes.

V točkah (b), (c), (d) in (e) je opredeljeno merilo za zakonitost obdelave:

(b) izvajanje pogodbe, katere stranka je posameznik, na katerega se nanašajo osebni podatki;
(c) skladnost z zakonsko obveznostjo, ki velja za upravljavca;
(d) varstvo življenjskih interesov posameznikov, na katere se osebni podatki nanašajo;
(e) izvajanje naloge, ki se opravlja v javnem interesu.

Točka (f) je manj natančna in se splošneje nanaša na (kateri koli) zakoniti interes, za katerega si prizadeva upravljavec (v katerem koli kontekstu). Za to splošno določbo pa je posebej

[27] Sodba nizozemskega vrhovnega sodišča z dne 9. septembra 2011 v zadevi ECLI:NL:HR:2011:BQ8097, točka 3.3(e), ki se nanaša na načelo sorazmernosti. Glej tudi stran 7 Mnenja delovne skupine št. 15/2011, navedenega v opombi 2: „[...] pridobitev privolitve upravljavca ne odvezuje obveznosti iz člena 6 v zvezi s pravičnostjo, potrebnostjo, sorazmernostjo in kakovostjo podatkov. Na primer, tudi če obdelava osebnih podatkov temelji na privolitvi uporabnika, to ne bi utemeljilo zbiranja podatkov, ki bi presegalo namen, za katerega se zbirajo.“

[28] Glej strani 11–25 Mnenja št. 15/2011, navedenega v opombi 2.

določen dodaten test tehtanja, katerega namen je varovati interese in pravice posameznikov, na katere se osebni podatki nanašajo, kot bo prikazano v oddelku III.2.

Ali je bilo merilo iz člena 7(a) do (f) izpolnjeno, najprej oceni upravljavec podatkov ob upoštevanju veljavnih zakonov in smernic za uporabo zakonov. Zakonitost obdelave je nato lahko odvisna od dodatne ocene in jo lahko izpodbijajo posamezniki, na katere se osebni podatki nanašajo, drugi deležniki in organi za varstvo podatkov, nazadnje pa o njej odločajo sodišča.

Za dopolnitev tega kratkega pregleda je treba omeniti, da lahko – kot bo obravnavano v oddelku III.3.6 – vsaj v primerih, na katere se sklicujeta točki (e) in (f), posameznik, na katerega se osebni podatki nanašajo, uveljavlja pravico do ugovora, kot je določena v členu 14.[29] To bo vzrok za novo oceno zadevnih interesov ali pa bo v primeru neposrednega trženja (člen 14(b)) zahtevalo, da upravljavec ustavi obdelavo osebnih podatkov brez dodatne ocene.

III.1.2 Razmerje s členom 8

Člen 8 Direktive dodatno ureja obdelavo nekaterih posebnih vrst osebnih podatkov. Uporablja se posebej za podatke, „ki kažejo na rasni ali etnični izvor, politična mnenja, verska ali filozofska prepričanja, pripadnost sindikatu, in obdelavo podatkov v zvezi z zdravjem ali spolnim življenjem“ (člen 8(1)), in podatke „v zvezi s prekrški [ali] kazenskimi obsodbami“ (člen 8(5)).

Obdelava takih podatkov je načeloma prepovedana, z nekaj izjemami. Člen 8(2) v točkah (a) do (e) določa nekatere izjeme od take prepovedi. Člen 8(3) in (4) določa še dodatne izjeme. Nekatere izmed teh določb so podobne – vendar ne enake – določbam v členu 7(a) do (f).

Zaradi posebnih pogojev iz člena 8 in dejstva, da so nekatere podlage, navedene v členu 7, podobne pogojem, določenim v členu 8, se postavlja vprašanje razmerja med tema določbama.

Če je člen 8 mišljen kot *lex specialis*, je treba ugotoviti, ali izključuje uporabo člena 7 v celoti. Če je tako, bi to pomenilo, da je mogoče posebne vrste osebnih podatkov obdelovati, ne da bi bile izpolnjene zahteve iz člena 7, pod pogojem, da se uporablja ena izmed izjem iz člena 8. Vseeno je mogoče tudi, da je razmerje bolj vsestransko ter je treba člena 7 in 8 uporabljati kumulativno.[30]

V vsakem primeru je jasno, da je cilj politike zagotoviti dodatno varstvo za posebne vrste podatkov. Zato mora biti končni rezultat analize enako jasen: namen uporabe samega člena 8 ali v povezavi s členom 7 je zagotoviti višjo raven varstva posebnih vrst podatkov.

[29] Kar zadeva člen 14(a), se ta pravica uporablja, „razen, kjer nacionalna zakonodaja določa drugače“. Na primer, švedska nacionalna zakonodaja ne omogoča ugovora zoper obdelavo, ki temelji na členu 7(e).

[30] Ker je člen 8 določen kot *prepoved z izjemami*, je te izjeme mogoče obravnavati kot zahteve, ki omejujejo le področje uporabe prepovedi, vendar same po sebi niso zadostna pravna podlaga za obdelavo. Ob taki razlagi uporaba izjem iz člena 8 ne izključuje uporabe zahtev iz člena 7, zato je treba oba člena, če je primerno, uporabljati kumulativno.

Čeprav člen 8 za nekatere primere določa strožje zahteve – kot je „izrecna“ privolitev v členu 8(2)(a) v primerjavi z „nedvoumno“ privolitvijo v členu 7 –, to v praksi ne velja za vse določbe. Nekatere izjeme, določene v členu 8, niso enakovredne podlagam, navedenim v členu 7, ali strožje od njih. Neprimerno bi bilo na primer sklepati, da bi bilo to, da je nekdo javno objavil nekatere vrste podatkov v skladu s členom 8(2)(e), – vedno in samo po sebi – zadosten pogoj za dovolitev katere koli vrste obdelave podatkov brez ocene ravnovesja med zadevnimi interesi in pravicami, kot se zahteva v členu 7(f).[31]

V nekaterih primerih bi se zato, ker je upravljavec podatkov politična stranka, odpravila tudi prepoved obdelave posebnih vrst podatkov v skladu s členom 8(2)(d). To vseeno ne pomeni, da je vsaka obdelava v okviru področja uporabe določbe nujno zakonita. To je treba oceniti ločeno, upravljavec pa morda mora na primer dokazati, da je obdelava podatkov potrebna za izvajanje pogodbe (člen 7(b)) ali da prevladajo njegovi zakoniti interesi v skladu s členom 7(f). V zadnjem primeru je treba opraviti test tehtanja v skladu s členom 7(f), potem ko je bilo ugotovljeno, da upravljavec podatkov izpolnjuje zahteve iz člena 8.

Podobno le to, da „se podatki obdelujejo za potrebe preventivne medicine, zdravstvene diagnoze, za zagotovitev oskrbe, ali zdravljenja, ali vodenje zdravstvenih služb“ ter da se ti podatki obdelujejo v skladu z dolžnostjo molčečnosti – vse to je navedeno v členu 8(3) –, pomeni, da je taka obdelava občutljivih podatkov *izvzeta iz prepovedi* iz člena 8(1). Vendar to ni nujno dovolj, da bi bila zagotovljena tudi zakonitost v skladu s členom 7, in bo zahtevalo pravno podlago, kot je pogodba z bolnikom v skladu s členom 7(b), zakonska obveznost v skladu s členom 7(c), izvajanje naloge v javnem interesu v skladu s členom 7(e) ali ocena v skladu s členom 7(f).

Skratka, delovna skupina meni, da je treba v vsakem posameznem primeru analizirati, ali člen 8 sam po sebi določa strožje in zadostne pogoje[32] ali pa je potrebna kumulativna uporaba členov 7 in 8, da se zagotovi polno varstvo posameznikov, na katere se osebni podatki nanašajo. V nobenem primeru pa rezultat preučitve ne sme povzročiti manjšega varstva za posebne vrste podatkov.[33]

To pomeni tudi, da se upravljavec, ki obdeluje posebne vrste podatkov, lahko nikoli ne sklicuje *le* na pravno podlago iz člena 7, da bi upravičil obdelavo podatkov. Kadar je primerno, člen 7 ne bo *prevladal*, ampak se bo vedno uporabljal *kumulativno* s členom 8 za zagotovitev, da se ravna v skladu z vsemi ustreznimi zaščitnimi in drugimi ukrepi. To bo še toliko bolj pomembno, če se države članice odločijo določiti dodatne izjeme poleg tistih iz člena 8, kot je predvideno v členu 8(4).

[31] Poleg tega se člen 8(2)(e) ne bi smel *a contrario* razlagati tako, da se podatki, ki jih javno objavi posameznik, na katerega se osebni podatki nanašajo, kadar ti niso občutljivi, lahko obdelujejo brez dodatnega pogoja. Javno dostopni podatki so še vedno osebni podatki, za katere veljajo zahteve glede varstva podatkov, tudi glede skladnosti s členom 7, ne glede na to, ali so podatki občutljivi ali ne.

[32] Glej točko 3.3 analize v mnenju WADA delovne skupine, v kateri se obravnavata člena 7 in 8 Direktive: Drugo mnenje 4/2009 o Mednarodnem standardu Svetovne protidopinške agencije (WADA) o varstvu zasebnosti in osebnih podatkov, o povezanih določbah Kodeksa WADA ter o drugih vprašanjih glede zasebnosti v boju Svetovne protidopinške agencije in (nacionalnih) protidopinških organizacij proti dopingu v športu, sprejeto 6. aprila 2009 (WP 162).

[33] Ni treba posebej poudariti, da je treba tudi ob uporabi člena 8 zagotoviti upoštevanje drugih določb Direktive, skupaj s členom 6.

III.2 Člen 7(a) do (e)

Ta oddelek III.2 vsebuje kratek pregled vseh pravnih podlag iz člena 7(a) do (e) Direktive, preden se bo delovna skupina v oddelku III.3 osredotočila na člen 7(f). V tej analizi bodo poudarjene tudi nekatere najbolj običajne stične točke med temi pravnimi podlagami, ki na primer vključujejo „pogodbo“, „zakonsko obveznost“ in „zakoniti interes“ glede na posebne okoliščine in dejstva posameznega primera.

III.2.1 Privolitev

Privolitev kot pravna podlaga je bila analizirana v Mnenju delovne skupine št. 15/2011 o opredelitvi privolitve. Glavne ugotovitve so, da je privolitev ena od številnih pravnih podlag za obdelavo osebnih podatkov, ne pa glavna. Ima pomembno nalogo, vendar to ne izključuje možnosti, da so glede na okoliščine druge pravne podlage z vidika upravljavca in posameznika, na katerega se osebni podatki nanašajo, lahko primernejše. Privolitev ob pravilni uporabi pomeni orodje, ki posamezniku, na katerega se osebni podatki nanašajo, omogoča nadzor nad obdelavo njegovih podatkov. Ob nepravilni uporabi nadzor posameznika, na katerega se osebni podatki nanašajo, postane navidezen, privolitev pa pomeni neprimerno podlago za obdelavo.

Delovna skupina je pri priporočilih poudarila, da je treba pojasniti pomen „nedvoumne“ privolitve: „Pojasnitev bi morala biti namenjena poudarku, da je za nedvoumno privolitev potrebna uporaba mehanizmov, ki ne vzbujajo dvomov glede namere posameznika, na katerega se osebni podatki nanašajo, o privolitvi. Hkrati je treba pojasniti, da uporaba privzetih možnosti, ki jih mora posameznik, na katerega se osebni podatki nanašajo, spremeniti, da bi zavrnil obdelavo (privolitev na podlagi molka), sama po sebi ne pomeni nedvoumne privolitve. To zlasti velja v spletnem okolju.“[34] Zahteva se tudi, da upravljavci podatkov uvedejo mehanizme za izražanje privolitve (v okviru splošne obveznosti odgovornosti) ter da zakonodajalci dodajo izrecno zahtevo glede kakovosti in razpoložljivosti informacij, ki so podlaga za privolitev.

III.2.2 Pogodba

Člen 7(b) določa pravno podlago v primerih, ko je „obdelava potrebna za izvajanje pogodbe, katere stranka je posameznik, na katerega se nanašajo osebni podatki, ali pa za izvajanje ukrepov na zahtevo posameznika, na katerega se osebni podatki nanašajo, pred sklenitvijo pogodbe“. To zajema dva scenarija.

(i) Prvič, določba zajema primere, v katerih je obdelava potrebna za izvajanje pogodbe, katere stranka je posameznik, na katerega se nanašajo osebni podatki. To lahko na primer vključuje obdelavo naslova posameznika, na katerega se osebni podatki nanašajo, da se lahko dobavi blago, kupljeno na spletu, ali obdelavo podatkov o kreditni kartici zaradi izvršitve plačila. Na področju zaposlovanja lahko ta podlaga dovoljuje na primer obdelavo podatkov o plači in bančnem računu, da se lahko izplačajo plače.

[34] Glej stran 36 Mnenja delovne skupine št. 15/2011 o opredelitvi privolitve.

Določba, ki jo je treba razlagati ozko, ne zajema primerov, v katerih obdelava ni resnično *potrebna* za izvajanje pogodbe, ampak jo upravljavec enostransko vsili posamezniku, na katerega se osebni podatki nanašajo. Tudi dejstvo, da pogodba zajema nekatere postopke obdelave podatkov, ne pomeni samodejno, da je obdelava potrebna za njeno izvajanje. Na primer, člen 7(b) ni primerna pravna podlaga za oblikovanje profila uporabnikovih okusov in življenjskih odločitev na podlagi klikov na spletnem mestu in kupljenih izdelkov. Pogodba z upravljavcem podatkov namreč ni bila sklenjena za oblikovanje profila, ampak, na primer, za dobavo nekega blaga in opravljanje nekih storitev. Tudi če so te dejavnosti obdelave posebej omenjene v drobnem tisku v pogodbi, to samo po sebi ne pomeni, da so „potrebne“ za izvajanje pogodbe.

Obstaja jasna povezava med oceno nujnosti in skladnostjo z načelom omejitve namena. Pomembno je opredeliti natančne razloge za pogodbo, to je njeno vsebino in temeljni cilj, saj bo glede na to preskušeno, ali je obdelava podatkov potrebna za izvajanje pogodbe.

V nekaterih mejnih primerih je lahko sporno ali pa se zahteva natančnejše ugotavljanje dejstev, da se ugotovi, ali je obdelava potrebna za izvajanje pogodbe. Na primer, oblikovanje notranje podatkovne zbirke o pogodbah zaposlenih za celotno družbo, ki vsebuje ime, poslovni naslov, telefonsko številko in elektronski naslov vseh zaposlenih, da bi lahko ti vzpostavili stik s sodelavci, se lahko v nekaterih primerih šteje za potrebno za izvajanje pogodbe v skladu s členom 7(b), vendar je lahko zakonito tudi v skladu s členom 7(f), če je dokazan prevladujoč interes upravljavca in so sprejeti vsi ustrezni ukrepi, tudi na primer ustrezno posvetovanje s predstavniki zaposlenih.

Drugi primeri, kot je elektronski nadzor uporabe spleta, elektronske pošte in telefona zaposlenega ali videonadzor zaposlenih, bolj nedvoumno pomenijo obdelavo, ki bi lahko presegla to, kar je potrebno za izvajanje pogodbe o zaposlitvi, čeprav je tudi v tem primeru to lahko odvisno od narave zaposlitve. Preprečevanje goljufij – ki lahko med drugim zajema spremljanje kupcev in oblikovanje njihovih profilov – je še eno značilno področje, za katero se lahko šteje, da presega to, kar je potrebno za izvajanje pogodbe. Taka obdelava je še vedno lahko zakonita na podlagi druge podlage iz člena 7, kot so privolitev, če je primerno, zakonska obveznost ali zakoniti interes upravljavca (člen 7(a), (c) ali (f)).[35] V zadnjem primeru morajo za obdelavo veljati dodatni zaščitni ukrepi, da se ustrezno varujejo interesi ter pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo.

Člen 7(b) se uporablja le za to, kar je potrebno za *izvajanje* pogodbe. Ne uporablja se za vse dodatne ukrepe, potrebne zaradi neskladnosti, ali za vse druge incidente, ki se zgodijo pri izvajanju pogodbe. Dokler obdelava zajema običajno izvajanje pogodbe,

[35] Drug primer več pravnih podlag je mogoče najti v Mnenju delovne skupine št. 15/2011 o opredelitvi privolitve (navedeno v opombi 2). Upravljavec podatkov je lahko pri nakupu avtomobila upravičen do obdelave osebnih podatkov za različne namene in na različnih podlagah:
– podatki, ki so potrebni za nakup avtomobila: člen 7(b),
– za obdelavo dokumentacije v zvezi z avtomobilom: člen 7(c),
– za storitve upravljanja s strankami (npr. za servisiranje avtomobila v različnih podružnicah v EU): člen 7(f),
– za prenos podatkov tretjim osebam za njihove lastne dejavnosti trženja: člen 7(a).

lahko spada v člen 7(b). Če pri izvajanju pogodbe nastane incident, zaradi katerega nastane spor, se lahko obdelava podatkov izvede drugače. Za obdelavo osnovnih podatkov o posamezniku, na katerega se osebni podatki nanašajo, kot so ime, naslov in podatki o neporavnanih pogodbenih obveznostih, za pošiljanje opominov se mora še vedno šteti, da spada v okvir obdelave podatkov, potrebne za izvajanje pogodbe. V zvezi z bolj izpopolnjeno obdelavo podatkov, ki lahko vključuje tretje osebe ali ne, kot je zunanja izterjava dolgov ali vložitev tožbe zoper kupca, ki ni plačal storitve, bi bilo mogoče trditi, da taka obdelava ne spada več v okvir „običajnega“ izvajanja pogodbe in zato ne spada več na področje uporabe člena 7(b). Vendar zato obdelava kot taka še ni nezakonita: upravljavec ima zakonit interes uporabiti pravna sredstva za zagotovitev spoštovanja svojih pogodbenih pravic. Opreti se je mogoče na druge pravne podlage, kot je člen 7(f), ob upoštevanju ustreznih zaščitnih ukrepov in ob opravljenem testu tehtanja.[36]

(ii) Drugič, člen 7(b) zajema tudi obdelavo, ki se izvede *pred* sklenitvijo pogodbe. To zajema predpogodbena razmerja, če se izvedejo ukrepi na zahtevo posameznika, na katerega se osebni podatki nanašajo, in ne na pobudo upravljavca ali tretje osebe. Na primer, če posameznica od trgovca zahteva, naj ji pošlje ponudbo za izdelek, je obdelava za te namene, kot je hramba podatkov o naslovu in informacij o zahtevanem izdelku v omejenem obdobju, primerna v skladu s to pravno podlago. Podobno, če posameznik od zavarovalnice zahteva ponudbo za svoj avtomobil, lahko zavarovalnica obdela potrebne podatke, na primer znamko in starost avtomobila ter druge upoštevne in sorazmerne podatke, da pripravi ponudbo.

Vendar se podrobno preverjanje preteklosti, pri katerem se na primer obdelajo podatki o zdravstvenih pregledih, preden zavarovalnica zagotovi zdravstveno ali življenjsko zavarovanje prosilcu, ne bi štelo za potreben ukrep, izveden na zahtevo posameznika, na katerega se osebni podatki nanašajo. Tudi preverjanje bonitetnih podatkov pred odobritvijo kredita se ne izvede na *zahtevo* posameznika, na katerega se osebni podatki nanašajo, v skladu s členom 7(b), ampak v skladu s členom 7(f) ali 7(c) na podlagi zakonske obveznosti bank, da preverijo uradni seznam dolžnikov.

Neposredno trženje na pobudo trgovca/upravljavca tudi ne bo mogoče na tej podlagi. V nekaterih primerih bi lahko člen 7(f) zagotavljal ustreznejšo pravno podlago kot člen 7(b), ob upoštevanju ustreznih zaščitnih ukrepov in ob opravljenem testu tehtanja. V drugim primerih, tudi v primerih, ki vključujejo celovito oblikovanje profilov, izmenjavo podatkov, spletno neposredno trženje ali vedenjsko oglaševanje, je treba upoštevati privolitev iz člena 7(a), kot je razvidno iz analize v nadaljevanju.[37]

[36] Kar zadeva posebne vrste podatkov, je morda treba upoštevati tudi obdelavo iz člena 8(1)(e) – „potrebna za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov“.
[37] Glej oddelek III.3.6(b) pod naslovom Primer: razvoj pristopa k neposrednemu trženju na straneh 45 in 46.

III.2.3 Zakonska obveznost

Člen 7(c) določa pravno podlago v primerih, v katerih „je obdelava potrebna za skladnost z zakonsko obveznostjo, ki velja za upravljavca“. Tak je primer, v katerem morajo delodajalci pošiljati podatke o plačah svojih zaposlenih organom za socialno varnost ali davčnim organom, ali primer, v katerem morajo finančne institucije pristojnim organom poročati o nekaterih sumljivih transakcijah v skladu s pravili o preprečevanju pranja denarja. Lahko gre tudi za obveznost, ki velja za javni organ, saj nič ne omejuje uporabe člena 7(c) na zasebni ali javni sektor. To bi veljalo na primer za zbiranje podatkov s strani lokalnega organa zaradi obravnavanja glob za nedovoljeno parkiranje.

Člen 7(c) je podoben členu 7(e), saj naloga v javnem interesu pogosto temelji na zakonski določbi ali izhaja iz nje. Področje uporabe člena 7(c) je vseeno ozko opredeljeno.

Da se lahko člen 7(c) uporablja, mora biti obveznost določena z zakonom (in ne na primer s pogodbenim dogovorom). Zakon mora izpolnjevati vse upoštevne pogoje, da je obveznost veljavna in zavezujoča, skladen pa mora biti tudi z zakonom o varstvu podatkov, skupaj z zahtevami glede nujnosti, sorazmernosti[38] in omejitve namena.

Pomembno je še poudariti, da se člen 7(c) sklicuje na zakonodajo Evropske unije ali države članice. Ta podlaga ne zajema obveznosti, ki izhajajo iz zakonodaje tretjih držav (kot je obveznost vzpostavitve shem za prijavo nepravilnosti v skladu z zakonom Sarbanes-Oxley iz leta 2002 v Združenih državah). Da bi bila zakonska obveznost tretje države veljavna, bi morala biti uradno priznana in vnesena v pravni red zadevne države članice, na primer v obliki mednarodnega sporazuma.[39] Nasprotno lahko potreba po skladnosti s tujo obveznostjo pomeni zakonit interes upravljavca, vendar le ob upoštevanju testa tehtanja iz člena 7(f) in če se vzpostavijo ustrezni zaščitni ukrepi, kakršne odobri pristojni organ za varstvo podatkov.

Upravljavec ne sme imeti izbire, ali naj izpolni obveznost ali ne. Prostovoljne enostranske zaveze in javno-zasebna partnerstva, ki obdelujejo podatke, ki presegajo to, kar se zahteva z zakonom, tako niso zajeti v členu 7(c). Na primer, če se ponudnik spletnih storitev – brez jasne in točno določene zakonske obveznosti – odloči nadzirati svoje uporabnike zaradi preprečevanja nezakonitega prenosa podatkov, člen 7(c) ne bo ustrezna pravna podlaga za ta namen.

Poleg tega mora biti zakonska obveznost dovolj jasna glede tega, kakšno obdelavo osebnih podatkov zahteva. Člen 7(c) se tako uporablja na podlagi zakonskih določb, ki se izrecno sklicujejo na naravo in predmet obdelave. Upravljavec ne sme imeti pretirane možnosti za samovoljno odločitev, kako izpolnjevati zakonsko obveznost.

Zakonodaja lahko v nekaterih primerih določa le splošni cilj, natančnejše obveznosti pa so določene na različnih ravneh, bodisi v sekundarni zakonodaji bodisi z zavezujočo odločitvijo

[38] Glej tudi Mnenje št. 1/2014 o uporabi konceptov nujnosti in sorazmernosti ter varstva podatkov v sektorju kazenskega pregona, ki ga je delovna skupina sprejela 27. februarja 2014 (WP 211).

[39] V zvezi s tem glej oddelek 4.2.2 Mnenja 10/2006 o obdelavi osebnih podatkov Družbe za svetovne medbančne finančne telekomunikacije (SWIFT), ki ga je delovna skupina sprejela 20. novembra 2006 (WP 128), in Mnenje 1/2006 o uporabi pravil EU o varstvu podatkov v notranjih shemah za prijavo nepravilnosti na področjih računovodstva, internih računovodskih kontrol, revizijskih zadev, boja proti podkupovanju, bančnemu in finančnemu kriminalu, ki ga je delovna skupina sprejela 1. februarja 2006 (WP 117).

javnega organa v konkretnem primeru. Tudi to lahko privede do zakonskih obveznosti iz člena 7(c), če sta narava in predmet obdelave dobro opredeljena in zanju velja ustrezna pravna podlaga.

Drugače pa je, če bi regulativni organ določil le splošne smernice glede politike in pogoje, pod katerimi bi lahko razmislil o uporabi svojih izvršilnih pooblastil (na primer regulativna navodila za finančne institucije glede nekaterih standardov potrebne skrbnosti). V takih primerih je treba postopke obdelave oceniti na podlagi člena 7(f), za zakonite pa se lahko štejejo le, če se opravi dodaten test tehtanja.[40]

Na splošno je treba ugotoviti, da lahko nekateri postopki obdelave skoraj spadajo v okvir člena 7(c) ali (b), ne da bi v celoti izpolnjevali merila za uporabo teh podlag. To ne pomeni, da je taka obdelava vedno nujno nezakonita: včasih je lahko zakonita, vendar bolj v okviru člena 7(f), ob upoštevanju dodatnega testa tehtanja.

III.2.4 Življenjski interesi

Člen 7(d) določa pravno podlago v primerih, v katerih „je obdelava potrebna za varstvo življenjskih interesov posameznikov, na katere se osebni podatki nanašajo“. Ta ubeseditev je drugačne od tiste v členu 8(2)(c), ki je natančnejša in se nanaša na primere, v katerih „je obdelava potrebna za varstvo življenjskih interesov posameznika, na katerega se osebni podatki nanašajo, ali druge osebe, kadar posameznik, na katerega se osebni podatki nanašajo, fizično ali pravno ni sposoben dati svoje privolitve“.

Obe določbi vseeno kažeta, da bi morala biti uporaba te pravne podlage omejena. Najprej, izraz „življenjski interes“ omejuje uporabo te podlage na vprašanja življenja in smrti ali vsaj na grožnje, ki jih pomeni tveganje poškodbe ali druge škode za zdravje posameznika, na katerega se osebni podatki nanašajo (ali v primeru člena 8(2)(c) tudi druge osebe).

Uvodna izjava 31 potrjuje, da je cilj te pravne podlage „zaščit[a] interesa, ki je bistven za življenje posameznika, na katerega se osebni podatki nanašajo“. Vendar v Direktivi ni natančno navedeno, ali mora biti grožnja neposredna. S tem se postavljajo vprašanja glede obsega zbiranja podatkov, na primer kot preventivnega ukrepa ali na širši ravni, kot je zbiranje podatkov o letalskih potnikih, ko je bila ugotovljena nevarnost epidemije ali varnostni incident.

Delovna skupina meni, da je treba to določbo razlagati ozko, skladno s smislom člena 8. Čeprav s členom 7(d) uporaba te podlage ni posebej omejena na primere, v katerih kot pravno podlago ni mogoče uporabiti privolitve, in to iz razlogov, navedenih v členu 8(2)(c), je razumno sklepati, da je treba v primerih, v katerih je mogoče in nujno zahtevati veljavno privolitev, resnično zaprositi za privolitev, kadar koli je to izvedljivo. To tudi omejuje uporabo te določbe na analizo vsakega posameznega primera in se ne more običajno uporabljati za upravičenje vsakršnega masovnega zbiranja ali obdelave osebnih podatkov. Če bi bilo to potrebno, bi bil ustreznejša podlaga za obdelavo člen 7(c) ali (e).

[40] Smernice regulativnega organa so lahko še vedno pomembne pri oceni zakonitega interesa upravljavca (glej točko (a) oddelka III.3.4, zlasti na strani 36).

III.2.5 Javna naloga

Člen 7(e) določa pravno podlago v primerih, v katerih „je obdelava potrebna za izvajanje naloge, ki se opravlja v javnem interesu ali pri izvrševanju javne oblasti, dodeljene upravljavcu ali tretji stranki, ki so ji posredovani podatki“.

Pomembno je poudariti, da se člen 7(e) tako kot člen 7(c) nanaša na javni interes Evropske unije ali države članice. Podobno izraz „javna oblast“ pomeni pristojnost, ki jo podeli Evropska unija ali država članica. Z drugimi besedami, naloge, ki se izvajajo v javnem interesu tretje države ali pri izvajanju javne oblasti, dodeljene s tujo zakonodajo, ne spadajo na področje uporabe te določbe.[41]

Člen 7(e) zajema dva primera ter je upošteven v javnem in zasebnem sektorju. Prvič, zajema primere, v katerih je upravljavcu dodeljena javna oblast ali naloga v javnem interesu (ne pa nujno tudi zakonska obveznost za obdelavo podatkov), obdelava pa je potrebna za izvajanje te oblasti ali naloge. Na primer, davčni organ lahko zbira in obdela posameznikovo davčno napoved, da ugotovi in preveri znesek davka, ki ga mora ta plačati. Ali pa lahko poklicna združenja, kot je odvetniška ali zdravniška zbornica, ki jim je dodeljena javna oblast, da to storijo, izvajajo disciplinske postopke zoper nekatere izmed svojih članov. Še en primer je lahko lokalni vladni organ, kot je občinski organ, ki mu je zaupana naloga vodenja knjižnice, šole ali lokalnega bazena.

Drugič, člen 7(e) zajema tudi primere, v katerih upravljavcu ni bila dodeljena javna oblast, ga je pa tretja oseba, ki ima tako oblast, zaprosila za posredovanje podatkov. Na primer, uradnik javnega organa, pristojnega za preiskavo kaznivega dejanja, lahko zaprosi upravljavca za sodelovanje v potekajoči preiskavi, namesto da od njega zahteva, da ravna skladno s posebno zahtevo po sodelovanju. Člen 7(e) lahko zajema še primere, v katerih upravljavec proaktivno posreduje podatke tretji osebi, ki ima tako javno oblast. Tak je lahko primer, v katerem upravljavec ugotovi, da je bilo storjeno kaznivo dejanje, in to informacijo na svojo pobudo posreduje pristojnim organom kazenskega pregona.

Drugače kot v primeru člena 7(c), za upravljavca ne velja nobena zahteva, da ravna skladno z zakonsko obveznostjo. Če uporabimo zgornji primer, upravljavec, ki po naključju opazi, da je bila storjena tatvina ali goljufija, lahko ni zakonsko zavezan to sporočiti policiji, lahko pa v ustreznih primerih vseeno to stori prostovoljno na podlagi člena 7(e).

Vendar mora biti obdelava „potrebna za izvajanje naloge, ki se opravlja v javnem interesu“. Alternativno, javna oblast mora biti dodeljena upravljavcu ali tretji osebi, kateri upravljavec posreduje podatke, obdelava podatkov pa mora biti potrebna za izvrševanje te oblasti.[42] Pomembno je tudi poudariti, da je bila ta javna oblast ali javna naloga običajno dodeljena z zakoni ali drugimi predpisi. Če obdelava vključuje poseganje v zasebnost ali če se to sicer zahteva v skladu z nacionalno zakonodajo, da se zagotovi zaščita zadevnih posameznikov, mora biti pravna podlaga točno določena in dovolj natančna pri opredelitvi, kakšna vrsta obdelave podatkov se lahko dovoli.

[41] Glej oddelek 2.4 Delovnega dokumenta o skupni razlagi člena 26(1) Direktive 95/46/ES z dne 24. oktobra 1995, ki ga je delovna skupina sprejela 25. novembra 2005 (WP 114), v zvezi s podobno razlago izraza „na temelju pomembnega javnega interesa“ iz člena 26(1)(d).

[42] Z drugimi besedami, v teh primerih bosta še naprej upoštevna javni pomen nalog in ustrezna odgovornost, tudi če je bilo izvajanje naloge preneseno na druge subjekte, skupaj z zasebnimi.

Ti primeri postajajo čedalje bolj običajni tudi zunaj javnega sektorja, glede na razširjenost oddajanja vladnih del v izvajanje subjektom v zasebnem sektorju. Tako je lahko pri obdelavi podatkov v prevoznem ali zdravstvenem sektorju (na primer epidemiološke študije, raziskave). Na to podlago se je mogoče sklicevati tudi pri kazenskem pregonu, kot je bilo že nakazano v zgornjih primerih. Vendar to, koliko se zasebnemu podjetju lahko dovoli sodelovanje z organi kazenskega pregona, na primer v boju proti goljufijam ali nezakonitim vsebinam na spletu, zahteva analizo ne le z vidika člena 7, ampak tudi z vidika člena 6 ob upoštevanju zahtev glede omejitve namena, zakonitosti in poštenosti.[43]

Člen 7(e) ima lahko zelo široko področje uporabe, zaradi česar sta potrebna stroga razlaga in v vsakem posameznem primeru jasna opredelitev zadevnega javnega interesa in javne oblasti, ki upravičuje obdelavo. To široko področje uporabe tudi pojasnjuje, zakaj je bila v členu 14 – tako kot za člen 7(f) – določena pravica do ugovora, ko obdelava temelji na členu 7(e).[44] V obeh primerih se lahko uporabljajo podobni dodatni zaščitni in drugi ukrepi[45].

V tem smislu je člen 7(e) podoben členu 7(f) in v nekaterih okoliščinah, zlasti za javne organe, lahko člen 7(e) nadomesti člen 7(f).

Pri oceni področja uporabe teh določb za javne organe, zlasti z vidika predlaganih sprememb v pravnem okviru varstva podatkov, je koristno ugotoviti, da trenutno besedilo Uredbe št. 45/2001[46], ki določa pravila o varstvu podatkov, ki se uporabljajo za institucije in organe Evropske unije, ne vsebuje določbe, primerljive s členom 7(f).

Vendar je v uvodni izjavi 27 te uredbe navedeno, da „[o]bdelava osebnih podatkov za opravljanje nalog, ki jih *v javnem interesu* izvajajo institucije in organi Skupnosti, vključuje obdelavo osebnih podatkov, potrebnih za upravljanje in delovanje teh institucij in organov“. S to določbo se torej dovoljuje obdelava podatkov na podlagi „javne naloge“, ki se razlaga široko, v številnih primerih, ki bi jih sicer pokrivala podobna določba iz člena 7(f). Videonadzor prostorov iz varnostnih razlogov, elektronski nadzor prometa elektronskih sporočil ali ocenjevanje zaposlenih je le nekaj primerov, ki lahko spadajo na področje uporabe te široko razlagane določbe, ki se nanaša na „naloge, ki [se izvajajo] v javnem interesu“.

Za v prihodnje je tudi pomembno ugotoviti, da predlagana uredba zlasti v členu 6(1)(f) določa, da pravna podlaga, ki se nanaša na zakonite interese, „ne velja za obdelavo s strani javnih organov pri opravljanju njihovih nalog“. Če bo ta določba sprejeta in se bo razlagala široko, tako da bodo javni organi v celoti izključeni iz uporabe zakonitih interesov kot pravne podlage, potem bi bilo treba podlagi iz člena 7(e), ki se nanašata na „javni interes“ in „javno oblast“, razlagati tako, da javnim organom dovoljujeta neko stopnjo prožnosti, vsaj zato, da

[43] V tem smislu glej mnenje delovne skupine o SWIFT (navedeno v opombi 39), Mnenje 4/2003 o ravni varstva, zagotovljeni v Združenih državah za prenos podatkov o potnikih, ki ga je delovna skupina sprejela 13. junija 2003 (WP 78), in Delovni dokument o vprašanjih v zvezi z varstvom podatkov, povezanih s pravicami intelektualne lastnine, ki ga je delovna skupina sprejela 18. januarja 2005 (WP 104).

[44] Kot je bilo navedeno zgoraj, v nekaterih državah članicah (na primer na Švedskem) ugovor zoper obdelavo podatkov na podlagi člena 7(e) ni mogoč.

[45] Kot bo prikazano v nadaljevanju, so bili v osnutku poročila odbora LIBE predlagani dodatni zaščitni ukrepi – zlasti večja preglednost –, ko se uporablja člen 7(f).

[46] Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1).

zagotovijo svoje upravljanje in delovanje, kot se zdaj razlaga Uredba št. 45/2001.

Alternativno bi bilo mogoče navedeni zadnji stavek člena 6(1)(f) predlagane uredbe razlagati tako, da javnih organov ne izključuje v celoti iz uporabe zakonitih interesov kot pravne podlage. V tem primeru bi bilo treba izraz „obdelava s strani javnih organov pri opravljanju njihovih nalog“ v predlaganem členu 6(1)(f) razlagati ozko. Ta ozka razlaga bi pomenila, da bi obdelava podatkov za upravljanje in delovanje teh javnih organov izpadla s področja uporabe izraza „obdelava s strani javnih organov pri opravljanju njihovih nalog“. To bi povzročilo, da bi bila obdelava za upravljanje in delovanje teh javnih organov še vedno mogoča na podlagi zakonitih interesov.

III.3 Člen 7(f): zakoniti interesi

Člen 7(f)[47] zahteva test tehtanja: pretehtati je treba zakonite interese upravljavca (ali tretjih oseb) ter interese ali temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo. Rezultat testa tehtanja zlasti kaže, ali je člen 7(f) mogoče uporabiti kot pravno podlago za obdelavo.

Že tu je vredno omeniti, da to ni preprost test tehtanja, ki bi zajemal le medsebojno tehtanje dveh zlahka opredeljivih in primerljivih „uteži“. Pravzaprav, kot bo podrobneje opisano v nadaljevanju, izvajanje testa tehtanja lahko zahteva vsestransko oceno, pri kateri se upoštevajo številni dejavniki. Da bi pomagali strukturirati in poenostaviti oceno, smo proces razdelili na več korakov za zagotovitev učinkovite izvedbe testa tehtanja.

V oddelku III.3.1 bomo preučili eno stran tehtnice: kaj pomenijo „zakoniti interesi, za katere si prizadeva upravljavec ali tretja stranka, ki so ji osebni podatki posredovani“. V oddelku III.3.2 bomo preučili še drugo stran tehtnice: kaj pomenijo „interesi ali temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo, ki se varujejo na podlagi člena 1(1)“.

V oddelkih III.3.3 in III.3.4 so navedene smernice za izvajanje testa tehtanja. Oddelek III.3.3 vsebuje splošen uvod ob možnosti treh scenarijev. Po tem uvodu so v oddelku III.3.4 predstavljeni najpomembnejši razmisleki, ki jih je treba upoštevati pri izvajanju testa tehtanja, skupaj z zaščitnimi in drugimi ukrepi, ki jih določi upravljavec podatkov.

Nazadnje bomo v oddelkih III.3.5 in III.3.6 obravnavali nekaj posebnih mehanizmov, kot so odgovornost, preglednost in pravica do ugovora, ki lahko pomagajo zagotoviti – in dodatno okrepiti – ustrezno ravnovesje med interesi, ki se lahko pojavijo.

III.3.1 Zakoniti interesi upravljavca (ali tretje osebe)

Koncept „interesa“

Koncept „interesa“ je tesno povezan s konceptom „namena“ iz člena 6 Direktive, vendar se od njega razlikuje. V razpravi o varstvu podatkov je „namen“ poseben razlog za obdelavo

[47] Celotno besedilo člena 7(f) je navedeno na strani 4.

podatkov: cilj obdelave podatkov. Interes pa pomeni večje tveganje, ki ga lahko ima upravljavec pri obdelavi, ali korist, ki jo ima upravljavec – ali ki jo lahko ima družba – od obdelave.

Na primer, *v interesu* družbe je lahko, da se zagotovita zdravje in varnost njenih zaposlenih, ki delajo v jedrski elektrarni. V povezavi s tem je lahko *namen* družbe, da uvede posebne postopke za nadzor vstopa, ki upravičujejo obdelavo nekaterih natančno opredeljenih osebnih podatkov, ki pomaga pri zagotavljanju zdravja in varnosti zaposlenih.

Interes mora biti dovolj jasno izražen, da omogoči izvedbo testa tehtanja interesov in temeljnih pravic posameznika, na katerega se osebni podatki nanašajo. Še več, za zadevni interes si mora „prizadevati [tudi] upravljavec“. To zahteva dejanski in trenutni interes, nekaj, kar ustreza trenutnim dejavnostim ali koristim, ki se pričakujejo v bližnji prihodnosti. Z drugimi besedami, preveč nejasni ali spekulativni interesi ne bodo zadostovali.

Narava interesa se lahko spreminja. Nekateri interesi so lahko zanimivi in koristni za širšo družbo, kot je interes medijev za objavo informacij o vladni korupciji ali interes za opravljanje znanstvenih raziskav (ob upoštevanju ustreznih zaščitnih ukrepov). Drugi interesi so lahko za celotno družbo manj nujni ali je vsaj učinek njihovega uresničevanja na družbo bolj mešan ali sporen. Tak je lahko primer gospodarskega interesa družbe, da izve čim več o potencialnih kupcih, da lahko bolje usmerja oglaševanje svojih izdelkov ali storitev.

Zakaj je interes „zakonit“ ali „nezakonit“?

Namen tega vprašanje je ugotoviti, kdaj je interes zakonit. Če je interes upravljavca podatkov nezakonit, testa tehtanja ne bo treba opraviti, ker prvotni prag za uporabo člena 7(f) ne bo dosežen.

Po mnenju delovne skupine lahko pojem zakonitega interesa vključuje širok nabor interesov, bodisi trivialnih bodisi zelo nujnih, neposrednih ali bolj spornih. Šele v drugi fazi, ko je treba te interese tehtati glede na interese in temeljne pravice posameznikov, na katere se osebni podatki nanašajo, bi bilo treba uporabiti bolj omejen pristop in opraviti bolj vsebinsko analizo.

V nadaljevanju je naveden neizčrpen seznam nekaterih najobičajnejših okoliščin, v katerih se lahko postavi vprašanje zakonitega interesa v smislu člena 7(f). Naveden je, ne da bi to vplivalo na to, ali bodo po opravljenem tehtanju interesi upravljavca nazadnje prevladali nad interesi in pravicami posameznikov, na katere se osebni podatki nanašajo:

- uveljavljanje pravice do svobode izražanja ali obveščanja, tudi v medijih in umetnosti,
- tradicionalno neposredno trženje in druge oblike trženja ali oglaševanja,
- neželena nekomercialna sporočila, tudi v zvezi s političnimi kampanjami ali zbiranjem sredstev v dobrodelne namene,
- izvršba pravnih zahtevkov, vključno z izterjavo dolgov v zunajsodnih postopkih,
- preprečevanje goljufije, zlorabe storitev ali pranja denarja,
- nadzor zaposlenih zaradi varnosti ali upravljanja,
- sheme za prijavo nepravilnosti,
- fizična varnost, varnost informacijske tehnologije in spleta,
- obdelava za zgodovinske, znanstvene ali statistične namene,

- obdelava za namene raziskav (skupaj z tržnimi raziskavami).

Skladno s tem se interes lahko šteje za zakonit, dokler si lahko upravljavec prizadeva za ta interes v skladu z zakonom o varstvu podatkov in drugimi zakoni. Z drugimi besedami, zakoniti interes mora biti „sprejemljiv v skladu z zakonom“[48].

Da bi bil „zakoniti interes“ upošteven na podlagi člena 7(f), mora zato:

- biti zakonit (to je v skladu z veljavno zakonodajo EU in nacionalno zakonodajo);
- biti dovolj jasno izražen, da omogoči izvedbo testa tehtanja z interesi in temeljnimi pravicami posameznika, na katerega se osebni podatki nanašajo (to je dovolj natančno določen);
- pomeniti dejanski in trenutni interes (to je ne biti spekulativen).

Dejstvo, da ima upravljavec tak zakoniti interes pri obdelavi nekaterih podatkov, ne pomeni, da se lahko nujno opre na člen 7(f) kot pravno podlago za obdelavo. Zakonitost interesa upravljavca podatkov je le izhodišče, eden izmed elementov, ki jih je treba analizirati na podlagi člena 7(f). Ali se je mogoče opreti na člen 7(f), bo odvisno od rezultata testa tehtanja.

Za ponazoritev: upravljavci imajo lahko zakonit interes, da spoznajo preference svojih kupcev, da lahko bolje prilagodijo svojo ponudbo ter nazadnje ponudijo izdelke in storitve, ki bolj ustrezajo potrebam in željam kupcev. S tega vidika je lahko člen 7(f) ustrezna pravna podlaga, ki se lahko uporablja za nekatere vrste trženja na spletu in zunaj njega, če so vzpostavljeni ustrezni zaščitni ukrepi (med drugim učinkovit mehanizem, ki omogoča ugovore zoper tako obdelavo na podlagi člena 14(b), kot bo prikazano v oddelku III.3.6 z naslovom *Pravica do ugovora in več*).

Vendar to ne pomeni, da bi se upravljavci lahko opirali na člen 7(f), da bi neupravičeno nadzirali dejavnosti svojih kupcev na spletu in zunaj njega, kopičili ogromne količine podatkov o njih iz različnih virov, ki so se prvotno zbirali v drugih okvirih in za drugačne namene, ter oblikovali vsestranske profile osebnosti in preferenc kupcev brez njihove vednosti, učinkovitega sistema ugovora in še manj brez njihove informirane privolitve – ter na primer prek posrednikov podatkov trgovali s temi profili. Tako oblikovanje profilov lahko pomeni veliko poseganje v zasebnost kupca in če je tako, bi v tem primeru nad interesom upravljavca prevladali interesi in pravice posameznika, na katerega se osebni podatki nanašajo.[49]

[48] Ugotovitve o naravi „zakonitosti“ v oddelku III.1.3 Mnenja delovne skupine št. 3/2013 o omejitvi namena (navedeno v opombi 9) se smiselno uporabljajo tudi tu. Pojem „zakona“ je tako kot na straneh 19 in 20 navedenega mnenja uporabljen v najširšem pomenu. To zajema druge veljavne predpise, kot so predpisi o zaposlovanju, pogodbah ali varstvu potrošnikov. Poleg tega pojem zakona „zajema vse oblike napisanega in občega prava, primarno in sekundarno zakonodajo, občinske odloke, sodne primere, ustavna načela, temeljne pravice, druga pravna načela in tudi sodno prakso, saj bi pristojna sodišča tak ‚zakon‘ razlagala in upoštevala. V mejah zakona se lahko tudi drugi elementi, kot so običajne prakse, kodeksi ravnanja, etični kodeksi, pogodbeni dogovori ter splošni okvir in dejstva primera, upoštevajo pri ugotavljanju, ali je neki interes zakonit. To bo vključevalo naravo temeljnega razmerja med upravljavcem in posamezniki, na katere se osebni podatki nanašajo, ne glede na to, ali je komercialno ali drugačno.“ Poleg tega se to, kar se lahko šteje za zakonit interes, „lahko sčasoma tudi spreminja glede na znanstveni in tehnološki razvoj ter spremembe v družbi in kulturnih navadah“.

[49] Vprašanje sledilnih tehnologij in vloga privolitve iz člena 5(3) Direktive o zasebnosti in elektronskih komunikacijah se bosta obravnavala ločeno. Glej oddelek III.3.6(b) pod naslovom Primer: razvoj pristopa k neposrednemu trženju.

Drug primer: delovna skupina je v mnenju o SWIFT[50] ugotovila, da se ni mogoče opreti na člen 7(f), čeprav je priznala, da je upoštevanje sodnih pozivov na podlagi zakonodaje ZDA v zakonitem interesu družbe, da ji organi ZDA ne bi naložili sankcij. Delovna skupina je zlasti menila, da imajo zaradi daljnosežnih učinkov obdelave podatkov, ki se izvaja „na skrivaj, sistematično, v velikem obsegu in dolgoročno“, na posameznike „interesi za temeljne pravice in svoboščine številnih posameznikov, na katere se osebni podatki nanašajo, prednost pred interesi družbe SWIFT, da ji ZDA ne naložijo sankcij zaradi morebitnega neupoštevanja sodnih pozivov“.

Kot bo prikazano v nadaljevanju, če interes, za katerega si prizadeva upravljavec, ni nujen, je verjetneje, da bodo interesi in pravice posameznika, na katerega se osebni podatki nanašajo, prevladali nad zakonitimi – vendar manj pomembnimi – interesi upravljavca. Hkrati to ne pomeni, da manj nujni interesi upravljavca včasih ne morejo prevladati nad interesi in pravicami posameznikov, na katere se osebni podatki nanašajo: to se običajno zgodi, ko je učinek obdelave na posameznika, na katerega se osebni podatki nanašajo, prav tako manj pomemben.

Zakoniti interes v javnem sektorju

Trenutno besedilo Direktive ne izključuje posebej, da se upravljavci, ki so javni organi, pri obdelavi podatkov opirajo na člen 7(f) kot pravno podlago za obdelavo.[51]

Vendar je v predlagani uredbi[52] izključena ta možnost „obdelave s strani javnih organov pri opravljanju njihovih nalog“.

Predlagana zakonodajna sprememba poudarja pomen splošnega načela, da bi morali javni organi praviloma obdelovati podatke le pri izvajanju svojih nalog, če imajo za to ustrezno dovoljenje po zakonu. Upoštevanje tega načela je posebej pomembno – in jasno zahtevano s sodno prakso Evropskega sodišča za človekove pravice – v primerih, v katerih je ogrožena zasebnost posameznikov, na katere se osebni podatki nanašajo, in bi dejavnosti javnega organa posegale v tako zasebnost.

Dovolj *podrobno in natančno* dovoljenje po zakonu se zato zahteva – tudi v skladu z veljavno direktivo –, če obdelava s strani javnih organov posega v zasebnost posameznikov, na katere se osebni podatki nanašajo. Tako dovoljenje ima lahko obliko posebne zakonske obveznosti za obdelavo podatkov, ki lahko izpolnjuje zahteve iz člena 7(c), ali posebnega dovoljenja (ne pa nujno obveznosti) za obdelavo podatkov, ki lahko izpolnjuje zahteve iz člena 7(e) ali (f).[53]

---

[50] Glej oddelek 4.2.3 mnenja, že navedenega v opombi 39. Zakoniti interes upravljavca v tem primeru je bil povezan tudi z javnim interesom tretje države, ki ga ni mogoče zadovoljiti v skladu z Direktivo 95/46/ES.

[51] Prvotno je prvi predlog Komisije za direktivo posebej obravnaval obdelavo podatkov v zasebnem sektorju in obdelavo v javnem sektorju. To formalno razlikovanje med pravili, ki veljajo za javni oziroma zasebni sektor, je bilo v spremenjenem predlogu opuščeno. To je lahko omogočilo tudi različno razlago in uporabo v državah članicah.

[52] Glej člen 6(1)(f) predlagane uredbe.

[53] V zvezi s tem glej tudi oddelek III.2.5 zgoraj o javnih nalogah (strani 21–23) in razpravo v nadaljevanju pod naslovom *Zakoniti interesi tretjih oseb* (strani 27 in 28). Glej tudi razmisleke o mejah „zasebnega izvrševanja“ zakona na strani 35 pod naslovom *Javni interesi/interesi širše skupnosti*. V vseh teh primerih je posebej pomembno zagotoviti, da se v celoti upoštevajo omejitve iz člena 7(f) in člena 7(e).

Zakoniti interesi tretjih oseb

Veljavno besedilo Direktive se ne sklicuje le na „zakonite interese, za katere si prizadeva upravljavec“, ampak dovoljuje uporabo člena 7(f) tudi, ko si za zakonite interese prizadeva „tretja stranka ali stranke, ki so jim osebni podatki posredovani“.[54] Naslednji primeri ponazarjajo nekatere okoliščine, v katerih se ta določba lahko uporablja.

Objava podatkov zaradi preglednosti in odgovornosti Pomemben okvir, v katerem je lahko člen 7(f) upošteven, je objava podatkov zaradi preglednosti in odgovornosti (na primer plače najvišjih vodstvenih delavcev v družbi). V tem primeru se lahko šteje, da se podatki ne razkrijejo javnosti predvsem v interesu upravljavca, ki objavi podatke, ampak bolj v interesu drugih deležnikov, kot so zaposleni ali novinarji ali splošna javnost, ki se jim podatki razkrijejo.

Z vidika varstva podatkov in zasebnosti ter zaradi zagotovitve pravne gotovosti na splošno je priporočljivo, da se zasebni podatki javnosti razkrijejo na podlagi zakona, ki dovoljuje in – kadar je primerno – jasno določa podatke, ki naj se objavijo, namene objave in vse potrebne zaščitne ukrepe.[55] To tudi pomeni, da je lahko bolje, da se kot pravna podlaga, ko se zasebni podatki razkrijejo zaradi preglednosti in odgovornosti, uporablja člen 7(c), in ne člen 7(f).[56].

Vendar bi bilo ob neobstoju posebne zakonske obveznosti ali dovoljenja za objavo podatkov vseeno mogoče osebne podatke posredovati ustreznim deležnikom. V ustreznih primerih bi bilo mogoče tudi objaviti podatke zaradi preglednosti in odgovornosti.

V obeh primerih – to je ne glede na to, ali se osebni podatki razkrijejo na podlagi zakona, ki to dovoljuje, ali ne – je razkritje neposredno odvisno od rezultata testa tehtanja iz člena 7(f) ter izvajanja ustreznih zaščitnih in drugih ukrepov.[57]

Poleg tega je lahko zaželena tudi nadaljnja uporaba za večjo preglednost že objavljenih osebnih podatkov (na primer ponovna objava podatkov v tisku ali nadaljnje širjenje prvotno objavljenega podatkovnega niza na bolj inovativen ali uporabniku prijazen način s strani

[54] Namen predlagane uredbe je omejiti uporabo te podlage na „zakonite interese, za katere si prizadeva upravljavec“. Iz besedila ni jasno, ali predlagana ubeseditev pomeni le poenostavitev besedila ali pa je njen namen izključiti primere, v katerih lahko upravljavec posreduje podatke na podlagi zakonitih interesov drugih. To besedilo vendarle ni dokončno. Interes tretjih oseb je bil na primer znova uveden v končnem poročilu odbora LIBE ob glasovanju odbora LIBE Evropskega parlamenta o dogovorjenih predlogih sprememb 21. oktobra 2013. Glej predlog spremembe 100, ki zadeva člen 6. Delovna skupina podpira ponovno uvedbo tretjih oseb v predlog, ker je njegova uporaba lahko še naprej ustrezna v nekaterih primerih, tudi v primerih, opisanih v nadaljevanju.

[55] Priporočilo glede dobre prakse ne bi smelo posegati v nacionalna pravna pravila o preglednosti in dostopu javnosti do dokumentov.

[56] V nekaterih državah članicah je pravzaprav treba izpolnjevati različna pravila v zvezi z obdelavo, ki jo izvajajo javne ali zasebne osebe. Na primer, v skladu z italijanskim zakonom o varstvu podatkov je javnemu organu dovoljeno širiti osebne podatke le, če je to določeno z zakonom ali uredbo (oddelek 19.3).

[57] Kot je delovna skupina pojasnila v Mnenju št. 06/2013 o odprtih podatkih (glej stran 9 tega mnenja, navedenega v opombi 88 spodaj), mora vsaka nacionalna praksa ali nacionalna zakonodaja o preglednosti „upoštevati člen 8 [EKČP] ter člena 7 in 8 Listine EU. Kot je Evropsko sodišče razsodilo v zadevah *Österreichischer Rundfunk* in *Schecke*, to pomeni, da je treba preveriti, ali je razkritje potrebno za legitimni cilj, ki mu sledi zakon, in je sorazmerno z njim“. Glej sodbi Sodišča z dne 20. maja 2003 v združenih zadevah Rundfunk (C-465/00, C-138/01 in C-139/01) in z dne 9. novembra 2010 v združenih zadevah Volker in Markus Schecke (C-92/09 in C-93/09).

nevladne organizacije). Možnost take ponovne objave in uporabe bo odvisna tudi od rezultata testa tehtanja, pri katerem bi bilo treba med drugim upoštevati naravo informacij in učinek ponovne objave ali uporabe na posameznike.[58]

Zgodovinske ali druge vrste znanstvenih raziskav Drug pomemben okvir, v katerem je lahko upoštevno razkritje v zakonitem interesu tretjih oseb, so zgodovinske ali druge vrste znanstvenih raziskav, zlasti kadar se zahteva dostop do nekaterih podatkovnih zbirk. Take dejavnosti so v Direktivi posebej priznane, ob upoštevanju ustreznih zaščitnih in drugih ukrepov,[59] vendar ne bi smeli pozabiti, da bo pravna podlaga za te dejavnosti pogosto dobro premišljena uporaba člena 7(f).[60]

Splošni javni interes ali interes tretje osebe Nazadnje, zakoniti interesi tretjih oseb so lahko upoštevni tudi drugače. Tak je primer, v katerem si upravljavec – ki ga včasih spodbudijo javni organi – prizadeva za interes, ki ustreza splošnemu javnemu interesu ali interesu tretje osebe. To lahko zajema primere, v katerih upravljavec preseže posebne zakonske obveznosti, določene v zakonih in drugih predpisih, da bi pomagal organom kazenskega pregona ali zasebnim deležnikom v njihovem prizadevanju za preprečevanje nezakonitih dejavnosti, kot so pranje denarja, navezovanje stikov z otroki za namene spolne zlorabe ali nezakonita souporaba datotek na spletu. Vendar je v teh primerih posebej pomembno zagotoviti, da se v celoti upoštevajo omejitve iz člena 7(f).[61]

Obdelava mora biti potrebna za predviden(-e) namen(-e)

Nazadnje, obdelava osebnih podatkov mora biti tudi „potrebna zaradi zakonitih interesov“, za katere si prizadeva upravljavec ali – v primeru razkritja – tretja oseba. Ta pogoj dopolnjuje zahtevo nujnosti iz člena 6 in zahteva povezavo med obdelavo in zadevnimi interesi. Ta zahteva „nujnosti“ se uporablja v vseh primerih, navedenih v točkah (b) do (f) člena 7, vendar je posebej upoštevna v primeru točke (f) za zagotovitev, da obdelava podatkov na podlagi zakonitih interesov ne bo privedla do neupravičene široke razlage nujnosti obdelave podatkov. V vseh drugih primerih to pomeni, da bi bilo treba ugotoviti, ali so za dosego istega cilja na voljo manj invazivna sredstva.

III.3.2 Interesi ali pravice posameznika, na katerega se osebni podatki nanašajo

Interesi <u>ali</u> pravice (namesto interesi <u>za</u> pravice)

[58] Tu je pomemben dejavnik tudi omejitev namena. Delovna skupina iz člena 29 je na strani 20 Mnenja št. 06/2013 o odprtih podatkih (navedeno v opombi 88 spodaj) priporočila, „da vsaka zakonodaja, ki poziva k javni dostopnosti podatkov, jasno določi namene za razkritje osebnih podatkov. Če se ti ne določijo ali se določijo le z uporabo nejasnih in splošnih pojmov, se bosta pravna varnost in predvidljivost zmanjšali. V zvezi s kakršnimi koli zahtevami za ponovno uporabo bodo organi javnega sektorja in zadevni potencialni ponovni uporabniki predvsem težko ugotovili, kateri so prvotni nameni objave, in nato določili, kateri nadaljnji nameni so združljivi s temi prvotnimi nameni. Kot je bilo že omenjeno, se tudi v primeru, da so osebni podatki objavljeni na internetu, ne sme predpostavljati, da se jih lahko obdeluje za kakršne koli namene.“

[59] Glej na primer člen 6(1)(b) in (e).

[60] Kot je delovna skupina pojasnila v Mnenju št. 3/2013 o omejitvi namena (navedeno v opombi 9), mora biti nadaljnja uporaba podatkov za druge namene odvisna od dvojnega testa. Prvič, zagotoviti je treba, da se bodo podatki uporabili za namene, združljive z zakonodajo. Drugič, zagotoviti je treba, da bo obstajala ustrezna pravna podlaga za obdelavo iz člena 7.

[61] V zvezi s tem glej na primer Delovni dokument o vprašanjih varstva podatkov, povezanih s pravicami intelektualne lastnine, ki ga je delovna skupina sprejela 18. januarja 2005 (WP 104).

Člen 7(f) Direktive se nanaša na „[interese za] temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo, ki se varujejo na podlagi člena 1(1)“.

Vendar je delovna skupina pri primerjavi jezikovnih različic Direktive ugotovila, da je bil izraz „interests for“ („interesi za“) v druge ključne jezike, ki so se uporabljali v času pogajanj o besedilu, preveden kot „interests or“ („interesi ali“).[62]

Nadaljnja analiza kaže, da je angleška različica Direktive le rezultat napačnega zapisa: „or“ je bil pomotoma zapisan kot „for“.[63] Besedilo bi se tako moralo pravilno glasiti „interests or fundamental rights and freedoms“ („interesi ali temeljne pravice in svoboščine“).

„Interese“ in „pravice“ je treba razlagati široko

Navedba „interesov ali temeljnih pravic in svoboščin“ ima neposreden učinek na področje uporabe določbe. Zagotavlja večje varstvo za posameznika, na katerega se osebni podatki nanašajo, saj predvsem zahteva, da se upoštevajo tudi „interesi“ posameznikov, na katere se osebni podatki nanašajo, ne le njihove temeljne pravice in svoboščine. Vendar zato ni treba domnevati, da se omejitev v členu 7(f) na temeljne pravice, „ki se varujejo na podlagi člena 1(1)“ – in tako izrecno sklicevanje na namen Direktive[64] –, ne bi uporabljala tudi za izraz „interesi“. Kljub temu je jasno, da je treba upoštevati vse ustrezne interese posameznika, na katerega se osebni podatki nanašajo.

Ta razlaga besedila je smiselna ne le z vidika slovnice, ampak tudi ob upoštevanju široke razlage pojma „zakonitih interesov“ upravljavca. Če si lahko upravljavec – ali tretja oseba v primeru posredovanja podatkov – prizadeva za katere koli interese, pod pogojem, da niso nezakoniti, bi moral biti tudi posameznik, na katerega se osebni podatki nanašajo, upravičen do tega, da se vse kategorije interesov upoštevajo in tehtajo z interesi upravljavca, dokler so pomembni v okviru področja uporabe Direktive.

V času čedalje večjega neravnovesja „informacijske moči“, ko vlade in podjetja kopičijo do zdaj nezaslišane količine podatkov o posameznikih in čedalje bolj zmorejo zbirati podrobne profile, ki bodo napovedovali njihovo vedenje (kar bo okrepilo informacijsko neravnovesje in zmanjšalo njihovo neodvisnost), je še toliko bolj pomembno zagotoviti, da se zaščitijo interesi posameznikov za varovanje njihove zasebnosti in neodvisnosti.

[62] Na primer „l'intérêt ou les droits et libertés fondamentaux de la personne concernée“ v francoščini, „l'interesse o i diritti e le libertà fondamentali della persona interessata“ v italijanščini in „das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person“ v nemščini.

[63] Delovna skupina ugotavlja, da bi se morala angleška različica slovnično pravilno glasiti „interests in“ namesto „interests for“, če je bilo to mišljeno. Poleg tega se zdi, da je besedna zveza „interests for“ oziroma „interests in“ odveč predvsem zato, ker bi morala navedba „temeljne pravice in svoboščine“ običajno zadostovati, če je bilo to mišljeno. Razlago glede napačnega zapisa potrjuje še dejstvo, da tudi Svet v Skupnem stališču (ES) št. 1/95, ki ga je sprejel 20. februarja 1995, omenja „interese ali temeljne pravice in svoboščine“. Nazadnje, delovna skupina ugotavlja še, da je Komisija v predlagani uredbi nameravala popraviti ta napačen zapis: Člen 6(1)(f) se nanaša na „[interese ali] temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo“, in ne na „interese za“ take pravice.

[64] Glej člen 1(1): „V skladu s to direktivo države članice varujejo temeljne pravice in svoboščine fizičnih oseb in predvsem njihovo pravico do zasebnosti pri obdelavi osebnih podatkov.“

Nazadnje, pomembno je ugotoviti, da se drugače kot v primeru interesov upravljavca pridevnik „zakonit“ ne uporablja pred izrazom „interesi“ posameznikov, na katere se osebni podatki nanašajo. To pomeni širše področje uporabe za varstvo posameznikovih interesov in pravic. Tudi posamezniki, ki sodelujejo v nezakonitih dejavnostih, ne bi smeli biti deležni nesorazmernega poseganja v svoje pravice in interese.[65] Na primer, interesi posameznika, ki bi lahko zagrešil tatvino v supermarketu, bi še vedno lahko prevladali nad interesom lastnika trgovine, da njegovo sliko in zasebni naslov objavi na stenah supermarketa in/ali na spletu.

III.3.3 Uvod v izvajanje testa tehtanja

Koristno si je predstavljati tako zakonite interese upravljavca kot učinek na interese in pravice posameznika, na katerega se osebni podatki nanašajo. Zakoniti interesi lahko segajo od nepomembnih prek nekoliko pomembnih do nujnih. Podobno je lahko učinek na interese in pravice posameznika, na katerega se osebni podatki nanašajo, bolj ali manj pomemben ter lahko sega od nepomembnega do zelo resnega.

Kadar so zakoniti interesi upravljavca manj pomembni in ne zelo nujni, lahko na splošno prevladajo nad interesi in pravicami posameznika, na katerega se osebni podatki nanašajo, le v primerih, v katerih je učinek na te interese in pravice še manjši. Po drugi strani lahko pomembni in nujni zakoniti interesi v nekaterih primerih in ob upoštevanju zaščitnih in drugih ukrepov upravičijo celo veliko poseganje v zasebnost ali druge velike učinke na interese ali pravice posameznikov, na katere se osebni podatki nanašajo.[66]

Pri tem je pomembno poudariti posebno nalogo, ki jo lahko imajo zaščitni ukrepi[67] pri zmanjšanju neupravičenega učinka na posameznike, na katere se osebni podatki nanašajo, in s tem pri takem spreminjanju ravnovesja pravic in interesov, da ne bo nič prevladalo nad zakonitimi interesi upravljavca podatkov. Samo uporaba zaščitnih ukrepov seveda ni dovolj za utemeljitev kakršne koli obdelave v vseh okoliščinah. Poleg tega morajo biti zadevni zaščitni ukrepi ustrezni in zadostni ter morajo nesporno in pomembno zmanjšati učinke na posameznike, na katere se osebni podatki nanašajo.

---

[65] Seveda sta lahko ena od posledic kriminala zbiranje in morebitna objava osebnih podatkov zločincev in osumljencev. Vendar morajo za to veljati strogi pogoji in zaščitni ukrepi.

[66] Za ponazoritev glej sklepanje delovne skupine v več mnenjih in delovnih dokumentih:
– Mnenje 4/2006 o Obvestilu o predlagani pripravi predpisa Ministrstva za zdravje in socialne zadeve ZDA o nadzoru nalezljivih bolezni in zbiranju podatkov o potnikih z dne 20. novembra 2005 (Nadzor nalezljivih bolezni, predlog, 42 CFR, del 70 in del 71), sprejeto 14. junija 2006 (WP 121), ko gre za posebne in resne grožnje za javno zdravje;
– Mnenje 1/2006 o shemah za prijavo nepravilnosti (navedeno v opombi 39), v katerem je resnost domnevne kršitve eden izmed elementov testa tehtanja;
– Delovni dokument o nadzoru elektronskih komunikacij na delovnem mestu, sprejet 29. maja 2002 (WP 55), v katerem je delovna skupina tehtala pravico delodajalca do učinkovitega poslovanja in človekovo dostojanstvo delavca ter zaupnost korespondence.

[67] Zaščitni ukrepi lahko med drugim zajemajo stroge omejitve o količini podatkov, ki se zbirajo, takojšen izbris podatkov po uporabi, tehnične in organizacijske ukrepe za zagotovitev funkcionalne ločitve, ustrezno uporabo tehnik anonimizacije, združevanje podatkov, tehnologije za boljše varovanje zasebnosti ter tudi večjo preglednost, odgovornost in možnost zavrnitve obdelave. Glej tudi oddelek III.3.4(d) in nadaljevanje.

Uvodni scenariji

Pred zagotovitvijo smernic za izvajanje testa tehtanja so lahko naslednji trije uvodni scenariji prvi prikaz, kakšno je lahko tehtanje interesov in pravic v resničnem življenju. Vsi trije primeri temeljijo na preprostem in nedolžnem scenariju, ki se začne s posebno ponudbo italijanske hrane za s sabo. Postopoma se uvajajo novi elementi, ki kažejo, kako se tehtnica nagiba, ko se povečuje učinek na posameznike, na katere se osebni podatki nanašajo.

Scenarij 1: posebna ponudba verige picerij

Klavdija naroči pico prek mobilne aplikacije na pametnem telefonu, vendar ne zavrne trženja na spletni strani. Njen naslov in podatki o kreditni kartici se shranijo za dostavo. Klavdija nekaj dni pozneje v domačem poštnem nabiralniku od verige picerij prejme kupone za popust za podobne izdelke.

Kratka analiza: veriga picerij ima zakonit, vendar ne posebno nujen interes, da poskuša svojim strankam prodati več izdelkov. Nasprotno se ne zdi, da to pomeni posebno veliko poseganje v Klavdijino zasebnost ali drug neupravičen učinek na njene interese in pravice. Podatki in okoliščine so razmeroma nedolžni (uživanje pice). Veriga picerij je uvedla nekaj zaščitnih ukrepov: uporabijo se samo razmeroma omejene informacije (kontaktni podatki) in kuponi se pošljejo po navadni pošti. Poleg tega je ponujena preprosta možnost za zavrnitev trženja na spletni strani.

V celoti gledano in tudi ob upoštevanju vzpostavljenih zaščitnih in drugih ukrepov (skupaj s preprostim orodjem za zavrnitev) se zdi, da interesi in pravice posameznice, na katero se osebni podatki nanašajo, niso prevladali nad zakonitimi interesi verige picerij, da izvede to minimalno obdelavo podatkov.

Scenarij 2: ciljno oglaševanje za isto posebno ponudbo

Okoliščine so iste, vendar tokrat veriga picerij ne shrani le Klavdijinega naslova in podatkov o kreditni kartici, ampak tudi njeno novejšo zgodovino naročil (za zadnja tri leta). Poleg tega je zgodovina nakupov povezana s podatki iz supermarketa, v katerem Klavdija nakupuje na spletu in ki ga upravlja ista družba, ki vodi verigo picerij. Klavdija od verige picerij prejema posebne ponudbe in ciljne oglase na podlagi zgodovine njenih naročil za dve povsem različni storitvi. Oglase in posebne ponudbe prejema na spletu in zunaj njega, po navadni pošti, elektronski pošti ter z objavo na spletni strani družbe in spletnih straneh nekaterih izbranih partnerjev (ko dostopa do teh strani na svojem računalniku ali prek mobilnega telefona). Sledi se tudi njeni zgodovini brskanja (toku klikov). Prek njenega mobilnega telefona se sledi tudi podatkom o njeni lokaciji. Programska oprema za analizo podatkov obdela podatke in napove njene preference, tudi čas in kraj, ko bo najverjetneje opravila večji nakup, pripravljena plačati višjo ceno, dovzetna za vpliv posebnega popusta ali ko si bo močno želela najljubše sladice ali pripravljene obroke.[68] Klavdijo zelo jezijo vztrajni oglasi, ki se pojavljajo na njenem mobilnem telefonu, ko preverja vozni red avtobusov na poti domov, in ki oglašujejo najnovejše ponudbe hrane za s sabo, ki se ji poskuša upreti. Ni mogla najti uporabnikom prijazne informacije ali preprostega načina za izklop teh oglasov, čeprav družba trdi, da obstaja sistem zavrnitve za celotno panogo. Presenetilo jo je tudi, da ni več prejemala posebnih ponudb, ko se je preselila v manj bogato sosesko. Zaradi tega se je njen mesečni račun za prehrano povečal za približno 10 %. Prijatelj, ki bolje obvlada tehnologijo, ji je na spletnem blogu pokazal nekaj špekulacij, da je supermarket zaračunaval več za naročila iz „slabih sosesk“ zaradi statistično večjega tveganja goljufije s kreditnimi karticami v takih primerih. Družba tega ni komentirala in je trdila, da sta njena politika glede popustov in algoritem, ki ga uporablja za določitev cen, njena last in ju ni mogoče razkriti.

Kratka analiza: podatki in okoliščine ostajajo razmeroma nedolžni. Vendar so obseg zbiranja podatkov in tehnike, uporabljene za prepričevanje Klavdije (skupaj z različnimi tehnikami sledenja, napovedovanja časa in kraja, ko hrepeni po hrani, in dejstvom, da Klavdija takrat najverjetneje podleže skušnjavi), dejavniki, ki jih je treba upoštevati pri oceni učinka obdelave. Pomanjkljiva preglednost logike obdelave podatkov te družbe, ki je lahko dejansko privedla do cenovne diskriminacije na podlagi lokacije oddaje naročila, in velik potencialni finančni učinek na potrošnike nazadnje prevesita tehtnico celo v razmeroma nedolžnem kontekstu hrane za s sabo in nakupovanja živil. Namesto le ponujanja možnosti zavrnitve tovrstnega oblikovanja profilov in ciljnega oglaševanja bi bila potrebna informirana privolitev v skladu s členom 7(a) in v skladu s členom 5(3) Direktive o zasebnosti in elektronskih komunikacijah. Zato se člen 7(f) ne sme uporabiti kot pravna podlaga za obdelavo.

[68] Glej na primer http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-boards: *„Novejše raziskave kažejo, da je moč volje omejen vir, ki ga je sčasoma mogoče izčrpati ali obnoviti.[10] Predstavljajte si, da potrošnica zaradi zaskrbljenosti zaradi debelosti poskuša vztrajati brez najljubše malovredne hrane. Izkaže se, da včasih in ponekod tega ne more. Obsežni podatki trgovcem pomagajo natančno razumeti, kako in kdaj naj se približajo tej potrošnici, ko je najbolj ranljiva – zlasti v svetu stalnega preživljanja časa pred zaslonom, ko so celo naše naprave sposobne nagovarjanja k nakupu.“*

Scenarij 3: uporaba naročil hrane za prilagoditev premij zdravstvenega zavarovanja

Veriga je Klavdijine navade glede uživanja pic, skupaj s časom in naravo naročil hrane, prodala zavarovalnici, ki jih uporablja za prilagoditev svojih premij zdravstvenega zavarovanja.

Kratka analiza: zdravstvena zavarovalnica ima lahko zakonit interes – kolikor to dovoljujejo veljavni predpisi – za ocenjevanje zdravstvenih tveganj svojih strank in zaračuna različne premije glede na različna tveganja. Vendar sta način zbiranja podatkov in obseg zbiranja podatkov pretirana. Razumna oseba v Klavdijinem položaju verjetno ne bi pričakovala, da bi se informacije o njenem uživanju pic uporabile za izračun njenih premij zdravstvenega zavarovanja.

Poleg pretiranosti oblikovanja profilov in možnih nepravilnih sklepanj (pica bi lahko bila naročena za koga drugega) sklepanje o občutljivih podatkih (podatki o zdravju) iz navidezno neškodljivih podatkov (naročila hrane za s sabo) prispeva k temu, da se tehtnica prevesi v korist interesov in pravic posameznice, na katero se osebni podatki nanašajo. Nazadnje, obdelava ima tudi velik finančni učinek nanjo.

V celoti gledano v tem posebnem primeru interesi in pravice posameznice, na katero se osebni podatki nanašajo, prevladajo nad zakonitimi interesi zdravstvene zavarovalnice. Zato se člen 7(f) ne sme uporabiti kot pravna podlaga za obdelavo. Vprašljivo je tudi, ali se lahko glede na pretiran obseg zbiranja podatkov in mogoče tudi zaradi dodatnih posebnih omejitev v nacionalni zakonodaji kot pravna podlaga uporabi člen 7(a).

Zgornji scenariji in možna uvedba različic z drugimi elementi poudarjajo potrebo po omejenem številu ključnih dejavnikov, ki lahko pomagajo pri nastavitvi ocene, ter potrebo po pragmatičnem pristopu, ki dovoljuje uporabo praktičnih domnev („izkustveno pravilo“), ki temeljijo predvsem na tem, kaj bi se razumni osebi zdelo sprejemljivo v zadevnih okoliščinah („razumna pričakovanja“), in na posledicah obdelave podatkov za posameznika, na katerega se osebni podatki nanašajo („učinek“).

III.3.4 Ključni dejavniki, ki se upoštevajo pri izvajanju testa tehtanja

Države članice so razvile številne uporabne dejavnike, ki jih je treba upoštevati pri izvajanju testa tehtanja. Ti dejavniki so v tem oddelku obravnavani pod štirimi glavnimi naslovi: (a) ocena zakonitega interesa upravljavca, (b) učinek na posameznike, na katere se osebni podatki nanašajo, (c) začasno ravnovesje in (d) dodatni zaščitni ukrepi, ki jih upravljavec uporablja za preprečevanje neupravičenega učinka na posameznike, na katere se osebni podatki nanašajo.[69]

Pri izvajanju testa tehtanja je zelo pomembno upoštevati naravo in vir zakonitih interesov na eni strani ter učinke na posameznike, na katere se osebni podatki nanašajo, na drugi strani. Ta ocena bi morala že vključevati ukrepe, ki jih namerava upravljavec sprejeti za uskladitev z Direktivo (na primer za zagotovitev omejitve namena in sorazmernosti v skladu s členom 6 ali

[69] Nekatera posebna vprašanja, povezana z zaščitnimi ukrepi, bodo zaradi pomembnosti dodatno obravnavana pod ločenimi naslovi v oddelkih III.3.5 in III.3.6.

za zagotovitev informacij posameznikom, na katere se osebni podatki nanašajo, v skladu s členoma 10 in 11).

Po analizi in tehtanju obeh strani je mogoče določiti začasno „ravnovesje“. Kadar rezultat ocene še vedno vzbuja dvom, je treba oceniti še, ali lahko dodatni zaščitni ukrepi, ki posamezniku, na katerega se osebni podatki nanašajo, zagotavljajo večje varstvo, prevesijo tehtnico tako, da bi bila obdelava upravičena.

(a) Ocena zakonitih interesov upravljavca

Čeprav je pojem zakonitih interesov precej širok, kot je pojasnjeno v oddelku III.3.1 zgoraj, je pri tehtanju med temi interesi ter pravicami in interesi posameznikov, na katere se osebni podatki nanašajo, ključna narava teh interesov. Čeprav ni mogoče sprejeti vrednostnih sodb glede na vse možne zakonite interese, je mogoče zagotoviti nekaj smernic. Kot je bilo že navedeno, lahko taki interesi segajo od povsem nepomembnih do nujnih in so lahko neposredni ali bolj sporni.

(i) Uveljavljanje temeljne pravice

Med temeljnimi pravicami in svoboščinami, potrjenimi v Listini Evropske unije o temeljnih pravicah (v nadaljnjem besedilu: Listina)[70] in Evropski konvenciji o človekovih pravicah (v nadaljnjem besedilu: EKČP), jih je lahko nekaj v nasprotju s pravico do zasebnosti in pravico do varstva osebnih podatkov, kot so svoboda izražanja in obveščanja[71], svoboda umetnosti in znanosti[72], pravica dostopa do dokumentov[73] ter na primer tudi pravica do svobode in varnosti[74], svoboda misli, vesti in vere[75], svoboda gospodarske pobude[76], lastninska pravica[77], pravica do učinkovitega pravnega sredstva in nepristranskega sodišča[78] ali domneva nedolžnosti in pravica do obrambe[79].

Da bi prevladal zakoniti interes upravljavca, mora biti obdelava podatkov „potrebna“ in „sorazmerna“, da se lahko uveljavlja zadevna temeljna pravica.

Za ponazoritev, glede na dejstva primera je lahko potrebno in sorazmerno, da časopis objavi nekatere obremenilne podrobnosti o nakupovalnih navadah visokega vladnega uradnika, vpletenega v domnevni korupcijski škandal. Nasprotno pa mediji ne bi smeli imeti splošnega dovoljenja za objavo katere koli in vseh nepomembnih podrobnosti iz zasebnega življenja javnih osebnosti. V teh in podobnih primerih se običajno postavljajo vsestranska vprašanja

[70] Določbe Listine se uporabljajo za institucije in organe EU ob spoštovanju načela subsidiarnosti, za nacionalne organe pa samo, ko izvajajo pravo Unije.
[71] Člen 11 Listine in člen 10 EKČP.
[72] Člen 13 Listine ter člena 9 in 10 EKČP.
[73] Člen 42 Listine. „Vsak državljan Unije in vsaka fizična ali pravna oseba s prebivališčem ali statutarnim sedežem v eni od držav članic ima pravico dostopa do dokumentov Evropskega parlamenta, Sveta in Komisije.“ Podobne pravice do dostopa obstajajo v številnih državah članicah za dokumente, ki jih javni organi hranijo v teh državah članicah.
[74] Člen 6 Listine in člen 5 EKČP.
[75] Člen 10 Listine in člen 9 EKČP.
[76] Člen 16 Listine.
[77] Člen 17 Listine ter člen 1 Protokola št. 1 k EKČP.
[78] Člen 47 Listine in člen 6 EKČP.
[79] Člen 48 Listine ter člena 6 in 13 EKČP.

glede ocene, za pomoč pri presoji pa imajo lahko pomembno vlogo posebna zakonodaja, sodna praksa, smernice, kodeksi ravnanja ter drugi formalni ali manj formalni standardi.[80]

Kadar je primerno, so lahko zaščitni ukrepi tudi v tem okviru pomembni in pomagajo pri ugotavljanju, v katero smer je treba nagniti – včasih krhko – ravnovesje.

(ii) Javni interesi/interesi širše skupnosti

V nekaterih primerih se lahko upravljavec želi sklicevati na javni interes ali interes širše skupnosti (ne glede na to, ali je to določeno v nacionalnih zakonih in drugih predpisih). Na primer, dobrodelna organizacija lahko obdeluje osebne podatke za namene zdravstvenih raziskav, neprofitna organizacija pa za ozaveščanje o vladni korupciji.

Lahko se tudi zgodi, da se zasebni poslovni interes družbe do določene mere ujema z javnim interesom. Tako je lahko na primer pri preprečevanju finančne goljufije ali drugih zlorab storitev.[81] Ponudnik storitev ima lahko zakonit poslovni interes za zagotovitev, da njegove stranke ne bodo zlorabljale storitve (ali da ne bodo mogle dobiti storitve brez plačila), medtem ko imajo stranke družbe, davčni zavezanci in širša javnost prav tako zakonit interes, da se zagotavljata odvračanje od goljufivih dejavnosti in njihovo odkrivanje, ko se zgodijo.

Na splošno to, da upravljavec ne ravna le v svojem zakonitem interesu (na primer poslovnem interesu), ampak tudi v interesu širše skupnosti, lahko da temu interesu večjo težo. Kolikor bolj je javni interes ali interes širše skupnosti nujen ter kolikor bolj skupnost in posamezniki, na katere se osebni podatki nanašajo, jasno priznavajo in pričakujejo, da lahko upravljavec ravna in obdeluje podatke v prizadevanju za te interese, težji je ta zakoniti interes na tehtnici.

Po eni strani se „zasebno izvrševanje“ zakonov ne sme uporabljati za upravičenje vsiljivih praks, ki bi bile, če bi jih izvajala vladna organizacija, prepovedane v skladu s sodno prakso Evropskega sodišča za človekove pravice, ker bi dejavnosti javnega organa posegale v zasebnost posameznikov, na katere se osebni podatki nanašajo, ne da bi bil izpolnjen strog test na podlagi člena 8(2) EKČP.

(iii) Drugi zakoniti interesi

V nekaterih primerih, kot je bilo že omenjeno v oddelku III.2, je lahko kontekst, v katerem se pojavi zakonit interes, podoben enemu od kontekstov, v katerih se lahko uporabijo katere izmed drugih pravnih podlag, zlasti pravne podlage iz točk (b) (pogodba), (c) (zakonska obveznost) ali (e) (naloga v javnem interesu) člena 7. Na primer, obdelava podatkov lahko ni nujno potrebna, vendar je lahko še vedno pomembna za izvajanje pogodbe – ali pa zakon lahko le dovoljuje obdelavo nekaterih podatkov, vendar je ne zahteva. Kot smo lahko videli,

[80] Glede na merila, ki jih je treba uporabljati v primerih, ki zadevajo svobodo izražanja, koristne smernice zagotavlja tudi sodna praksa Evropskega sodišča za človekove pravice. Glej na primer sodbo ESČP z dne 7. februarja 2012 v zadevi von Hannover proti Nemčiji (št. 2), zlasti točke 95 do 126. Treba je tudi upoštevati, da je s členom 9 Direktive (z naslovom *Obdelava osebnih podatkov in svoboda izražanja*) državam članicam dovoljeno, da „določijo izjeme ali odstopanja od določb tega poglavja, poglavja IV in poglavja VI za obdelavo osebnih podatkov, ki se izvaja zgolj v novinarske namene ali zaradi umetniškega ali literarnega izražanja samo, če so potrebna za uskladitev pravice do zasebnosti s predpisi, ki urejajo svobodo izražanja“.

[81] Glej na primer Primer 21: Podatki o pametnem merjenju, uporabljeni za odkrivanje zlorabe energije na strani 67 Mnenja delovne skupine št. 3/2013 o omejitvi namena (navedeno v opombi 9).

ni vedno preprosto potegniti jasne ločnice med podlagami, vendar je zato toliko bolj pomembno, da se v analizo vključi test tehtanja iz člena 7(f).

Tudi v tem in v vseh drugih možnih primerih, ki do zdaj niso bili omenjeni, kolikor bolj je interes upravljavca nujen in kolikor bolj jasno širša skupnost priznava in pričakuje, da lahko upravljavec ravna in obdeluje podatke v prizadevanju za ta interes, težji je ta zakoniti interes na tehtnici.[82] To nas pripelje do naslednje, splošnejše ugotovitve.

(iv) Zakonsko in kulturno/družbeno priznanje zakonitosti interesov

V vseh zgornjih kontekstih je seveda tudi pomembno, ali je z zakonodajo EU ali zakonodajo držav članic upravljavcem posebej dovoljeno (tudi če ni zahtevano), da izvajajo ukrepe v prizadevanju za zadevni javni ali zasebni interes. Pomemben je tudi obstoj kakršnih koli ustrezno sprejetih, nezavezujočih smernic, ki jih sprejmejo verodostojni organi, na primer regulativne agencije, ki upravljavce spodbujajo k obdelavi podatkov v prizadevanju za zadevni interes.

Tudi skladnost s kakršnimi koli nezavezujočimi smernicami, ki jih organi za varstvo podatkov ali drugi ustrezni organi sprejmejo v zvezi s podrobnimi pravili za obdelavo podatkov, bo verjetno prispevala k ugodni oceni ravnovesja. Kulturna in družbena pričakovanja, tudi ko se ne izražajo neposredno v zakonodajnih ali regulativnih instrumentih, so prav tako lahko pomembna in lahko pomagajo nagniti tehtnico na eno ali drugo stran.

Kolikor bolj izrecno je v zakonu ali drugem predpisu – ki upravljavca zavezuje ali ne – ali celo v kulturi dane skupnosti na splošno brez posebne pravne podlage priznano, da lahko upravljavec ravna in obdeluje podatke v prizadevanju za poseben interes, težji je ta zakoniti interes na tehtnici.[83]

(b) Učinek na posameznike, na katere se osebni podatki nanašajo

Z vidika še druge strani tehtnice je učinek obdelave na interese ali temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo, ključno merilo. V prvem pododdelku spodaj je na splošno obravnavano, kako oceniti učinek na posameznika, na katerega se osebni podatki nanašajo.

Koristnih je lahko več elementov, ki so analizirani v nadaljnjih pododdelkih, skupaj z naravo osebnih podatkov, načinom obdelave informacij, razumnimi pričakovanji posameznikov, na katere se osebni podatki nanašajo, ter statusom upravljavca in posameznika, na katerega se osebni podatki nanašajo. Na kratko bodo obravnavana tudi vprašanja, povezana z možnimi viri tveganja, ki lahko učinkujejo na zadevne posameznike, resnost katerih koli učinkov na zadevne posameznike in verjetnost uresničitve takih učinkov.

[82] Ocena mora seveda zajemati tudi razmislek o možni škodi, ki jo utrpi upravljavec, tretja oseba ali širša skupnost, če se podatki ne obdelajo.

[83] Vendar se ta interes ne more uporabiti za upravičenje vsiljivih praks, ki sicer ne bi opravile testa iz člena 8(2) EKČP.

(i) Ocena učinka

Pri ocenjevanju učinka[84] obdelave bi bilo treba upoštevati pozitivne in negativne posledice. To lahko vključuje morebitne prihodnje odločitve ali ukrepe tretjih oseb in položaje, v katerih lahko obdelava privede do izključevanja, diskriminacije ali obrekovanja posameznikov, ali širše položaje, v katerih obstaja tveganje oškodovanja ugleda, pogajalske moči ali neodvisnosti posameznikov, na katere se osebni podatki nanašajo.

Poleg neugodnega izida, ki ga je mogoče posebej predvideti, je treba upoštevati še širše čustvene vplive, kot so razdraženost, strah in trpljenje, ki so lahko posledica tega, da posameznik, na katerega se osebni podatki nanašajo, izgubi nadzor nad osebnimi podatki ali spozna, da so bili ti zlorabljeni ali ogroženi, na primer zaradi izpostavljenosti na spletu. Upoštevati je treba tudi srhljiv učinek na zaščiteno vedenje, kot je svoboda raziskovanja ali svoboda govora, ki je lahko posledica stalnega nadzora/spremljanja.

Delovna skupina poudarja, da je pomembno razumeti, da je poglavitni „učinek“ precej širši koncept kot pa krivica ali škoda, storjena enemu ali več zadevnim posameznikom, na katere se osebni podatki nanašajo. Izraz „učinek“, kot se uporablja v tem mnenju, zajema vse možne (morebitne ali trenutne) posledice obdelave podatkov. Zaradi jasnosti poudarjamo še, da koncept ni povezan s pojmom kršitve varnosti podatkov in je precej širši od koncepta učinkov, ki so lahko posledica kršitve varnosti podatkov. Namesto tega pojem učinka, kot se uporablja v tem mnenju, zajema različne načine, kako lahko na posameznika – pozitivno ali negativno – vpliva obdelava njegovih osebnih podatkov.[85]

Pomembno je tudi razumeti, da ima lahko najpogosteje vrsta povezanih in nepovezanih dogodkov končni negativni učinek na posameznika, na katerega se osebni podatki nanašajo, in da je lahko težko ugotoviti, kateri upravljavčev postopek obdelave je imel ključno vlogo pri negativnem učinku.

Ker posamezniki, na katere se osebni podatki nanašajo, v tem okviru pogosto težko dokažejo upravičenost zahteve po nadomestilu za nastalo škodo, tudi kadar je učinek zelo resničen, je toliko bolj pomembno osredotočiti se na preprečevanje in zagotavljanje, da se podatki obdelujejo le, če to pomeni nično ali zelo majhno tveganje pretiranega negativnega učinka na interese ali temeljne pravice in svoboščine posameznikov, na katere se osebni podatki nanašajo.

[84] To oceno učinka je treba razumeti v okviru člena 7(f). Z drugimi besedami, ne sklicujemo se na „analizo tveganja“ ali „oceno učinka o varstvu podatkov“ v smislu predlagane uredbe (člena 33 in 34) in različnih predlogov za njeno spremembo, ki jih je predlagal odbor LIBE. Vprašanje, katero metodologijo bi bilo treba uporabiti pri „analizi tveganja“ ali „oceni učinka o varstvu podatkov“, presega obseg tega mnenja. Nasprotno pa je treba upoštevati, da je lahko – tako ali drugače – analiza učinka na podlagi člena 7(f) pomemben del vsake „ocene tveganja“ ali „ocene učinka o varstvu podatkov“ ter lahko pomaga pri ugotavljanju, v katerih primerih se je treba posvetovati z organom za varstvo podatkov.

[85] Tveganje finančne škode, na primer, če se zaradi kršitve varnosti podatkov razkrijejo finančne informacije, ki bi morale biti v varnem okolju, in to na koncu vodi do kraje identitete ali drugih oblik goljufije, ali tveganje telesne poškodbe, bolečine, trpljenja in izgube uživanja življenja, ki so navsezadnje lahko posledica, na primer, nedovoljenega spreminjanja zdravstvene evidence in posledičnega slabega ravnanja z bolnikom, se mora vedno ustrezno upoštevati, čeprav nikakor ni omejeno na primere, ki spadajo na področje uporabe člena 7(f). Hkrati taka tveganja niso edina, ki jih je treba upoštevati pri oceni učinka na podlagi člena 7(f).

Pri oceni učinka lahko nekoliko pomagata terminologija in metodologija tradicionalne ocene tveganja, zato bodo v nadaljevanju na kratko poudarjeni nekateri elementi te metodologije. Vendar bi celovita metodologija ocene učinka – v okviru člena 7(f) ali širše – presegla obseg tega mnenja.

V tem okviru in tudi drugače je pomembno opredeliti vire morebitnih učinkov na posameznike, na katere se osebni podatki nanašajo.

Verjetnost, da se tveganje lahko uresniči, je eden izmed dejavnikov, ki jih je treba upoštevati. Na primer, dostop do spleta, izmenjave podatkov z lokacijami zunaj EU, medsebojno povezovanje z drugimi sistemi in visoka stopnja heterogenosti ali spremenljivosti sistema so lahko ranljive točke, ki jih lahko hekerji izkoristijo. Ta vir tveganja pomeni razmeroma veliko verjetnost, da se bo uresničilo tveganje ogrožanja podatkov. Nasprotno pa homogen, stabilen sistem, ki nima povezav z drugimi sistemi in ni povezan z spletom, pomeni precej manjšo verjetnost ogrožanja podatkov.

Drug element ocenjevanja tveganja je resnost posledic uresničenega tveganja. Resnost lahko sega od nizke (kot je neprijetna potreba po ponovnem vnosu osebnih kontaktnih podatkov, ki jih je upravljavec podatkov izgubil) do zelo visoke stopnje (kot je izguba življenja, ko pridejo podatki o lokaciji varovanih posameznikov v roke zločincev ali ko je na daljavo prekinjena oskrbo z elektriko s pametnimi merilnimi napravami v slabem vremenu ali v primeru slabega zdravstvenega stanja).

Ta ključna elementa – verjetnost uresničitve tveganja in resnost posledic – prispevata k splošni oceni morebitnega učinka.

Nazadnje, pri uporabi metodologije je treba upoštevati, da ocenjevanje učinka na podlagi člena 7(f) ne more privesti do mehanskega in popolnoma kvantitativnega izvajanja. V tradicionalnih scenarijih ocenjevanja tveganja se pri „resnosti“ lahko upošteva število posameznikov, na katere lahko učinkuje uporaba. Vseeno je treba upoštevati, da obdelava osebnih podatkov, ki učinkuje na manjšino posameznikov, na katere se osebni podatki nanašajo – ali celo na le enega posameznika –, še vedno zahteva posebno skrbno analizo, zlasti če je tak učinek na vsakega zadevnega posameznika lahko velik.

(ii) Narava podatkov

Najprej bi bilo treba presoditi, ali obdelava zadeva občutljive podatke, bodisi ker spadajo v posebno vrsto podatkov iz člena 8 Direktive bodisi iz drugih razlogov, kot v primeru biometričnih, genetskih, komunikacijskih podatkov, podatkov o lokaciji in drugih vrst osebnih informacij, ki zahtevajo posebno varstvo.[86]

Za ponazoritev, delovna skupina meni, da se na splošno uporaba biometričnih podatkov zaradi zahtev splošne varnosti lastnine ali posameznikov šteje za zakonit interes, nad katerim bi prevladali interesi ali temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo. Nasprotno pa se lahko biometrični podatki, kot so prstni odtisi in/ali

[86] Biometrični in genetski podatki se štejejo za posebni vrsti podatkov v predlagani uredbi o varstvu podatkov, ki jo je pripravila Komisija, v povezavi s spremembami, ki jih je predlagal odbor LIBE. Glej predlog spremembe 103 k členu 9 v končnem poročilu odbora LIBE. O razmerju med členoma 7 in 8 Direktive 95/46/ES glej oddelek III.1.2 zgoraj na straneh 14 in 15.

skeniranje šarenice, uporabljajo za varovanje območja z visokim tveganjem, kot je laboratorij, ki raziskuje nevarne viruse, če je upravljavec predložil dokaze o konkretnem obstoju precejšnjega tveganja.[87]

Na splošno, bolj ko so zadevne informacije občutljive, več je lahko posledic za posameznika, na katerega se osebni podatki nanašajo. Vendar to ne pomeni, da se lahko podatki, ki se sami po sebi zdijo neškodljivi, prosto obdelujejo na podlagi člena 7(f). Seveda imajo lahko tudi taki podatki glede na način njihove obdelave velik učinek na posameznike, kot bo prikazano v nadaljevanju v pododdelku (iii).

V zvezi s tem je lahko pomembno, ali so podatke že objavili posameznik, na katerega se osebni podatki nanašajo, ali tretje osebe. Pri tem je treba najprej poudariti, da se osebni podatki, tudi če so bili objavljeni, še naprej obravnavajo kot osebni podatki, zato se za njihovo obdelavo še vedno zahtevajo ustrezni zaščitni ukrepi.[88] Splošnega dovoljenja za ponovno uporabo in nadaljnjo obdelavo javno dostopnih osebnih podatkov na podlagi člena 7(f) ni.

Na podlagi tega se dejstvo, da so osebni podatki javno dostopni, lahko šteje kot dejavnik pri oceni, zlasti če so bili objavljeni brez razumnega pričakovanja nadaljnje uporabe podatkov v neke namene (na primer za raziskave ali zaradi preglednosti in odgovornosti).

(iii) Način obdelave podatkov

Ocenjevanje učinka v širšem pomenu lahko zahteva preučitev, ali so podatki objavljeni ali kako drugače dostopni veliko osebam ali pa se večje količine osebnih podatkov obdelujejo ali povezujejo z drugimi podatki (na primer pri oblikovanju profilov v komercialne namene, za kazenski pregon ali v drug namen). Navidezno neškodljivi podatki lahko pri obsežnejši obdelavi in povezavi z drugimi podatki privedejo do sklepanj o občutljivejših podatkih, kot je prikazano v scenariju 3 zgoraj, ki ponazarja razmerje med vzorci uživanja pice in premijami zdravstvenega zavarovanja.

Poleg tega, da lahko taka analiza privede do obdelave občutljivejših podatkov, lahko privede tudi do neverjetnih, nepričakovanih in včasih celo netočnih napovedi, na primer v zvezi z vedenjem ali osebnostjo zadevnih posameznikov. Odvisno od narave in učinka teh napovedi lahko to zelo posega v zasebnost posameznika.[89]

Delovna skupina je v prejšnjem mnenju poudarila tudi tveganja, povezana z nekaterimi varnostnimi rešitvami (skupaj s požarnimi zidovi, protivirusnimi programi ali programi za

[87] Glej Mnenje št. 3/2012 o razvoju na področju biometričnih tehnologij, ki ga je sprejela delovna skupina iz člena 29 (WP 193). Še en primer: delovna skupina je v Mnenju 4/2009 o Mednarodnem standardu Svetovne protidopinške agencije (navedeno v opombi 32) poudarila, da člen 7(f) ne bi bil veljavna podlaga za obdelavo zdravstvenih podatkov ali podatkov v zvezi s kršitvami v okviru protidopinških preiskav glede na „resnost posegov v zasebnost“. Obdelava podatkov bi morala biti predvidena z zakonom in izpolnjevati zahteve iz člena 8(4) ali (5) Direktive.

[88] Glej Mnenje št. 3/2013 o omejitvi namena (navedeno v opombi 9) in Mnenje št. 06/2013 o ponovni uporabi odprtih podatkov in informacij javnega sektorja, ki ga je delovna skupina sprejela 5. junija 2013 (WP 207).

[89] Glej oddelek III.2.5 Mnenja o omejitvi namena (navedeno v opombi 9) in Prilogo 2 (Masovni podatki in odprti podatki) k temu mnenju.

preprečevanje neželene pošte), ker lahko privedejo do obsežnega razvoja podrobnega pregledovanja paketov, ki lahko imajo velik vpliv na oceno ravnovesja pravic.[90]

Na splošno, bolj ko je lahko učinek obdelave negativen ali negotov, bolj neverjetno je, da se bo obdelava v celoti štela za zakonito. V tem okviru bi bilo seveda treba upoštevati dostopnost alternativnih metod za uresničevanje ciljev, za katere si prizadeva upravljavec, ki imajo manj negativen učinek na posameznika, na katerega se osebni podatki nanašajo. Kadar je primerno, se lahko za ugotovitev, ali je to mogoče, uporabijo ocene učinka na varstvo zasebnosti in podatkov.

(iv) Razumna pričakovanja posameznika, na katerega se osebni podatki nanašajo

Tudi razumna pričakovanja posameznika, na katerega se osebni podatki nanašajo, glede uporabe in razkritja podatkov, so v tem okviru zelo pomembna. Kot je bilo poudarjeno tudi pri analizi načela omejitve namena[91], je treba ugotoviti, ali status upravljavca podatkov[92], narava razmerja oziroma opravljene storitve[93] ali zakonske oziroma pogodbene obveznosti, ki se uporabljajo (ali druge obljube, dane ob zbiranju podatkov), lahko vzbudijo razumna pričakovanja glede strožje zaupnosti in strožjih omejitev nadaljnje uporabe. Na splošno, bolj ko so okoliščine zbiranja posebne in omejevalne, verjetneje je, da bo za uporabo veljalo več omejitev. Tudi pri tem je treba upoštevati dejanske okoliščine, ne pa se opirati le na besedilo v drobnem tisku.

(v) Status upravljavca podatkov in posameznika, na katerega se osebni podatki nanašajo

Pri ocenjevanju učinka obdelave je pomemben tudi status posameznika, na katerega se osebni podatki nanašajo, in upravljavca podatkov. Od tega, ali je upravljavec podatkov posameznik ali mala organizacija, veliko multinacionalno podjetje ali javni organ, in od posebnih okoliščin je odvisno, ali je njegov položaj bolj ali manj prevladujoč glede na posameznika, na katerega se osebni podatki nanašajo. Veliko multinacionalno podjetje ima lahko na primer več sredstev in večjo pogajalsko moč kot posameznik, na katerega se osebni podatki nanašajo, in je zato v boljšem položaju, da temu posamezniku vsili to, kar je po njegovem mnenju njegov „zakonit interes“. To lahko še toliko bolj velja, če ima podjetje prevladujoč položaj na trgu. Če se ne nadzira, se to lahko zgodi v škodo posameznikov, na katere se osebni podatki nanašajo. Tako kot zakonodaja o varstvu potrošnikov in konkurenci pomaga zagotavljati, da se ta moč ne bo zlorabljala, ima lahko zakonodaja o varstvu podatkov prav tako pomembno vlogo pri zagotavljanju, da se ne bo neupravičeno posegalo v pravice in interese posameznikov, na katere se osebni podatki nanašajo.

Po drugi strani je pomemben tudi status posameznika, na katerega se osebni podatki nanašajo. Čeprav bi bilo treba test tehtanja opraviti za povprečnega posameznika, bi morale posebne okoliščine zahtevati test v vsakem posameznem primeru: na primer, ugotoviti bi bilo treba, ali

[90] Glej oddelek 3.1 Mnenja delovne skupine št. 1/2009 o predlogih sprememb Direktive 2002/58/ES o zasebnosti in elektronskih komunikacijah (Direktiva o zasebnosti in elektronskih komunikacijah) (WP 159).
[91] Glej strani 24 in 25 Mnenja delovne skupine št. 3/2013 o omejitvi ukrepa (navedeno v opombi 9).
[92] „Kot na primer odvetnik ali zdravnik.“
[93] „Kot na primer storitve računalništva v oblaku za upravljanje osebnih dokumentov, storitve elektronske pošte, dnevniki, e-bralniki, opremljeni s funkcijami pisanja opomb, in razne aplikacije fotodnevnikov, ki lahko vsebujejo zelo osebne informacije.“

je posameznik, na katerega se osebni podatki nanašajo, otrok[94] ali pa spada v katero drugo ranljivejšo kategorijo prebivalstva, ki zahteva posebno varstvo, kot so duševno bolni, prosilci za azil ali starejši. Pomembni morata biti tudi vprašanji, ali je posameznik, na katerega se osebni podatki nanašajo, zaposlen, študent, bolnik in ali obstaja neravnovesje v razmerju med posameznikom, na katerega se osebni podatki nanašajo, in upravljavcem. Treba je oceniti učinek dejanske obdelave na zadevne posameznike.

Nazadnje, poudariti je treba, da vsi negativni učinki na posameznike, na katere se osebni podatki nanašajo, na tehtnici nimajo enake teže. Namen tehtanja iz člena 7(f) ni preprečiti vsakršnega negativnega učinka na posameznika, na katerega se osebni podatki nanašajo. Nasprotno, njegov namen je preprečiti nesorazmerni učinek. To je ključna razlika. Na primer, objava članka s točnimi in dobro raziskanimi podatki o domnevni vladni korupciji lahko škodi ugledu vpletenih vladnih uradnikov in ima hude posledice, tudi izgubo ugleda, izgubo na volitvah ali zaporno kazen, vendar je podlaga zanjo še vedno lahko člen 7(f).[95]

(c) Začasno ravnovesje

Pri tehtanju zadevnih interesov in pravic, kot je opisano zgoraj, bodo ukrepi, ki jih upravljavec sprejme za upoštevanja splošnih obveznosti iz Direktive, tudi glede sorazmernosti in preglednosti, zelo pripomogli k zagotovitvi, da upravljavec podatkov izpolnjuje zahteve iz člena 7(f). Popolno upoštevanje mora pomeniti, da je učinek na posameznike manjši, da je *manj verjetno* poseganje v interese ali temeljne pravice ali svoboščine posameznikov, na katere se osebni podatki nanašajo, in da je *bolj verjetno*, da se upravljavec podatkov lahko opre na člen 7(f). To mora upravljavce spodbuditi k boljšemu upoštevanju vseh horizontalnih določb Direktive.[96]

Vendar to ne pomeni, da bo upoštevanje teh horizontalnih zahtev kot tako vedno zadostovalo, da bo pravna podlaga temeljila na členu 7(f). Če bi bilo tako, bi bil člen 7(f) pravzaprav odvečen ali bi postal vrzel, zaradi katere bi brez pomena ostal celoten člen 7, ki zahteva ustrezno posebno pravno podlago za obdelavo.

Zato je pomembno izvesti dodatno oceno v okviru tehtanja v primerih, v katerih – na podlagi predhodne analize – ni jasno, na katero stran je treba nagniti tehtnico. Upravljavec lahko razmišlja, ali je mogoče uvesti dodatne ukrepe, ki presegajo upoštevanje horizontalnih določb Direktive, da bi lahko zmanjšal neupravičen učinek obdelave na posameznike, na katere se osebni podatki nanašajo.

Dodatni ukrepi lahko na primer zajemajo uvedbo preprostega, učinkovitega in dostopnega mehanizma, da se posameznikom, na katere se osebni podatki nanašajo, zagotovi brezpogojna možnost zavrnitve obdelave. Ti dodatni ukrepi lahko v nekaterih (vendar ne vseh) primerih

[94] Glej Mnenje št. 2/2009 o varstvu osebnih podatkov otrok (Splošne smernice in poseben primer šol), ki ga je delovna skupina sprejela 11. februarja 2009 (WP 160). Delovna skupina v tem mnenju poudarja posebno ranljivost otroka, in če ima otrok zastopnika, potrebo po upoštevanju otrokove koristi, in ne koristi njegovega zastopnika.

[95] Kot je bilo pojasnjeno zgoraj, je treba upoštevati tudi vsa ustrezna odstopanja v zvezi z obdelavo v novinarske namene na podlagi člena 9 Direktive.

[96] V zvezi s pomembno vlogo „horizontalne skladnosti“ glej tudi stran 54 Mnenja delovne skupine št. 3/2013 o omejitvi ukrepa, navedenega v opombi 9.

pomagajo prevesiti tehtnico in zagotoviti, da obdelava lahko temelji na členu 7(f), hkrati pa varujejo tudi pravice in interese posameznikov, na katere se osebni podatki nanašajo.

(d) Dodatni zaščitni ukrepi, ki jih izvaja upravljavec

Kot je bilo pojasnjeno zgoraj, način, kako bi upravljavec izvajal ustrezne ukrepe, bi lahko v nekaterih primerih pomagal prevesiti tehtnico. Ali je rezultat sprejemljiv, bo odvisno od celotne ocene. Večji ko je učinek na posameznika, na katerega se osebni podatki nanašajo, večjo pozornost bi bilo treba nameniti ustreznim zaščitnim ukrepom.

Primeri ustreznih ukrepov lahko med drugim zajemajo strogo omejitev količine podatkov, ki se zbirajo, ali takojšen izbris podatkov po uporabi. Nekateri izmed teh ukrepov so lahko obvezni že na podlagi Direktive, ob tem pa se pogosto spreminjajo in dajejo upravljavcem možnost za zagotovitev boljšega varstva posameznikov, na katere se osebni podatki nanašajo. Na primer, upravljavec lahko zbere manj podatkov ali zagotovi dodatne informacije, kot je posebej navedeno v členih 10 in 11 Direktive.

V nekaterih drugih primerih se zaščitni ukrepi v Direktivi ne zahtevajo *eksplicitno*, vendar se morda bodo v predlagani uredbi, ali se zahtevajo le v posebnih primerih, kot so:

- tehnični in organizacijski ukrepi za zagotovitev, da se podatki ne morejo uporabiti za sprejemanje odločitev ali drugih ukrepov v zvezi s posamezniki („funkcionalna ločitev“, kot se pogosto dogaja pri raziskavah),
- obsežna uporaba tehnik anonimizacije podatkov,
- združevanje podatkov,
- tehnologije za boljše varovanje zasebnosti, vgrajena zasebnost ter ocene učinka na varstvo zasebnosti in podatkov,
- večja preglednost,
- splošna in brezpogojna pravica do zavrnitve,
- prenosljivost podatkov in povezani ukrepi za krepitev moči posameznikov, na katere se osebni podatki nanašajo.

Delovna skupina ugotavlja, da je bilo v zvezi z nekaterimi ključnimi vprašanji, skupaj s funkcionalno ločitvijo in tehnikami anonimizacije, nekaj smernic zagotovljenih že v ustreznih delih njenih mnenj o omejitvi namena, odprtih podatkih in tehnikah anonimizacije.[97]

Delovna skupina bi rada v zvezi s psevdonimizacijo in šifriranjem poudarila, da če podatkov ni mogoče neposredno identificirati, to ne vpliva na presojo zakonitosti obdelave: na to se ne sme gledati, kot da se s tem nezakonita obdelava spremeni v zakonito.[98]

Obenem bosta imela psevdonimizacija in šifriranje – kot vsi drugi tehnični in organizacijski ukrepi, uvedeni za varstvo osebnih podatkov – pomembno vlogo pri ocenjevanju morebitnega

[97] Glede nadaljnje obdelave v zgodovinske, statistične in znanstvene namene glej oddelka III.2.3 in III.2.5 Mnenja delovne skupine št. 3/2013 o omejitvi namena in Prilogo 2 k temu mnenju, navedenemu v opombi 9, glede masovnih podatkov in odprtih podatkov pa glej tudi ustrezne dele Mnenja delovne skupine št. 06/2013 o odprtih podatkih (navedeno v opombi 88) in Mnenje št. 5/2014 o anonimizacijskih tehnikah.

[98] Glej v zvezi s tem predloge sprememb, ki jih je odbor LIBE izglasoval v svojem končnem poročilu, in zlasti predlog spremembe 15 k uvodni izjavi 38, ki povezuje psevdonimizacijo in legitimna pričakovanja posameznika, na katerega se osebni podatki nanašajo.

učinka obdelave na posameznika, na katerega se osebni podatki nanašajo, in lahko zato v nekaterih primerih pomagata prevesiti tehtnico v korist upravljavca. Uporaba manj tveganih oblik obdelave osebnih podatkov (na primer osebni podatki, ki se šifrirajo ob shranjevanju ali prenosu, ali osebni podatki, ki jih je manj neposredno in manj verjetno mogoče identificirati) morata na splošno pomeniti, da je verjetnost poseganja v interese ali temeljne pravice in svoboščine posameznikov, na katere se osebni podatki nanašajo, manjša.

Delovna skupina želi v zvezi s temi zaščitnimi ukrepi – in celovito oceno ravnovesja – poudariti tri posebne točke, ki imajo pogosto ključno vlogo v okviru člena 7(f):

- razmerje med testom tehtanja, preglednostjo in načelom odgovornosti;
- pravico posameznika, na katerega se osebni podatki nanašajo, do ugovora zoper obdelavo in poleg ugovora dostopnost zavrnitve brez potrebe po utemeljevanju ter
- krepitev moči posameznikov, na katere se osebni podatki nanašajo: prenosljivost podatkov in dostopnost učinkovitih mehanizmov, s katerimi lahko posameznik, na katerega se osebni podatki nanašajo, dostopa do svojih podatkov in jih spreminja, izbriše, pošlje ali kakor koli dodatno obdela (ali dovoli tretjim osebam nadaljnjo obdelavo).

Te točke bodo zaradi svojega pomena obravnavane v posebnih poglavjih.

III.3.5 Odgovornost in preglednost

Najprej, preden upravljavec izvede obdelavo na podlagi člena 7(f), mora presoditi, ali ima zakonit interes; ali je obdelava potrebna za ta zakonit interes in ali v zadevnem primeru nad tem interesom prevladajo interesi in pravice posameznikov, na katere se osebni podatki nanašajo.

V tem smislu člen 7(f) temelji na načelu odgovornosti. Upravljavec mora vnaprej opraviti skrben in učinkovit test, ki temelji na posebnih okoliščinah primera, namesto da bi bil abstrakten, pri čemer upošteva tudi razumna pričakovanja posameznikov, na katere se osebni podatki nanašajo. Dobra praksa je, da se, kadar je primerno, ta test dovolj podrobno in pregledno dokumentira, tako da bodo lahko zadevni deležniki, med katerimi so posamezniki, na katere se osebni podatki nanašajo, in organi za varstvo podatkov ter nazadnje sodišča, – po potrebi – preverili, ali je bil test opravljen v celoti in pravilno.

Upravljavec bo najprej opredelil zakoniti interes in opravil test tehtanja, vendar to ni nujno končna in dokončna ocena: če interes, za katerega si prizadeva, v resnici ni interes, ki ga je upravljavec določil, ali če upravljavec interesa ni določil dovolj podrobno, je treba ravnovesje znova oceniti na podlagi dejanskega interesa, ki ga določi bodisi organ za varstvo podatkov bodisi sodišče.[99] Kot pri drugih ključnih vidikih varstva podatkov, kot sta identifikacija upravljavca podatkov ali določitev namena,[100] je pomembna resničnost, ki se skriva za vsako trditvijo upravljavca.

Pojem odgovornosti je tesno povezan s pojmom preglednosti. Da bi se posameznikom, na katere se osebni podatki nanašajo, omogočilo uveljavljanje njihovih pravic in da bi deležniki

[99] Na primer na podlagi pritožbe ali ugovora iz člena 14.
[100] Glej mnenja, navedena v opombi 9.

lahko izvajali širši javni nadzor, delovna skupina priporoča, da upravljavci posameznikom, na katere se osebni podatki nanašajo, jasno in na uporabnikom prijazen način pojasnijo razloge, zaradi katerih menijo, da nad njihovimi interesi ne prevladajo interesi ali temeljne pravice in svoboščine posameznikov, na katere se osebni podatki nanašajo, in jim pojasnijo zaščitne ukrepe, ki so jih sprejeli za varstvo osebnih podatkov, skupaj s pravico do zavrnitve obdelave, kadar je to primerno.[101]

Delovna skupina v zvezi s tem poudarja, da je pri tem zelo pomembna tudi zakonodaja o varstvu podatkov, zlasti zakoni, ki potrošnike varujejo pred nepoštenimi poslovnimi praksami.

Če upravljavec skriva pomembne informacije o nepričakovani nadaljnji uporabi podatkov v pravnem smislu, skriti v drobnem tisku pogodbe, lahko s tem krši pravila o varstvu potrošnikov glede nepoštenih pogodbenih pogojev (skupaj s prepovedjo „presenetljivih pogojev“), poleg tega tudi ne bo izpolnil zahtev iz člena 7(a) glede veljavne in informirane privolitve ali zahtev iz člena 7(f) glede razumnih pričakovanj posameznika, na katerega se osebni podatki nanašajo, in splošno sprejemljivega ravnovesja interesov. Postavila bi se tudi vprašanja o skladnosti s členom 6 v zvezi s pošteno in zakonito obdelavo osebnih podatkov.

Na primer, v številnih primerih se uporabniki „brezplačnih“ spletnih storitev, kot so iskanje, elektronska pošta, družbeni mediji, shranjevanje datotek ali druge spletne ali mobilne aplikacije, ne zavedajo v celoti, v kakšnem obsegu se njihova dejavnost zapisuje in analizira, da se ustvarja vrednost za ponudnika storitve, in jih zato obstoječa tveganja ne skrbijo.

Da bi v teh primerih okrepili moč posameznikov, na katere se osebni podatki nanašajo, je prvi potrebni – vendar nikakor ne sam po sebi zadosten – pogoj[102] pojasniti, da storitve niso brezplačne in da potrošniki pravzaprav plačujejo s svojimi osebnimi podatki. Ob tem morajo biti v vsakem primeru jasno navedeni pogoji in zaščitni ukrepi za morebitno uporabo podatkov, s čimer se zagotovi veljavnost privolitve iz člena 7(a) ali ugodno ravnovesje iz člena 7(f).

III.3.6 Pravica do ugovora in več

(a) Pravica do ugovora iz člena 14 Direktive

Točki (e) in (f) člena 7 sta posebni, ker čeprav temeljita predvsem na objektivni oceni zadevnih interesov in pravic, omogočata tudi samoodločanje posameznikov, na katere se osebni podatki nanašajo, da uveljavljajo pravico do ugovora[103]: vsaj v primeru teh dveh

[101] Kot je delovna skupina pojasnila na strani 46 Mnenja št. 3/2013 o omejitvi namena (navedeno v opombi 9), je treba v primeru oblikovanja profilov in samodejnega sprejemanja odločitev „za zagotovitev preglednosti […] posameznikom, na katere se osebni podatki nanašajo/potrošnikom omogočiti dostop do njihovih ‚profilov‘ in do logike sprejemanja odločitev (algoritem), na podlagi katere je bil profil razvit. Z drugimi besedami: organizacije bi morale razkriti svoja merila za odločanje. To je ključni zaščitni ukrep, ki je še pomembnejši v svetu masovnih podatkov“. Dejstvo, ali organizacija omogoča to preglednost ali ne, je zelo pomemben dejavnik, ki ga je treba upoštevati pri tehtanju.

[102] Glede možnih dodatnih zaščitnih ukrepov v zvezi s čedalje pogostejšimi primeri, v katerih potrošniki plačujejo z osebnimi podatki, glej oddelek III.3.6, zlasti strani 47 in 48 o Varstvu podatkov prijazne alternative za „brezplačne“ spletne storitve ter Prenosljivost podatkov, „midata“ in povezana vprašanja.

[103] Ta pravica do ugovora se ne sme zamenjevati s privolitvijo na podlagi člena 7(a), ko upravljavec podatkov ne more obdelati, dokler ne dobi privolitve. Upravljavec lahko v okviru člena 7(f) obdela podatke, za katere veljajo

razlogov člen 14(a) Direktive določa, da („razen kjer nacionalna zakonodaja določa drugače“) lahko posameznik, na katerega se osebni podatki nanašajo, „na podlagi zakonitih in nujnih razlogov, povezanih z njegovim posebnim položajem kadar koli ugovarja obdelavi podatkov, ki se nanašajo nanj“. Dodano je še, da se mora obdelava končati, kadar je ugovor utemeljen.

Načeloma bodo morali posamezniki, na katere se osebni podatki nanašajo, na podlagi veljavne zakonodaje dokazati, da imajo „zakonite in nujne interese“ za ustavitev obdelave svojih osebnih podatkov (člen 14(a)), razen v primeru neposrednega trženja, ko ugovora ni treba utemeljiti (člen 14(b)).

Na to se ne sme gledati, kot da je v nasprotju s testom tehtanja iz člena 7(f), ki se izvede „*a priori*“: nasprotno, dopolnjuje tehtanje, saj kadar je obdelava dovoljena na podlagi razumne in objektivne ocene raznih zadevnih pravic in interesov, ima posameznik, na katerega se osebni podatki nanašajo, še vedno *dodatno* možnost ugovarjati na podlagi svojega posebnega položaja. To bo nato moralo privesti do nove ocene, pri kateri se bodo upoštevali posebni argumenti posameznika, na katerega se osebni podatki nanašajo. Ta nova ocena je načeloma spet predmet preverjanja organa za varstvo podatkov ali sodišč.

(b) Onkraj ugovora: vloga zavrnitve kot dodatnega zaščitnega ukrepa

Delovna skupina poudarja, da čeprav je pravica do ugovora iz člena 14(a) pogojena z utemeljitvijo posameznika, na katerega se osebni podatki nanašajo, upravljavcu nič ne preprečuje, da ponudi zavrnitev, ki bi bila širša in od posameznika, na katerega se osebni podatki nanašajo, ne bi zahtevala dodatnega dokazovanja zakonitega interesa (nujnega ali drugačnega). Ne bi bilo treba, da taka brezpogojna pravica temelji na posebnem položaju posameznikov, na katere se osebni podatki nanašajo.

Pravzaprav ima lahko zlasti v mejnih primerih, v katerih je težko najti ravnovesje, dobro pripravljen in učinkovit mehanizem zavrnitve, ki posameznikom, na katere se osebni podatki nanašajo, ne zagotavlja nujno vseh elementov, da bi bile izpolnjeni zahteve za veljavno privolitev iz člena 7(a), pomembno vlogo pri varovanju pravic in interesov posameznikov, na katere se osebni podatki nanašajo.

Zato je potreben podrobno izdelan pristop, ki razlikuje med primeri, v katerih se zahteva privolitev iz člena 7(a), in primeri, v katerih lahko učinkovita možnost zavrnitve obdelave (v povezavi z drugimi možnimi dodatnimi ukrepi) prispeva k varstvu posameznikov, na katere se osebni podatki nanašajo, na podlagi člena 7(f).

Širše in lažje ko je mogoče uporabljati mehanizem zavrnitve, bolj bo prispeval k temu, da se bo tehtnica prevesila v korist obdelave na podlagi člena 7(f).

Primer: razvoj pristopa k neposrednemu trženju

Za ponazoritev razlikovanja med primeri, v katerih se zahteva privolitev iz člena 7(a), in primeri, v katerih se lahko zavrnitev uporabi kot zaščitni ukrep iz člena 7(f), je koristno uporabiti primer neposrednega trženja, za katero je bila posebna določba o zavrnitvi že

pogoji in zaščitni ukrepi, dokler posameznik, na katerega se osebni podatki nanašajo, temu ne ugovarja. V tem smislu je mogoče pravico do ugovora pravzaprav obravnavati kot posebno obliko zavrnitve. Za več podrobnosti glej Mnenje delovne skupine št. 15/2011 o opredelitvi privolitve (navedeno v opombi 2).

vključena v člen 14(b) Direktive. Zaradi novega tehnološkega razvoja je bila ta določba pozneje dopolnjena s posebnimi določbami v Direktivi o zasebnosti in elektronskih komunikacijah.[104]

V skladu s členom 13 Direktive o zasebnosti in elektronskih komunikacijah je privolitev za nekatere vrste – vsiljivejšega – neposrednega trženja (kot sta trženje po elektronski pošti in klicni avtomati) pravilo. Izjemoma je v obstoječih razmerjih s stranko, ko upravljavec oglašuje svoje „podobne“ izdelke ali storitve, dovolj zagotoviti (brezpogojno) možnost „zavrnitve“ brez utemeljitve.

Zaradi razvoja tehnologij so bile za nove prakse trženja potrebne podobne, razmeroma preproste rešitve, ki sledijo podobni logiki.

Prvič, razvil se je način dostave tržnega gradiva: namesto elektronske pošte, ki prispe v poštni predal, se novi ciljni vedenjski oglasi pojavljajo na pametnih telefonih in računalniških zaslonih. V bližnji prihodnosti bodo lahko oglasi vdelani tudi v pametne predmete, povezane v internet stvari.

Drugič, oglasi postajajo čedalje bolj natančno usmerjeni: namesto da bi temeljili le na profilih strank, se dejavnosti strank čedalje bolj sledijo in shranjujejo na spletu in zunaj njega ter analizirajo z bolj izpopolnjenimi avtomatiziranimi metodami.[105]

Zaradi tega razvoja se je namen tehtanja spremenil: ne gre več za pravico do svobodnega komercialnega oglaševanja, ampak predvsem za ekonomske interese poslovnih organizacij, da spoznajo stranke s sledenjem in nadziranjem njihovih dejavnosti na spletu in zunaj njega, kar bi bilo treba tehtati s (temeljno) pravico do zasebnosti ter varstvom osebnih podatkov teh posameznikov in njihovim interesom, da niso predmet neupravičenega nadzora.

Ta sprememba v prevladujočih poslovnih modelih in dvig vrednosti osebnih podatkov kot sredstva poslovnih organizacij pojasnjujeta novejšo zahtevo po privolitvi v tem okviru v skladu s členom 5(3) in členom 13 Direktive o zasebnosti in elektronskih komunikacijah.

Tako veljajo različna posebna pravila glede na obliko trženja, ki zajemajo:

- brezpogojno pravico do ugovora zoper neposredno trženje (zasnovano za tradicionalen kontekst pošiljanja po navadni pošti in trženje podobnih izdelkov) v skladu s členom 14(b) Direktive; v tem primeru bi člen 7(f) lahko bil pravna podlaga;
- zahtevo po privolitvi iz člena 13 Direktive o zasebnosti in elektronskih komunikacijah za trženje prek avtomatičnih klicnih sistemov, telefaksa, besedilnih sporočil in elektronske pošte (ob upoštevanju izjem)[106] ter dejansko uporabo člena 7(a) Direktive o varstvu podatkov;
- zahtevo po privolitvi iz člena 5(3) Direktive o zasebnosti in elektronskih komunikacijah (in člena 7(a) Direktive o varstvu podatkov) za vedenjsko oglaševanje

[104] V zvezi s členom 13 Direktive o zasebnosti in elektronskih komunikacijah glej tudi oddelek III.2.4 Mnenja delovne skupine št. 3/2013 o omejitvi namena (navedeno v opombi 9).
[105] Glej oddelek III.2.5 Mnenja delovne skupine št. 3/2013 o omejitvi namena (navedeno v opombi 9) in Prilogo 2 k temu mnenju (o masovnih podatkih in odprtih podatkih).
[106] Glej tudi člen 13(3) Direktive o zasebnosti in elektronskih komunikacijah, ki daje državam članicam možnost izbire med privolitvijo in zavrnitvijo neposrednega trženja na druge načine.

na podlagi tehnik sledenja, kot so piškotki, ki shranjujejo informacije na terminalu uporabnika.[107]

Čeprav so pravne podlage, ki se uporabljajo, jasne, kar zadeva člen 5(3) in člen 13 Direktive o zasebnosti in elektronskih komunikacijah, niso zajete vse oblike trženja, zato bi bile zaželene smernice o tem, v katerih primerih se zahteva privolitev iz člena 7(a) in v katerih se doseže ravnovesje iz člena 7(f), skupaj z možnostjo zavrnitve.

V zvezi s tem je koristno opozoriti na mnenje o omejitvi namena, v katerem je delovna skupina posebej navedla, da „kadar želi organizacija posebej analizirati ali napovedati osebne preference, vedenje in ravnanje posameznih strank, na podlagi katerih bo nazadnje sprejela informirane ‚ukrepe ali odločitve' v zvezi s temi strankami[,] se bo skoraj vedno zahtevala svobodna, posebna, informirana in nedvoumna privolitev, saj v nasprotnem primeru nadaljnje uporabe ni mogoče šteti za skladno. Pomembno je, da bi se morala taka privolitev zahtevati na primer za sledenje in oblikovanje profilov za namene neposrednega trženja, vedenjskega oglaševanja, trgovanja s podatki, oglaševanja na podlagi lokacije ali raziskave digitalnega trga na podlagi sledenja".[108]

Varstvu podatkov prijazne alternative za „brezplačne" spletne storitve

Ko potrošniki, ki se prijavijo na „brezplačne" spletne storitve, te storitve dejansko „plačujejo" tako, da dovolijo uporabo svojih osebnih podatkov, bi k ugodni oceni ravnovesja – ali ugotovitvi, da je imel potrošnik resnično svobodo izbire in je tako dal veljavno privolitev iz člena 7(a) – prispevalo tudi, če bi upravljavec ponudil tudi alternativno različico svojih storitev, v katerih se „osebni podatki" ne bi uporabljali za trženje.

Dokler take alternativne storitve niso na voljo, je težje trditi, da je bila dana veljavna (svobodna) privolitev iz člena 7(a) že le z uporabo brezplačnih storitev ali da se mora ravnovesje iz člena 7(f) nagniti v korist upravljavca.

Zgornji premisleki poudarjajo pomembno vlogo, ki jo lahko imajo dodatni zaščitni ukrepi, skupaj z učinkovitim mehanizmom zavrnitve obdelave, pri spreminjanju začasnega ravnovesja. Hkrati kažejo tudi, da se v nekaterih primerih ni mogoče opreti na člen 7(f) kot na pravno podlago za obdelavo ter da si morajo upravljavci zagotoviti veljavno privolitev iz člena 7(a) – ali izpolniti nekatere druge pogoje iz Direktive – za obdelavo.

Prenosljivost podatkov, „midata" in povezana vprašanja

Med dodatnimi zaščitnimi ukrepi, ki lahko pomagajo nagniti tehtnico, je treba posebno pozornost nameniti prenosljivosti podatkov in povezanim ukrepom, katerih pomen v spletnem okolju je lahko čedalje večji. Delovna skupina opozarja na svoje mnenje o omejitvi namena, v katerem je poudarila, da „v številnih primerih zaščitni ukrepi, kot je posameznikom, na katere se osebni podatki nanašajo, ali strankam omogočiti neposreden dostop do njihovih podatkov v prenosljivi, uporabnikom prijazni in strojno berljivi obliki, lahko pomagajo okrepiti njihovo moč in odpraviti ekonomsko neravnovesje med velikimi družbami na eni strani in

[107] V zvezi z uporabo te določbe glej Mnenje delovne skupine št. 2/2010 o spletnem vedenjskem oglaševanju (WP 171).
[108] Glej Prilogo 2 (o masovnih podatkih in odprtih podatkih) k Mnenju št. 3/2013 (navedeno v opombi 9), stran 45.

posamezniki, na katere se osebni podatki nanašajo, ali strankami na drugi. To bi posameznikom tudi omogočilo, da ‚souporabljajo bogastvo', ustvarjeno iz masovnih podatkov, in spodbudilo razvijalce, da uporabnikom ponudijo dodatne funkcije in aplikacije".[109]

Dostopnost učinkovitih mehanizmov, s katerimi lahko posamezniki, na katere se osebni podatki nanašajo, dostopajo do svojih podatkov ter jih spreminjajo, izbrišejo, pošljejo ali kakor koli drugače dodatno obdelajo (ali dovolijo tretjim osebam nadaljnjo obdelavo), bo tem posameznikom dala večjo moč in omogočila, da bodo bolje izkoristili digitalne storitve. Poleg tega lahko spodbuja konkurenčnejše tržno okolje, saj potrošnikom omogoča lažjo zamenjavo ponudnikov (na primer pri spletnem bančništvu ali dobaviteljih energije v okolju pametnih omrežij). Nazadnje, prispeva lahko tudi k temu, da tretje osebe, ki lahko na podlagi zahteve in privolitve potrošnikov dostopajo do njihovih podatkov, razvijajo dodatne storitve z dodano vrednostjo. S tega vidika prenosljivost podatkov ni le dobra za varstvo podatkov, ampak tudi za konkurenco in varstvo potrošnikov.[110]

IV. Končne ugotovitve

Delovna skupina je v tem mnenju analizirala merila za zakonitost obdelave podatkov, ki so določena v členu 7 Direktive. Poleg tega, da ponuja smernice za razlago in uporabo člena 7(f) v praksi na podlagi trenutnega pravnega okvira, je njen cilj pripraviti priporočila glede politike, ki bodo oblikovalcem politik pomagala pri razmisleku o spremembah trenutnega pravnega okvira varstva podatkov. Pred predstavitvijo teh priporočil so v nadaljevanju na kratko predstavljene glavne ugotovitve glede razlage člena 7.

IV.1 Sklepne ugotovitve

Pregled člena 7

Člen 7 določa, da se osebni podatki obdelujejo le, če se uporablja ena izmed šestih pravnih podlag, naštetih v tem členu.

Prva podlaga iz člena 7(a) se osredotoča na privolitev posameznika, na katerega se osebni podatki nanašajo, kot podlago za zakonitost. Preostale podlage pa, nasprotno, dovoljujejo obdelavo – ob upoštevanju zaščitnih ukrepov – v primerih, v katerih je ne glede na privolitev primerno in nujno obdelati podatke v nekem kontekstu v prizadevanju za poseben zakoniti interes.

V točkah (b), (c), (d) in (e) so opredeljeni posebni konteksti, v katerih se obdelava osebnih podatkov lahko šteje za zakonito. Pogoji, ki veljajo v vsakem izmed teh kontekstov, zahtevajo

[109] „Glej pobude, kot so ‚midata' v Združenem kraljestvu, ki temeljijo na ključnem načelu, da je treba podatke vrniti potrošnikom. Midata je prostovoljni program, ki bi moral potrošnikom sčasoma dati čedalje večji dostop do njihovih osebnih podatkov v prenosljivi, elektronski obliki. Glavna zamisel je, da bi morali tudi potrošniki imeti koristi od masovnih podatkov, tako da bi z dostopom do svojih informacij lahko sprejemali boljše odločitve. Glej tudi pobude ‚Green button', ki potrošnikom omogočajo dostop do podatkov o njihovi porabi energije." Več informacij o pobudah v Združenem kraljestvu in Franciji je na voljo na http://www.midatalab.org.uk/ in http://mesinfos.fing.org/.

[110] O pravici do prenosljivosti podatkov glej člen 18 predlagane uredbe.

posebno pozornost, saj določajo področje uporabe različnih podlag za zakonitost. Natančneje, merila „potrebna za izvajanje pogodbe“, „potrebna za skladnost z zakonsko obveznostjo“, „potrebna za varstvo življenjskih interesov posameznikov, na katere se osebni podatki nanašajo“ in „potrebna za izvajanje naloge, ki se opravlja v javnem interesu ali pri izvrševanju javne oblasti“ vsebujejo različne zahteve, ki so bile obravnavane v oddelku III.2.

Točka (f) se splošneje nanaša na (kateri koli) zakoniti interes, za katerega si prizadeva upravljavec (v katerem koli kontekstu). Vendar je za to splošno določbo posebej določen dodaten test tehtanja, ki zahteva, da se tehtajo zakoniti interesi upravljavca – ali tretje osebe ali oseb, ki so jim osebni podatki posredovani –, ter interesi ali temeljne pravice posameznikov, na katere se osebni podatki nanašajo.

Vloga člena 7(f)

Člen 7(f) se ne sme šteti za pravno podlago, ki se lahko uporablja le zmerno kot „zadnja možnost“ – ali vsaj kot zadnja priložnost, če se ne uporabi druga podlaga – za zapolnitev vrzeli v redkih in nepredvidenih okoliščinah. Niti se ne sme šteti za prednostno možnost in njena uporaba se ne sme neupravičeno razširiti, ker bi se ta podlaga štela za manj zavezujočo od drugih. Nasprotno, je prav toliko veljavno sredstvo kot katera koli druga podlaga za zakonitost obdelave osebnih podatkov.

Ustrezna uporaba člena 7(f) v pravih okoliščinah in ob ustreznih zaščitnih ukrepih lahko pomaga preprečevati zlorabo drugih pravnih podlag in pretirano opiranje nanje. Primerna ocena ravnovesja iz člena 7(f), pogosto z možnostjo zavrnitve obdelave, je lahko v nekaterih primerih ustrezna alternativa za, na primer, neprimerno uporabo „privolitve“ ali „potrebe za izvajanje pogodbe“ kot podlage. Obravnava člena 7(f) s tega vidika zagotavlja dodatne zaščitne ukrepe v primerjavi z drugimi predhodno določenimi podlagami. Zato se ne sme šteti za najšibkejši člen ali odprta vrata za upravičenje vseh postopkov obdelave podatkov, za katere se ne more uporabiti nobena druga pravna podlaga.

Zakoniti interesi upravljavca/interesi ali temeljne pravice posameznika, na katerega se osebni podatki nanašajo

Koncept „interesa“ pomeni večje tveganje, ki ga lahko ima upravljavec pri obdelavi, ali korist, ki jo ima upravljavec – ali ki jo lahko ima družba – od obdelave. Lahko je nujen, neposreden ali bolj sporen. Primeri, na katere se nanaša člen 7(f), lahko tako segajo od uveljavljanja temeljnih pravic ali varstva pomembnih osebnih ali družbenih interesov do drugih manj očitnih ali celo spornih kontekstov.

Da se interes šteje za „zakonitega“ in da spada na področje uporabe člena 7(f), bo moral biti zakonit, to pomeni, skladen z evropsko in nacionalno zakonodajo. Biti mora tudi dovolj jasno izražen in natančno določen, da omogoči izvedbo testa tehtanja interesov in temeljnih pravic posameznika, na katerega se osebni podatki nanašajo. Pomeniti mora tudi dejanski in trenutni interes, torej ne sme biti spekulativen.

Dejstvo, da ima upravljavec ali tretja oseba, ki so ji osebni podatki posredovani, tak zakoniti interes, ne pomeni nujno, da se lahko opre na člen 7(f) kot pravno podlago za obdelavo. Ali se je mogoče opreti na člen 7(f), bo odvisno od rezultata testa tehtanja. Obdelava mora biti tudi „potrebna zaradi zakonitih interesov“, za katere si prizadeva upravljavec ali – v primeru

razkritja – tretja oseba. Zato je treba vedno dati prednost manj vsiljivim načinom za doseganje istega namena.

Pojem „interesi“ posameznikov, na katere se osebni podatki nanašajo, je opredeljen še širše, saj ne zahteva, da so „zakoniti“. Če si lahko upravljavec ali tretja oseba prizadeva za katere koli interese, pod pogojem, da niso nezakoniti, pa je posameznik, na katerega se osebni podatki nanašajo, upravičen do tega, da se vse kategorije interesov upoštevajo in tehtajo z interesi upravljavca, dokler so pomembne v okviru področja uporabe Direktive.

Izvajanje testa tehtanja

Delovna skupina si pri razlagi člena 7(f) prizadeva za uravnotežen pristop, ki upravljavcem podatkov zagotavlja potrebno prožnost v primerih, v katerih ni neupravičenega učinka na posameznike, na katere se osebni podatki nanašajo, tem posameznikom pa zadostno pravno gotovost in jamstva, da se ta neomejena določba ne bo zlorabila.

Pri izvajanju tega testa tehtanja je zelo pomembno upoštevati naravo in vir zakonitih interesov ter ali je obdelava potrebna za uresničevanje teh interesov, na eni strani, in kakšen učinek ima na posameznike, na katere se osebni podatki nanašajo, na drugi strani. Ta začetna ocena bi morala upoštevati ukrepe, kot sta preglednost ali omejeno zbiranje podatkov, ki jih upravljavec namerava sprejeti za uskladitev z Direktivo.

Po analizi in tehtanju obeh strani je mogoče določiti začasno „ravnovesje“: najprej se lahko ugotovi, ali zakoniti interesi upravljavca prevladajo nad pravicami in interesi posameznikov, na katere se osebni podatki nanašajo. Vendar je lahko v nekaterih primerih rezultat testa tehtanja nejasen in obstaja dvom, ali zakoniti interes upravljavca (ali tretje osebe) prevlada ter ali lahko obdelava temelji na členu 7(f).

Zato je pomembno izvesti dodatno oceno v okviru tehtanja. Upravljavec lahko v tej fazi razmišlja, ali lahko uvede dodatne ukrepe, ki presegajo upoštevanje drugih horizontalnih določb Direktive, da bi pomagal varovati posameznike, na katere se osebni podatki nanašajo. Dodatni ukrepi lahko na primer zajemajo uvedbo preprostega, učinkovitega in dostopnega mehanizma, da se posameznikom, na katere se osebni podatki nanašajo, zagotovi brezpogojna možnost zavrnitve obdelave.

Ključni dejavniki, ki se upoštevajo pri izvajanju testa tehtanja

Pri izvajanju testa tehtanja je treba glede na navedeno upoštevati te koristne dejavnike:

- naravo in vir zakonitega interesa, skupaj z ugotavljanjem:

  – ali je obdelava podatkov potrebna za uveljavljanje temeljne pravice ali
  – je v javnem interesu oziroma je družbeno, kulturno ali pravno/zakonsko priznana v zadevni skupnosti;

- učinek na posameznike, na katere se osebni podatki nanašajo, ki zajema:

  – naravo podatkov, na primer, ali obdelava zajema podatke, ki se lahko štejejo za občutljive ali pa so bili pridobljeni iz javno dostopnih virov;
  – način obdelave podatkov, skupaj s tem, ali so podatki objavljeni ali kako drugače dostopni veliko osebam ali pa se večje količine osebnih podatkov obdelujejo ali povezujejo z drugimi podatki (na primer pri oblikovanju profilov v komercialne namene, za kazenski pregon ali v drug namen);
  – razumna pričakovanja posameznika, na katerega se osebni podatki nanašajo, zlasti glede uporabe in razkritja podatkov v zadevnih okoliščinah;
  – status upravljavca podatkov in posameznika, na katerega se osebni podatki nanašajo, skupaj z ravnovesjem moči med posameznikom, na katerega se osebni podatki nanašajo, in upravljavcem podatkov, ali dejstvom, ali je ta posameznik otrok ali spada v katero drugo ranljivejšo kategorijo prebivalstva;

- dodatne zaščitne ukrepe za preprečevanje neupravičenega učinka na posameznike, na katere se osebni podatki nanašajo, ki zajemajo:

  – zmanjšanje količine podatkov (na primer stroge omejitve zbiranja podatkov ali takojšen izbris podatkov po uporabi);
  – tehnične in organizacijske ukrepe za zagotovitev, da se podatki ne morejo uporabiti za sprejemanje odločitev ali drugih ukrepov v zvezi s posamezniki („funkcionalna ločitev“);
  – širšo uporabo tehnik anonimizacije, združevanje podatkov, tehnologije za boljše varovanje zasebnosti, vgrajeno zasebnost, ocene učinka na varstvo zasebnosti in podatkov;
  – večjo preglednost, splošno in brezpogojno pravico do zavrnitve, prenosljivost podatkov in povezane ukrepe za krepitev moči posameznikov, na katere se osebni podatki nanašajo.

Odgovornost, preglednost, pravica do ugovora in več

V zvezi s temi zaščitnimi ukrepi – in celovito oceno ravnovesja – imajo tri točke pogosto ključno vlogo v okviru člena 7(f) in zato zahtevajo posebno pozornost:

- obstoj določene ali možne potrebe po dodatnih ukrepih za povečanje preglednosti in odgovornosti;
- pravica posameznika, na katerega se osebni podatki nanašajo, do ugovora zoper obdelavo, in poleg ugovora dostopnost zavrnitve brez potrebe po utemeljevanju;
- krepitev moči posameznikov, na katere se osebni podatki nanašajo: prenosljivost podatkov in dostopnost učinkovitih mehanizmov, s katerimi lahko posameznik, na katerega se osebni podatki nanašajo, dostopa do svojih podatkov ter jih spreminja, izbriše, pošlje ali kakor koli dodatno obdela (ali dovoli tretjim osebam nadaljnjo obdelavo).

IV.2 Priporočila

Trenutno besedilo člena 7(f) Direktive je mogoče razlagati na več načinov. Ta prožna ubeseditev pušča precej prostora za razlago in je včasih – kot so pokazale izkušnje – privedla do pomanjkanja predvidljivosti in pravne gotovosti. Vendar ima člen 7(f), če se uporablja v pravem kontekstu in skupaj s pravim merilom, kot je navedeno v tem mnenju, ključno vlogo kot pravna podlaga za zakonitost obdelave podatkov.

Delovna skupina zato podpira trenutni pristop v členu 6 predlagane uredbe, ki ohranja ravnovesje interesov kot ločeno pravno podlago. Za zagotovitev ustreznega izvajanja testa tehtanja bi bile vseeno dobrodošle dodatne smernice.

Področje uporabe in sredstva za dodatna pojasnila

Poglavitna zahteva bi bila, da določba ostane dovolj prožna ter da izraža tako vidike upravljavca podatkov in posameznika, na katerega se osebni podatki nanašajo, kot dinamično naravo ustreznih kontekstov. Zato delovna skupina meni, da določitev – v besedilu predlagane uredbe ali delegiranih aktih – podrobnih in izčrpnih seznamov primerov, v katerih bi bil interes opredeljen kot dejansko zakonit, ni priporočljiva. Delovna skupina bi nasprotovala

tudi določitvi primerov, v katerih bi interes ali pravica ene stranke *načeloma* ali *domnevno* prevladala nad interesom ali pravico druge stranke le zaradi narave takega interesa ali pravice ali zaradi sprejetja nekaterih zaščitnih ukrepov, na primer, podatki so bili le psevdonimizirani. To bi lahko bilo zavajajoče in po nepotrebnem predpisano.

Delovna skupina namesto sprejemanja dokončnih odločitev o vrednosti različnih pravic in interesov poudarja *ključno vlogo testa tehtanja* pri ocenjevanju člena 7(f). Obstaja potreba po ohranitvi prožnosti testa, vendar mora biti njegova izvedba v praksi učinkovitejša in omogočiti dejansko skladnost. To se mora kazati v *večji* obveznosti *odgovornosti* za upravljavce podatkov, ko mora upravljavec *dokazati*, da nad njegovim interesom ne prevladajo interesi in pravice posameznika, na katerega se osebni podatki nanašajo.

Smernice in odgovornost

Da bi to dosegli, delovna skupina priporoča, da se v predlagani uredbi zagotovijo smernice, in sicer tako:

1) koristno bi bilo opredeliti in v uvodni izjavi navesti neizčrpen seznam ključnih dejavnikov, ki bi jih bilo treba upoštevati pri testu tehtanja, kot so narava in vir zakonitega interesa, učinek na posameznike, na katere se osebni podatki nanašajo, ter dodatni zaščitni ukrepi, ki bi jih upravljavec lahko izvajal za preprečevanje vsakršnega neupravičenega učinka obdelave na te posameznike. Ti zaščitni ukrepi lahko med drugim zajemajo:
   - funkcionalno ločitev podatkov, ustrezno uporabo tehnik anonimizacije, šifriranje ter druge tehnične in organizacijske ukrepe za omejitev morebitnih tveganj za posameznike, na katere se osebni podatki nanašajo;
   - ob tem tudi ukrepe za zagotovitev večje preglednosti in izbire posameznikom, na katere se osebni podatki nanašajo, kot je, kadar je primerno, brezpogojna možnost zavrnitve obdelave, ki je brezplačna ter jo je mogoče preprosto in učinkovito priklicati;

2) delovna skupina bi podprla tudi, da se v predlagani uredbi dodatno pojasni, kako lahko upravljavec *dokaže*[111] večjo odgovornost.

   Sprememba pogojev, pod katerimi lahko posamezniki, na katere se osebni podatki nanašajo, uveljavljajo pravico do ugovora, kot je določena v členu 19 predlagane uredbe, je že pomemben element odgovornosti. Če bo posameznik, na katerega se osebni podatki nanašajo, ugovarjal obdelavi svojih podatkov na podlagi člena 7(f), bo moral v skladu s predlagano uredbo upravljavec podatkov dokazati, da prevladuje njegov interes. Delovna skupina odločno podpira to obrnitev dokaznega bremena, saj prispeva k obveznosti večje odgovornosti.

   Če upravljavec podatkov v nekem primeru posamezniku, na katerega se osebni podatki nanašajo, ne zmore dokazati, da njegov interes prevladuje, ima lahko to širše posledice za celotno obdelavo, ne le za posameznika, ki je ugovarjal. Posledično lahko upravljavec podvomi o obdelavi ali se jo odloči reorganizirati, po potrebi v korist ne le zadevnega posameznika, na katerega se osebni podatki nanašajo, ampak tudi v korist vseh drugih

[111] Tako dokazovanje mora ostati razumno in osredotočeno na rezultat, ne na administrativni postopek.

posameznikov, na katere se osebni podatki nanašajo, ki bi lahko bili v podobnem položaju.[112]

Ta zahteva je nujna, ne pa zadostna. Da bi bilo že od začetka zagotovljeno varstvo in da se prepreči obidenje obrnitve dokaznega bremena,[113] je pomembno, da se ukrepi izvedejo *pred* začetkom obdelave, ne le v poznejših postopkih „ugovora".

Zato se predlaga, da upravljavec podatkov v prvi fazi kakršne koli obdelave izvede nekaj ukrepov. Prva ukrepa bi lahko bila navedena v uvodni izjavi predlagane uredbe, tretji pa v posebni določbi:

- Opraviti oceno[114], ki bi morala zajemati različne faze analize, predstavljene v tem mnenju in povzete v Prilogi 1. Upravljavec bi moral izrecno opredeliti zadevni prevladujoči interes ali interese in navesti, zakaj ti prevladajo nad interesi posameznikov, na katere se osebni podatki nanašajo. Taka predhodna ocena ne bi smela biti preveč težavna in se mora še vedno *stopnjevati*: lahko je omejena na poglavitna merila, če je učinek obdelave na posameznike, na katere se osebni podatki nanašajo, na prvi pogled nepomemben, če pa je bilo ravnovesje težko doseči in bi zahtevala na primer sprejetje več dodatnih ukrepov, mora biti temeljitejša. Kadar je primerno – to je, ko postopek obdelave pomeni posebna tveganja za pravice in svoboščine posameznikov, na katere se osebni podatki nanašajo –, je treba izvesti

[112] Delovna skupina poleg obrnitve dokaznega bremena podpira tudi, da se v predlagani uredbi ne bi več zahtevalo, da ugovor temelji na „zakonitih in *nujnih* razlog[ih], povezanih [s] posebnim položajem" posameznika, na katerega se osebni podatki nanašajo. Nasprotno, v skladu s predlagano uredbo bi zadostovalo sklicevanje na katere koli (ne predvsem „nujne") zakonite razloge, povezane s posebnim položajem posameznika, na katerega se osebni podatki nanašajo. Pravzaprav je kot dodatna možnost, ki je bila predlagana v končnem poročilu odbora LIBE, tudi odprava zahteve, da bi moral biti ugovor povezan s posebnim položajem posameznika, na katerega se osebni podatki nanašajo. Delovna skupina podpira ta pristop, saj priporoča, da bi imeli posamezniki, na katere se osebni podatki nanašajo, možnost izkoristiti eno ali drugo možnost ali pa obe, če je to primerno, torej bodisi ugovarjati na podlagi svojega posebnega položaja bodisi s splošnega vidika, in v tem v zadnjem primeru ne da bi se od njih zahtevala posebna utemeljitev. Glej v tem smislu predlog spremembe 114 k členu 19(1) predlagane uredbe v končnem poročilu odbora LIBE.

[113] Upravljavce podatkov lahko na primer zamika, da bi se izognili temu, da bi za vsak posamezni primer dokazovali, da prevladuje njihov interes, tako da bi uporabljali standardne oblike utemeljevanja ali drugače otežili uveljavljanje pravice do ugovora.

[114] Ta ocena, kot je bilo navedeno v opombi 84, se ne sme zamenjevati s celovito oceno učinka na varstvo zasebnosti in podatkov. Trenutno ni celovitih smernic za ocene učinka na evropski ravni, čeprav je bilo na nekaterih področjih, zlasti na področju radiofrekvenčne identifikacije in pametnih meritev, nekaj dobrodošlega prizadevanja za opredelitev področne metodologije/okvira (in/ali predloge), ki bi se lahko uporabljali v vsej Evropski uniji. Glej Predlog industrije glede okvira ocene učinka na varstvo zasebnosti in podatkov za aplikacije radiofrekvenčne identifikacije (RFID) in Predlogo za oceno učinka na varstvo podatkov za pametno omrežje in pametne merilne sisteme, ki ju je pripravila strokovna skupina 2 projektne skupine za pametna omrežja Komisije. Delovna skupina je izdala več mnenj o obeh metodologijah.
Poleg tega je bilo danih nekaj pobud za opredelitev metodologije za oceno učinka na varstvo splošnih podatkov, od katere bi lahko imela korist „področna" prizadevanja. Glej na primer Projekt PIAF (Okvir za ocene učinka na zasebnost za pravice do varstva podatkov in zasebnosti): http://www.piafproject.eu/.
Za smernice na nacionalni ravni glej na primer metodologijo CNIL (francoski organ za varstvo podatkov) na naslovu:
http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf
in Privacy Impact Assessment Handbook ICO (urad informacijskega pooblaščenca v Združenem kraljestvu) na naslovu:
http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

celovitejšo oceno učinka na varstvo zasebnosti in podatkov (v skladu s členom 33 predlagane uredbe), pri čemer bi ocena na podlagi člena 7(f) postala pomemben del.

- Dokumentirati to oceno. Prav toliko, kolikor je mogoče *stopnjevati*, kako podrobno je treba opraviti oceno, bi moralo biti mogoče stopnjevati tudi obseg njenega dokumentiranja. Skratka, nekaj osnovne dokumentacije bi moralo biti na voljo v vseh, razen najbolj banalnih primerih, ne glede na oceno učinka obdelave na posameznika. Na podlagi take dokumentacije je mogoče nadalje oceniti in morda izpodbijati oceno upravljavca.

- Zagotoviti preglednost in prepoznavnost teh informacij za posameznike, na katere se osebni podatki nanašajo, in druge deležnike. Preglednost bi bilo treba zagotoviti za posameznike, na katere se osebni podatki nanašajo, in za organe za varstvo podatkov, kadar bi bilo primerno, tudi za širšo javnost. Delovna skupina se glede posameznikov, na katere se osebni podatki nanašajo, sklicuje na osnutek poročila odbora LIBE[115], v katerem je navedeno, da mora upravljavec posameznika, na katerega se osebni podatki nanašajo, obvestiti o razlogih, zakaj verjame, da nad njegovimi interesi ne prevladujejo interesi ali temeljne pravice in svoboščine posameznika, na katerega se osebni podatki nanašajo. Po mnenju delovne skupine je treba take informacije posameznikom, na katere se osebni podatki nanašajo, zagotoviti skupaj z informacijami, ki jih mora upravljavec zagotoviti na podlagi členov 10 in 11 veljavne direktive (člen 11 predlagane uredbe). To bo omogočilo morebitni ugovor posameznika, na katerega se osebni podatki nanašajo, v drugi fazi in dodatno utemeljitev upravljavca glede prevladujočih interesov v vsakem posameznem primeru. Poleg tega mora biti dokumentacija, na katero je upravljavec oprl oceno, dostopna organom za varstvo podatkov na njihovo zahtevo, da bi se omogočila preverjanje in pregon, kadar bi bilo primerno.

Delovna skupina bi podprla izrecno vključitev teh treh ukrepov v predlagano uredbo na zgoraj predstavljeni način. S tem bi se v predlaganem novem pravnem okviru priznala posebna vloga pravnih podlag pri ocenjevanju zakonitosti in pojasnil pomen testa tehtanja v širšem okviru ukrepov za odgovornost in ocen učinka.

Delovna skupina meni, da bi bilo tudi priporočljivo, da se Evropskemu odboru za varstvo podatkov po potrebi zagotovijo dodatne smernice na podlagi tega okvira. Ta pristop bi omogočil zadostno jasnost v besedilu in zadostno prožnost pri njegovem izvajanju.

[115] Osnutek poročila o predlogu uredbe Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Splošna uredba o varstvu podatkov) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

Priloga 1: Hiter vodnik za izvajanje testa tehtanja iz člena 7(f)

Korak 1: Oceniti, katera pravna podlaga se lahko uporablja v skladu s členom 7(a) do (f)

Obdelava podatkov se lahko izvaja le, če se uporablja ena ali več izmed šestih podlag – (a) do (f) – iz člena 7 (različne podlage se lahko uporabljajo v različnih fazah iste obdelave). Če je na prvi pogled očitno, da je člen 7(f) ustrezna pravna podlaga, nadaljujte na korak 2.

Hitri namigi:
− Člen 7(a) se uporablja le, če je dana svobodna, informirana, posebna in nedvoumna privolitev; dejstvo, da posameznik ni ugovarjal obdelavi na podlagi člena 14, se ne sme zamenjevati s privolitvijo iz člena 7(a) – vendar se lahko preprost mehanizem ugovora zoper obdelavo šteje za pomemben zaščitni ukrep v skladu s členom 7(f).
− Člen 7(b) zajema obdelavo, ki je potrebna za izvajanje pogodbe; samo zato, ker je obdelava podatkov povezana s pogodbo ali predvidena nekje v pogodbenih pogojih, ne pomeni nujno, da se uporablja ta pravna podlaga; če je primerno, je treba kot alternativo upoštevati člen 7(f).
− Člen 7(c) zadeva le jasne in natančno določene zakonske obveznosti iz zakonodaje EU ali države članice; v primeru nezavezujočih smernic (ki jih na primer sprejmejo regulativne agencije) ali tuje zakonske obveznosti je treba kot alternativo upoštevati člen 7(f).

Korak 2: Opredeliti interes kot „zakonit“ ali „nezakonit“

Da se interes šteje za zakonit, mora kumulativno izpolnjevati te pogoje:
− mora biti zakonit (to je v skladu z evropsko in nacionalno zakonodajo);
− mora biti dovolj jasno izražen, da omogoči izvedbo testa tehtanja interesov in temeljnih pravic posameznika, na katerega se osebni podatki nanašajo (to je dovolj konkreten);
− mora pomeniti dejanski in trenutni interes (to je ne biti spekulativen).

Korak 3: Ugotoviti, ali je obdelava potrebna za uresničitev zadevnega interesa

Za izpolnitev te zahteve je treba ugotoviti, ali obstajajo drugi manj vsiljivi načini za doseganje opredeljenega namena obdelave in služenje zakonitemu interesu upravljavca podatkov.

Korak 4: Vzpostaviti začasno ravnovesje na podlagi ocene, ali nad interesom upravljavca podatkov prevladajo temeljne pravice ali interesi posameznikov, na katere se osebni podatki nanašajo

− Upoštevati naravo interesov upravljavca (temeljna pravica, druga vrsta interesa, javni interes).
− Preučiti možno škodo za upravljavca, tretje osebe ali širšo skupnost, če se podatki ne obdelajo.
− Upoštevati naravo podatkov (občutljivi v ožjem ali širšem pomenu?).
− Upoštevati status posameznika, na katerega se osebni podatki nanašajo (mladoletna oseba, zaposleni itd.) in upravljavca (na primer, ali ima poslovna organizacija prevladujoč položaj na trgu).
− Upoštevati način obdelave podatkov (obsežna, podatkovno rudarjenje, oblikovanje profilov, razkritje veliko osebam ali objava).

− Opredeliti temeljno pravico in/ali interese posameznika, na katerega se osebni podatki nanašajo, na katere lahko učinkuje obdelava.
− Upoštevati razumna pričakovanja posameznikov, na katere se osebni podatki nanašajo.
− Preučiti učinke na posameznika, na katerega se osebni podatki nanašajo, in jih primerjati s koristjo, ki jo od obdelave pričakuje upravljavec podatkov.

Hitri namig: Upoštevati učinek dejanske obdelave na zadevne posameznike – ne glejte na to kot na abstraktno ali hipotetično vajo.

Korak 5: Vzpostaviti končno ravnovesje ob upoštevanju dodatnih zaščitnih ukrepov

Opredeliti in izvesti ustrezne dodatne zaščitne ukrepe, ki izhajajo iz dolžnosti vestnosti in skrbnosti, kot so:
− zmanjšanje količine podatkov (na primer stroge omejitve zbiranja podatkov ali takojšen izbris podatkov po uporabi),
− tehnični in organizacijski ukrepi za zagotovitev, da se podatki ne morejo uporabiti za sprejemanje odločitev ali drugih ukrepov v zvezi s posamezniki („funkcionalna ločitev“),
− širša uporaba tehnik anonimizacije, združevanje podatkov, tehnologije za boljše varovanje zasebnosti, vgrajena zasebnost, ocene učinka na varstvo zasebnosti in podatkov,
− večja preglednost, splošna in brezpogojna pravica do ugovora (zavrnitev), prenosljivost podatkov in povezani ukrepi za krepitev moči posameznikov, na katere se osebni podatki nanašajo.

Hitri namig: Uporaba tehnologij in pristopov za boljše varovanje zasebnosti lahko prevesi tehtnico v korist upravljavca podatkov in hkrati ščiti posameznike.

Korak 6: Dokazati skladnost in zagotoviti preglednost

− Pripraviti načrt korakov 1 do 5 za upravičenje obdelave pred njenim začetkom.
− Obvestiti posameznike, na katere se osebni podatki nanašajo, o razlogih, zakaj je tehtnica nagnjena v korist upravljavca.
− Dajati dokumentacijo na razpolago organom za varstvo podatkov.

Hitri namig: Ta korak se *stopnjuje*: podrobnosti ocene in dokumentacijo je treba prilagoditi naravi in kontekstu obdelave. Ti ukrepi bodo obsežnejši, ko se bo večja količina podatkov o številnih osebah obdelovala tako, da bo to lahko imelo velik učinek nanje. Celovita ocena učinka na varstvo zasebnosti in podatkov (v skladu s členom 33 predlagane uredbe) bo potrebna le, ko bo postopek obdelave pomenil posebna tveganja za pravice in svoboščine posameznikov, na katere se osebni podatki nanašajo. V teh primerih bo lahko ocena na podlagi člena 7(f) postala ključni del širše ocene učinka.

Korak 7: Kaj, če posameznik, na katerega se osebni podatki nanašajo, uveljavlja svojo pravico do ugovora?

− Kadar je kot zaščitni ukrep na voljo le kvalificirana pravica do zavrnitve (to se kot minimalni zaščitni ukrep izrecno zahteva na podlagi člena 14(a)): če posameznik, na katerega se osebni podatki nanašajo, ugovarja obdelavi, bi bilo treba zagotoviti, da je na voljo ustrezen in uporabnikom prijazen mehanizem za ponovno oceno ravnovesja, kar zadeva posameznika, in

ustavitev obdelave njegovih podatkov, če ponovna ocena pokaže, da njegovi interesi prevladajo.

− Kadar je kot dodatni zaščitni ukrep na voljo brezpogojna pravica do zavrnitve (ker se izrecno zahteva na podlagi člena 14(b) ali ker se sicer šteje za potreben ali koristen dodatni zaščitni ukrep): če posameznik, na katerega se osebni podatki nanašajo, ugovarja obdelavi, bi bilo treba zagotoviti, da se ta odločitev spoštuje, ne da bi bil potreben dodaten ukrep ali ocena.

Priloga 2: Praktični primeri za ponazoritev izvajanja testa tehtanja na podlagi člena 7(f)

V tej prilogi so navedeni primeri nekaterih najobičajnejših okoliščin, v katerih se lahko postavi vprašanje zakonitih interesov v smislu člena 7(f). Večinoma smo pod enim naslovom združili dva ali več povezanih primerov, ki jih je vredno primerjati. Številni primeri temeljijo na resničnih primerih ali elementih resničnih primerov, ki so jih obravnavali organi za varstvo podatkov v različnih državah članicah. Smo pa včasih nekoliko spremenili dejstva za boljšo ponazoritev, kako opraviti test tehtanja.

Primeri so vključeni za ponazoritev *miselnega procesa*, metode, ki jo je treba uporabiti za izvedbo testa tehtanja na podlagi več dejavnikov. Z drugimi besedami, namen primerov *ni* ponuditi *dokončne* ocene opisanih primerov. V številnih primerih se lahko namreč ob neki spremembi dejstev (na primer, če bi moral upravljavec sprejeti dodatne zaščitne ukrepe, kot so popolnejša anonimizacije, boljši varnostni ukrepi ter večja preglednost in pristnejša izbira za posameznike, na katere se osebni podatki nanašajo) spremeni rezultat testa tehtanja.[116]

To bi moralo spodbuditi upravljavce k boljšemu upoštevanju vseh horizontalnih določb Direktive in zagotoviti dodatno varstvo, kjer je to potrebno, na podlagi vgrajene zasebnosti in varstva podatkov. Skrbneje ko upravljavci varujejo osebne podatke na splošno, verjetneje je, da bodo uspešno opravili test tehtanja.

Uveljavljanje pravice do svobode izražanja ali obveščanja[117], tudi v medijih in umetnosti

Primer 1: Nevladna organizacija znova objavi podatke o izdatkih poslancev

Javni organ – na podlagi zakonske obveznosti (člen 7(c)) – objavi podatke o izdatkih poslancev; nevladna organizacija za preglednost pa te podatke analizira in znova objavi v točni in sorazmerni, vendar bolj informativni različici z opombami, s čimer prispeva k večji preglednosti in odgovornosti.

Ob domnevi, da nevladna organizacija te podatke točno in sorazmerno znova objavi z dodanimi opombami, sprejme ustrezne zaščitne ukrepe in širše spoštuje pravice zadevnih posameznikov, bi morala imeti možnost uporabiti člen 7(f) kot pravno podlago za obdelavo. Dejavniki, kot so narava zakonitega interesa (temeljna pravica do svobode izražanja ali obveščanja) in interes javnosti za preglednost in odgovornost ter dejstvo, da so bili podatki že objavljeni in gre za (razmeroma manj občutljive) osebne podatke v zvezi z dejavnostmi posameznikov, povezanimi z opravljanjem njihove javne funkcije,[118] potrjujejo zakonitost obdelave. Tudi to, da je bila prvotna objava zahtevana z zakonom in da bi posamezniki zato

[116] Ob pravilni uporabi člena 7(f) se lahko postavljajo vsestranska vprašanja glede ocenjevanja, za pomoč pri ocenjevanju pa imajo lahko pomembno vlogo posebna zakonodaja, sodna praksa, smernice, kodeksi ravnanja in drugi formalni ali manj formalni standardi.

[117] O svobodi izražanja ali obveščanja glej stran 34 tega mnenja. Pri presoji teh primerov je treba upoštevati tudi vsa ustrezna odstopanja iz nacionalne zakonodaje v zvezi z obdelavo v novinarske namene na podlagi člena 9 Direktive.

[118] Ni mogoče izključiti, da lahko nekateri izdatki razkrijejo bolj občutljive podatke, kot so podatki o zdravju. V tem primeru je treba take podatke izbrisati iz podatkovnega niza pred njihovo objavo. Dobra praksa je uporabiti „proaktivni pristop“, dati posameznikom priložnost, da pred objavo pregledajo svoje podatke, in jih jasno seznaniti z možnostmi in načini objave.

morali pričakovati, da bodo njihovi podatki objavljeni, prispeva k ugodni presoji. Na drugi stran tehtnice je učinek na posameznika lahko velik, na primer, ker se lahko zaradi javnega nadzora postavljajo vprašanja o osebni integriteti nekaterih posameznikov, kar lahko na primer privede do izgube volitev, v nekaterih primerih pa celo do kazenske preiskave goljufivih dejavnosti. Zgornji dejavniki skupaj vseeno kažejo, da pri tehtanju interesi upravljavca (in interesi javnosti, kateri podatki se razkrijejo) prevladajo nad interesi posameznikov, na katere se osebni podatki nanašajo.

Primer 2: Krajevni svetnik imenoval hčer za posebno pomočnico

Novinar v krajevnem spletnem časopisu objavi članek s točnimi in dobro raziskanimi podatki o lokalnem svetniku, v katerem razkrije, da se je ta udeležil le ene izmed zadnjih enajstih sej sveta in da verjetno ne bo znova izvoljen zaradi nedavnega škandala, ki je izbruhnil zaradi imenovanja njegove sedemnajstletne hčere za posebno pomočnico.

Tudi v tem primeru se uporabi podobna analiza kot v *primeru 1*. Glede na dejstva je objava informacij v zakonitem interesu zadevnega časopisa. Čeprav so bili razkriti osebni podatki o svetniku, nad temeljno pravico do svobode izražanja in objave zgodbe v časopisu ne prevlada svetnikova pravica do zasebnosti. To pa zato, ker so pravice do zasebnosti javnih osebnosti razmeroma omejene glede na njihove javne dejavnosti in zaradi posebnega pomena svobode izražanja – zlasti, kadar je objava zgodbe v javnem interesu.

Primer 3: Glavni rezultati iskanja še vedno prikazujejo lažje kaznivo dejanje

Spletni arhiv časopisa vsebuje star članek o posamezniku, nekoč slavni lokalni osebnosti, kapetanu amaterskega nogometnega kluba v majhnem mestu. Posameznik je imenovan s polnim imenom, zgodba pa se nanaša na njegovo vpletenost v kazenski postopek zaradi razmeroma lažjega kaznivega dejanja (kaljenje javnega reda in miru pod vplivom alkohola). Kazenska evidenca posameznika je zdaj prazna in v njej ni več preteklega kaznivega dejanja, zaradi katerega je pred več leti prestal kazen. Za posameznika je najbolj vznemirjajoče, da se pri iskanju njegovega imena v običajnih spletnih iskalnikih med prvimi rezultati prikaže povezava do tega starega članka. Časopis ne glede na njegovo zahtevo zavrača sprejetje tehničnih ukrepov, s katerimi bi omejili širšo dostopnost članka o posamezniku, na katerega se osebni podatki nanašajo. Na primer, časopis noče sprejeti tehničnih in organizacijskih ukrepov, s katerimi bi – kolikor tehnologija omogoča – omejil dostop do informacije iz zunanjih iskalnikov, v katerih bi se kot iskalna kategorija uporabilo posameznikovo ime.

To je še en primer za ponazoritev možnega navzkrižja med svobodo izražanja in zasebnostjo. Kaže tudi, da imajo lahko v nekaterih primerih dodatni zaščitni ukrepi – kot je zagotovitev, da vsaj v primeru utemeljenega ugovora na podlagi člena 14(a) Direktive upoštevni del časopisnega arhiva ne bo več dostopen iz zunanjega iskalnika ali da format, uporabljen za prikaz informacije, ne bo dovoljeval iskanja po imenu – ključno vlogo pri iskanju ustreznega ravnovesja med zadevnima temeljnima pravicama. To ne posega v druge ukrepe, ki bi jih lahko uporabili iskalniki ali druge tretje osebe.[119]

Tradicionalno neposredno trženje in druge oblike trženja ali oglaševanja

[119] Glej tudi zadevo C-131/12, Google Spain proti Agencia Española de Proteccion de Datos, ki se zdaj obravnava pred Sodiščem Evropske unije.

Primer 4: Računalniška trgovina kupcem oglašuje podobne izdelke

Računalniška trgovina ob prodaji izdelka pridobi od kupcev kontaktne podatke, ki jih uporabi za trženje lastnih podobnih izdelkov po navadni pošti. Trgovina izdelke prodaja tudi na spletu in pošilja reklamna elektronska sporočila, ko ima na zalogi nov program izdelkov. Kupci so jasno seznanjeni, da imajo možnost brezplačno in preprosto ugovarjati, ko se zberejo njihovi kontaktni podatki in vsakič, ko je sporočilo poslano, če temu niso ugovarjali že na začetku.

Preglednost postopka, to, da lahko kupec razumno pričakuje, da bo kot stranka trgovine prejel ponudbe za podobne izdelke, in to, da ima pravico do ugovora, pomagajo povečevati zakonitost obdelave in varujejo posameznikove pravice. Zdi se, da na drugi strani tehtnice ni nobenega nesorazmernega učinka na posameznikovo pravico do zasebnosti (v tem primeru smo domnevali, da računalniška trgovina ni oblikovala vsestranskih profilov za svoje kupce, na primer, tako da bi uporabila podrobno analizo podatkov o klikih).

Primer 5: Spletna lekarna obsežno oblikuje profile

Spletna lekarna izvaja trženje na podlagi zdravil in drugih izdelkov, ki so jih kupile stranke, vključno z izdelki, dobljenimi na recept. Te informacije – skupaj z demografskimi podatki o strankah, npr. njihovo starostjo in spolom – analizira za oblikovanje profila o „zdravju in dobrem počutju“ posameznih strank. Uporablja tudi podatke o klikih, ki se zberejo ne le o izdelkih, ki so jih stranke kupile, ampak tudi o drugih izdelkih in informacijah, ki so jih iskali na spletni strani. Profili strank zajemajo informacije ali napovedi, ki kažejo, da je neka stranka noseča, ima neko kronično bolezen ali bi jo v nekem letnem času zanimal nakup prehranskih dopolnil, losjona za porjavitev ali drugih izdelkov za nego kože. Analitiki spletne lekarne te informacije uporabljajo za ponujanje zdravil brez recepta, prehranskih dopolnil in drugih izdelkov določenim posameznikom po elektronski pošti. V tem primer se lekarna ne more sklicevati na zakonite interese, ko oblikuje in uporablja profile strank za trženje. Opisano oblikovanje profilov povzroča več težav. Informacije so posebno občutljive in lahko veliko razkrijejo o zadevah, za katere bi številni posamezniki pričakovali, da ostanejo zasebne.[120] Obseg in način oblikovanja profilov (uporaba podatkov o klikih, napovedni algoritmi) kažeta tudi na visoko stopnjo vsiljivosti. Privolitev na podlagi členov 7(a) in 8(2)(a) (ko gre za občutljive podatke) bi se vseeno lahko štela za alternativo, kjer bi bilo primerno.

[120] Poleg vseh omejitev, določenih z zakonodajo o varstvu podatkov, je v EU strogo urejeno tudi oglaševanje izdelkov na recept, obstajajo pa tudi nekatere omejitve za oglaševanje zdravil brez recepta. Poleg tega je treba upoštevati tudi zahteve iz člena 8 o posebnih vrstah podatkov (kot so podatki o zdravju).

Nezaželena nekomercialna sporočila, tudi v zvezi s političnimi kampanjami ali zbiranjem sredstev v dobrodelne namene

Primer 6: Kandidatka na lokalnih volitvah uporablja volilni imenik za svoj cilj

Kandidatka na lokalnih volitvah uporablja elektronski imenik[121] za pošiljanje predstavitvenih dopisov za obveščanje o svoji kampanji na prihajajočih volitvah vsem potencialnim volivcem v njenem volilnem okrožju. Kandidatka uporablja podatke, pridobljene iz volilnega imenika, le za pošiljanje dopisa in jih ne obdrži, ko je kampanja končana.

Taka uporaba lokalnega imenika je v mejah razumnih pričakovanj posameznikov, če se zgodi v predvolilnem obdobju: interes upravljavca je jasen in zakonit. Omejena in osredotočena uporaba informacij prispeva tudi k temu, da se tehtnica prevesi na stran zakonitih interesov upravljavca. Taka uporaba volilnih imenikov je lahko urejena tudi z zakoni na nacionalni ravni z vidika javnega interesa, ki določajo posebna pravila, omejitve in zaščitni ukrepi glede uporabe volilnega imenika. Če je tako, se za zagotovitev zakonitosti obdelave zahteva tudi upoštevanje teh posebnih pravil.

Primer 7: Neprofitna organizacija zbira informacije v ciljne namene

Filozofska organizacija, ki se ukvarja z razvojem človeka in družbe, se odloči organizirati zbiranje sredstev na podlagi profila svojih članov. V ta namen zbere podatke na družbenih omrežjih z začasno programsko opremo, ki izbere posameznike, ki jim je bila „všeč“ organizatorjeva stran, ki so jim bila „všeč“ sporočila organizacije, objavljena na strani, in so jih „delili“, ki so redno gledali nekatere prispevke ali širili tvite organizacije. Organizacija nato članom pošlje sporočila in novice na podlagi njihovih profilov. Na primer, starejši lastniki psov, ki so jim bili „všeč“ članki o zavetiščih za živali, prejmejo drugačna vabila za zbiranje sredstev kot družine z majhnimi otroki, tudi ljudje iz različnih etničnih skupin prejemajo različna sporočila.

Dejstvo, da se obdelujejo posebne vrste podatkov (filozofska prepričanja), zahteva upoštevanje člena 8, ta pogoj pa je očitno izpolnjen, saj se podatki obdelujejo v okviru zakonitih dejavnosti organizacije. Vendar v tem primeru to ni zadosten pogoj: način uporabe podatkov presega razumna pričakovanja posameznikov. Količina zbranih podatkov ter pomanjkljiva preglednost zbiranja in ponovne uporabe podatkov, prvotno objavljenih za en namen, za drug namen prispevata k ugotovitvi, da se v tem primeru ni mogoče opreti na člen 7(f). Obdelava torej ne bi smela biti dovoljena, razen če se uporabi druga podlaga, na primer privolitev posameznikov iz člena 7(a).

[121] Domneva se, da je v državi članici, za katero velja ta primer, volilni imenik vzpostavljen z zakonom.

Izvršba pravnih zahtevkov, skupaj z izterjavo dolgov v zunajsodnih postopkih

Primer 8: Spor o kakovosti obnovitvenih del

Stranka izpodbija kakovost obnovitvenih del, izvedenih v kuhinji, in zavrača plačilo celotne cene. Gradbeno podjetje posreduje upoštevne in sorazmerne podatke svojemu odvetniku, da bi ta lahko stranki poslal opomin in se dogovoril o rešitvi spora, če bo ta še vedno zavračala plačilo.

V tem primeru prvotni ukrepi gradbenega podjetja, ki uporabi osnovne podatke o posamezniku, na katerega se osebni podatki nanašajo (na primer ime, naslov, kontaktne podatke), za pošiljanje opomina temu posamezniku (neposredno ali prek odvetnika, kot v tem primeru), lahko še vedno spada na področje obdelave, potrebne za izvajanje pogodbe (člen 7(b)). Nadaljnje ukrepe[122], skupaj z vključitvijo agencije za izterjavo terjatev, pa bi bilo treba presoditi na podlagi člena 7(f) glede na, med drugim, njihovo vsiljivost in učinek na posameznika, na katerega se osebni podatki nanašajo, kot bo prikazano v naslednjem primeru.

Primer 9: Stranka izgine z avtomobilom, kupljenim na kredit

Stranka ne plača obrokov za drag športni avtomobil, kupljen na kredit, in nato izgine. Prodajalec avtomobilov najame tretjo osebo, „izterjevalca“. Izterjevalec opravi vsiljivo „kazensko“ preiskavo, pri kateri med drugim uporabi prakse, kot sta prikrit videonadzor in prisluškovanje.

Čeprav so interesi prodajalca avtomobilov in izterjevalca zakoniti, se tehtnica ne prevesi na njuno stran, ker so bile za zbiranje informacij uporabljene vsiljive metode, od katerih so nekatere izrecno prepovedane z zakonom (prisluškovanje). Sklepna ugotovitev bi bila drugačna, če bi na primer prodajalec avtomobilov ali izterjevalec opravila omejena preverjanja za potrditev kontaktnih podatkov posameznika, na katerega se osebni podatki nanašajo, da bi lahko začela sodni postopek.

Preprečevanje goljufije, zlorabe storitev ali pranja denarja

Primer 10: Preverjanje podatkov strank pred odprtjem bančnega računa

Finančna institucija uporablja razumne in sorazmerne postopke – v skladu z nezavezujočimi smernicami pristojnega vladnega organa za finančni nadzor –, da preveri identiteto vseh oseb, ki želijo odpreti račun. Vodi evidenco informacij, uporabljenih za preverjanje identitete osebe.

Interes upravljavca je zakonit, obdelava podatkov zajema le omejene in potrebne informacije (standardna praksa v panogi, ki jo posamezniki, na katere se osebni podatki nanašajo, lahko razumno pričakujejo, in ki jo priporočajo pristojni organi). Vzpostavljeni so ustrezni zaščitni ukrepi za omejitev vsakršnega nesorazmernega in neupravičenega učinka na posameznike, na katere se osebni podatki nanašajo. Upravljavec se torej lahko sklicuje na člen 7(f). Alternativno in kolikor se izvedeni ukrepi izrecno zahtevajo v veljavni zakonodaji, se lahko uporabi člen 7(c).

[122] Med državami članicami so zdaj razlike glede ukrepov, ki jih štejejo za potrebne za izvajanje pogodbe.

Primer 11: Izmenjava informacij za preprečevanje pranja denarja

Finančna institucija – po pridobitvi nasveta pristojnega organa za varstvo podatkov – uvede postopke, temelječe na posebnih in omejenih merilih, za izmenjavo podatkov o domnevni zlorabi pravil o preprečevanju pranja denarja z drugimi družbami v isti skupini, s strogo omejitvijo dostopa, varnostjo in prepovedjo vsakršne nadaljnje uporabe v druge namene.

Iz podobnih razlogov, kot so bili pojasnjeni zgoraj, in glede na dejstva zadeve je obdelavo podatkov mogoče opreti na člen 7(f). Alternativno in kolikor se izvedeni ukrepi izrecno zahtevajo v veljavni zakonodaji, se lahko uporabi člen 7(c).

Primer 12: Črni seznam nasilnih odvisnikov od drog

Skupina bolnišnic oblikuje skupni črni seznam „nasilnih“ posameznikov, ki iščejo droge, da bi jim prepovedala dostop do vseh zdravstvenih prostorov sodelujočih bolnišnic.

Tudi če je interes upravljavcev za zagotovitev varnosti prostorov zakonit, ga je treba tehtati s temeljno pravico do zasebnosti in drugimi nujnimi razmisleki, kot je potreba, da se zadevnih posameznikov ne izključi iz dostopa do zdravljenja. Dejstvo, da se obdelujejo občutljivi podatki (na primer podatki o zdravju, povezani z odvisnostjo od drog), še potrjuje ugotovitev, da v tem primeru obdelava malo verjetno sprejemljiva na podlagi člena 7(f).[123] Obdelava bi lahko bila sprejemljiva, če bi bila na primer urejena z zakonom, v katerem bi bili določeni posebni zaščitni ukrepi (preverjanja in nadzor, preglednost, preprečevanje samodejnih odločitev), s katerimi bi se zagotovilo, da obdelava ne bi privedla do diskriminacije ali kršitve temeljnih pravic posameznikov[124]. V zadnjem primeru bi se lahko kot pravna podlaga uporabil člen 7(c) ali (f) glede na to, ali poseben zakon zahteva ali le dovoljuje obdelavo.

Nadzor zaposlenih zaradi varnosti ali upravljanja

Primer 13: Delovni čas odvetnikov, uporabljen za izdajanje računov in dodeljevanje nagrad

Število zaračunljivih delovnih ur odvetnikov v odvetniški pisarni se obdeluje za izdajanje računov in določitev letnih nagrad. Sistem je pregledno predstavljen zaposlenim, ki imajo izrecno pravico izraziti nestrinjanje z ugotovitvami glede izdajanja računa in izplačila nagrad, o čemer se nato pogovorijo z vodstvom.

Obdelava se zdi potrebna zaradi zakonitih interesov upravljavca in videti je, da ni manj vsiljivega načina za doseganje namena. Zaradi vzpostavljenih zaščitnih ukrepov in postopkov je omejen tudi učinek na zaposlene. V tem primeru je torej lahko člen 7(f) ustrezna pravna podlaga. Mogoče je tudi trditi, da je obdelava za enega ali oba namena potrebna tudi za izvajanje pogodbe.

[123] Upoštevati je treba tudi zahteve iz člena 8 o posebnih vrstah podatkov (kot so podatki o zdravju).

[124] Glej Delovni dokument o črnih seznamih (WP 65), sprejet 3. oktobra 2002.

Primer 14: Elektronski nadzor nad uporabo spleta[125]

Delodajalec nadzira uporabo spleta svojih zaposlenih med delovnim časom zaradi preverjanja, da informacijske tehnologije družbe ne uporabljajo pretirano v zasebne namene. Zbrani podatki vsebujejo začasne datoteke in piškotke, ustvarjene na računalnikih zaposlenih, ki kažejo, katere spletne strani so obiskali in kaj so prenesli na računalnik med delovnim časom. Podatki se obdelujejo brez predhodnega posvetovanja s posamezniki, na katere se osebni podatki nanašajo, in predstavniki sindikata/sveta delavcev v družbi. Zadevni posamezniki tudi niso dobili zadostnih informacij o teh praksah.

Količina in narava zbranih podatkov pomenita velik poseg v zasebno življenje zaposlenih. Poleg sorazmernosti je pomemben dejavnik, ki ga je treba upoštevati, tudi preglednost praks, tesno povezana z razumnimi pričakovanji posameznikov, na katere se osebni podatki nanašajo. Tudi če ima delodajalec zakonit interes za omejitev časa, ki ga zaposleni porabijo za ogledovanje spletnih strani, ki niso neposredno povezane z njihovim delom, uporabljene metode ne izpolnjujejo zahtev testa tehtanja iz člena 7(f). Delodajalec bi moral uporabiti manj vsiljive metode (na primer omejitev dostopnosti nekaterih strani), o katerih bi se pogovoril in dogovoril s predstavniki zaposlenih ter o katerih bi zaposlene pregledno obvestil, kar bi bila dobra praksa.

Sheme za prijavo nepravilnosti

Primer 15: Sheme za prijavo nepravilnosti zaradi izpolnjevanja tujih zakonskih obveznosti

Evropska podružnica ameriške skupine uvede omejeno shemo za prijavo nepravilnosti za poročanje o resnih kršitvah na področju računovodstva in financ. Za subjekte skupine velja kodeks dobrega upravljanja, ki zahteva okrepitev postopkov notranjega nadzora in obvladovanja tveganja. Evropska podružnica mora zaradi mednarodnih dejavnosti drugim članom skupine v ZDA zagotavljati zanesljive finančne podatke. Shema je oblikovana tako, da je skladna z ameriško zakonodajo in smernicami, ki so jih določili nacionalni organi za varstvo podatkov v EU.

Eden izmed zaščitnih ukrepov je, da so zaposleni na usposabljanjih in z drugimi sredstvi dobili jasna navodila glede okoliščin, v katerih je treba uporabiti shemo. Opozorjeni so bili, da sheme ne smejo zlorabljati za, na primer, lažne ali neutemeljene obtožbe drugih zaposlenih. Pojasnjeno jim je bilo še, da lahko shemo uporabijo anonimno, če pa želijo, lahko navedejo svoje ime. V zadnjem primeru so zaposleni seznanjeni z okoliščinami, v katerih bodo informacije o njihovi identiteti sporočene njihovemu delodajalcu ali posredovane drugim agencijam.

Če bi se uvedba sheme zahtevala s skladu z evropsko zakonodajo ali zakonodajo države članice EU, bi obdelava lahko temeljila na členu 7(c). Vendar tuje zakonske obveznosti niso zakonska obveznost za namene člena 7(c), zato taka obveznost ne more upravičiti obdelave na podlagi člena 7(c). Obdelava lahko vseeno temelji na členu 7(f), na primer, če obstaja zakonit

[125] Nekaj držav članic meni, da je delno omejen elektronski nadzor lahko „potreben za izvajanje pogodbe“ in zato lahko temelji na pravni podlagi iz člena 7(b) namesto na podlagi iz člena 7(f).

interes za zagotavljanje stabilnosti finančnih trgov ali za preprečevanje korupcije ter če shema vsebuje zadostne zaščitne ukrepe v skladu s smernicami ustreznih regulativnih organov v EU.

Primer 16: Notranja shema za prijavo nepravilnosti brez skladnih postopkov

Družba za finančne storitve se odloči uvesti shemo za prijavo nepravilnosti, ker sumi, da so med zaposlenimi zelo razširjene tatvine in korupcija, in želi zaposlene spodbuditi k ovajanju drug drugega. Da bi prihranila nekaj denarja, se družba odloči za interno upravljanje sheme, za kar bodo skrbeli zaposleni v oddelku za človeške vire. Da bi zaposlene spodbudila k uporabi sheme, ponuja gotovinsko nagrado „brez postavljanja vprašanj“ tistim, katerih prijave nepravilnosti privedejo do odkritja neprimernega ravnanja in povračila denarja.

Družba ima zakonit interes za odkrivanje in preprečevanje tatvin in korupcije. Vendar je njena shema za prijavo nepravilnosti tako slabo oblikovana in brez zaščitnih ukrepov, da nad njenimi interesi prevladajo interesi in pravica do zasebnosti njenih zaposlenih – zlasti tistih, ki so lahko žrtve lažnih prijav, vloženih le zaradi finančne koristi. To, da se shema upravlja interno, ne pa, da jo upravlja neodvisna oseba, povzroča še eno težavo, to je pomanjkanje usposabljanja in navodil za njeno uporabo.

Fizična varnost, varnost informacijske tehnologije in spleta

Primer 17: Biometrično preverjanje v raziskovalnem laboratoriju

Znanstvenoraziskovalni laboratorij, ki preučuje smrtonosne viruse, uporablja sistem vstopa na podlagi biometričnih podatkov zaradi velikega tveganja za javno zdravje, če bi ti virusi ušli iz njegovih prostorov. Izvajajo se ustrezni zaščitni ukrepi, tudi to, da se biometrični podatki shranjujejo na osebnih karticah zaposlenih, in ne v centralnem sistemu.

Tudi če so podatki občutljivi v širšem pomenu besede, se obdelujejo v javnem interesu. Zato in zaradi dejstva, da so tveganja zlorabe manjša zaradi ustrezne uporabe zaščitnih ukrepov, je člen 7(f) ustrezna podlaga za obdelavo.

Primer 18: Skrite kamere za odkrivanje obiskovalcev in zaposlenih, ki kadijo

Družba uporablja skrite kamere za odkrivanje zaposlenih in obiskovalcev, ki v stavbi kadijo na mestih, kjer kajenje ni dovoljeno.

Čeprav ima upravljavec zakonit interes za zagotovitev upoštevanja pravil o prepovedi kajenja, so sredstva, uporabljena za dosego tega cilja, – splošno rečeno – nesorazmerna in po nepotrebnem vsiljiva. Na voljo so manj vsiljive in preglednejše metode (kot so detektorji dima in vidni znaki). Obdelava tako ni skladna s členom 6, ki zahteva, da morajo biti podatki „ne pretirani“ glede na namene, za katere se zbirajo in/ali naprej obdelujejo. Hkrati verjetno ne bo opravila niti testa tehtanja iz člena 7.

Znanstvene raziskave

Primer 19: Raziskava o učinkih razveze in brezposelnosti staršev na stopnjo izobrazbe otrok

Na podlagi raziskovalnega programa, ki ga je sprejela vlada in odobril pristojen odbor za etiko, se izvaja raziskava o razmerju med razvezo, brezposelnostjo staršev in stopnjo izobrazbe otrok. Čeprav niso opredeljena kot „posebna vrsta podatkov“, se raziskava osredotoča na vprašanja, ki bi jih številne družine obravnavale kot zelo zasebne osebne informacije. Raziskava bo omogočila posebno pomoč pri izobraževanju, namenjeno otrokom, ki bi sicer lahko začeli neopravičeno izostajati od pouka, dosegli nizko stopnjo izobrazbe, bili kot odrasli brezposelni in se ukvarjali s kriminalnimi dejavnostmi. Zakonodaja zadevne države članice izrecno dovoljuje obdelavo osebnih podatkov (ki niso posebne vrste podatkov) v raziskovalne namene, če je raziskava potrebna in v nujnem javnem interesu ter se izvaja ob upoštevanju ustreznih zaščitnih ukrepov, ki so nato dodatno opredeljeni v izvedbenih predpisih. Ta zakonski okvir vsebuje posebne zahteve, okvir odgovornosti, ki omogoča oceno dopustnosti raziskave (če se izvaja brez privolitve zadevnih posameznikov) v vsakem posameznem primeru, in posebne ukrepe, ki jih je treba izvajati za zaščito posameznikov, na katere se osebni podatki nanašajo.

Raziskovalec vodi varovan raziskovalni objekt, ustrezne informacije pa na varen način dobiva od matičnega urada, sodišč, zavodov za zaposlovanje in šol. Raziskovalno središče nato prikrije identiteto posameznikov, tako da je mogoče povezati razvezo, brezposelnost in izobrazbo, ne da bi se razkrila „državljanska“ identiteta posameznikov, na primer njihova imena in naslovi. Vsi izvirni podatki se nato nepreklicno izbrišejo. Izvajajo se tudi dodatni ukrepi za zagotovitev funkcionalne ločitve (da se bodo podatki uporabili le v raziskovalne namene) in zmanjšanje vsakršnega nadaljnjega tveganja ponovne identifikacije.

Zaposleni v raziskovalnem središču so deležni strogega varnostnega usposabljanja in so osebno – mogoče celo kazensko – odgovorni za vsako kršitev varnosti podatkov, za katere so odgovorni. Tehnični in organizacijski ukrepi se izvajajo na primer za zagotovitev, da zaposleni, ki uporabljajo ključe USB, osebnih podatkov ne bi mogli odnesti iz objekta.

Raziskovalno središče ima zakonit interes za izvedbo raziskave, ki je tudi v velikem javnem interesu. Raziskava je tudi v zakonitem interesu organov za zaposlovanje, izobraževalnih ustanov in drugih organov, ki sodelujejo v programu, ker jim bo pomagala načrtovati in nuditi storitve tistim, ki jih najbolj potrebujejo. Vidiki zasebnosti programa so bili dobro pripravljeni, vzpostavljeni zaščitni ukrepi pa pomenijo, da nad zakonitimi interesi organizacij, ki sodelujejo pri raziskavi, ne prevladajo interesi ali pravice do zasebnosti staršev ali otrok, katerih podatki so bili podlaga za raziskavo.

Primer 20: Raziskava o debelosti

Univerza želi izvesti raziskavo o stopnjah debelosti pri otrocih v več mestih in podeželskih skupnostih. Čeprav ima običajno težave pri pridobivanju ustreznih podatkov od šol in drugih institucij, ji uspe prepričati nekaj deset šolskih učiteljev, da v nekem obdobju v svojih razredih spremljajo otroke, ki se zdijo debeli, in jim postavijo vprašanja o njihovi prehrani, stopnji telesne dejavnosti, uporabi računalniških igric in tako naprej. Ti šolski učitelji si zapisujejo tudi imena in naslove vprašanih otrok, da se jim lahko pošlje kupon za spletno glasbo kot nagrada za sodelovanje v raziskavi. Raziskovalci sestavljajo zbirko podatkov o otrocih, pri čemer stopnje debelosti povezujejo s telesno dejavnostjo in drugimi dejavniki. Celotni vprašalniki na papirju – še vedno v obliki, iz katere je razvidna identiteta posameznih otrok – se hranijo v arhivu univerze za nedoločeno obdobje in brez ustreznih varnostnih ukrepov. Fotokopije vseh vprašalnikov se na prošnjo dajo vsakemu podiplomskemu študentu

iste ali partnerske univerze po vsem svetu, ki jih zanima nadaljnja uporaba raziskovalnih podatkov.

Čeprav ima univerza zakonite interese za izvedbo raziskave, več vidikov oblike raziskave pomeni, da nad temi interesi prevladajo interesi in pravice do zasebnosti otrok. Poleg raziskovalne metode, ki ni dovolj znanstveno natančna, težave povzročata zlasti pomanjkanje pristopov za boljše varovanje zasebnosti pri pripravi raziskave in širok dostop do zbranih osebnih podatkov. Podatki o otrocih niso nikoli kodirani ali anonimizirani, prav tako se ne izvaja noben ukrep za zagotovitev varnosti podatkov ali funkcionalne ločitve. Tudi veljavna privolitev iz členov 7(a) in 8(2)(a) ni pridobljena in ni jasno, ali je bilo otrokom in njihovim staršem pojasnjeno, za kaj se bodo uporabili njihovi osebni podatki oziroma komu bodo posredovani.

Tuja zakonska obveznost

Primer 21: Izpolnjevanje zahtev davčne zakonodaje tretje države

Evropske banke zbirajo in pošiljajo nekatere podatke o svojih strankah, zato da ti izpolnjujejo davčne obveznosti tretjih držav. Zbiranje in pošiljanje sta opredeljena in se izvajata pod pogoji in ob upoštevanju zaščitnih ukrepov, ki sta jih EU in tuja država določili v mednarodnem sporazumu.

Tuje obveznosti same po sebi ni mogoče šteti za zakonito podlago za obdelavo na podlagi člena 7(c), vendar se lahko šteje za zakonito, če je taka obveznost določena v mednarodnem sporazumu. V zadnjem primeru se obdelava lahko šteje za potrebno za skladnost z zakonsko obveznostjo, ki je v notranji pravni okvir vključena z mednarodnim sporazumom. Če takega sporazuma ni, bo treba zbiranje in prenos presojati na podlagi zahtev iz člena 7(f), za dopustna pa se lahko štejeta le, če so vzpostavljeni ustrezni zaščitni ukrepi, kakršne odobri pristojni organ za varstvo podatkov (glej tudi *primer 15* zgoraj).

Primer 22: Pošiljanje podatkov o disidentih

Evropska družba na podlagi zahteve pošilja podatke o tujih rezidentih represivnemu režimu tretje države, ki želi dostopati do podatkov o disidentih (na primer podatke o prometu njihovih elektronskih sporočil, vsebino teh sporočil, zgodovino brskanja ali zasebna sporočila na družbenih omrežjih).

V tem primeru – drugače kot v prejšnjem – ni mednarodnega sporazuma, ki bi dovoljeval uporabo člena 7(c) kot pravne podlage. Poleg tega več dejavnikov nasprotuje temu, da se kot ustrezna podlaga za obdelavo uporabi člen 7(f). Čeprav ima lahko upravljavec ekonomski interes, da izpolnjuje zahteve tuje vlade (sicer ga lahko vlada tretje države obravnava manj ugodno kot druge družbe), sta zakonitost in sorazmernost pošiljanja podatkov zelo sporna glede na okvir EU o temeljnih pravicah. Tudi morebiten velik učinek tega pošiljanja na zadevne posameznike (na primer diskriminacija, zaporna kazen, smrtna kazen) tehtnico prevesi v korist interesov in pravic teh posameznikov.

Ponovna uporaba javno dostopnih podatkov

Primer 23: Ocenjevanje politikov[126]

Nevladna organizacija, ki se ukvarja s preglednostjo, uporablja javno dostopne podatke o politikih (obljube, dane ob izvolitvi, in podatke o dejanskem glasovanju), da jih preuči na podlagi tega, kako dobro so izpolnili svoje obljube.

Tudi če je lahko učinek na zadevne politike precejšen, dejstvo, da obdelava temelji na javno dostopnih informacijah, je povezana z njihovimi javnimi pooblastili ter ima jasen namen povečati preglednost in odgovornost, tehtnico prevesi na stran interesov upravljavca.[127]

Otroci in druge ranljive osebe

Primer 24: Spletne strani z informacijami za najstnike

Nevladna organizacija, ki na svoji spletni strani svetuje najstnikom glede vprašanj, kot so zloraba drog, neželena nosečnost in zloraba alkohola, na svojem strežniku zbira podatke o obiskovalcih te spletne strani. Te podatke nato takoj anonimizira in spremeni v splošne statistične podatke o tem, kateri deli spletne strani so najbolj priljubljeni pri obiskovalcih iz različnih geografskih območij države.

Člen 7(f) bi se lahko uporabil kot pravna podlaga, tudi če gre za podatke o ranljivih posameznikih, ker je obdelava v javnem interesu in so vzpostavljeni strogi zaščitni ukrepi (podatki so takoj anonimizirani in se uporabljajo le za pripravo statistike), zaradi česar se tehtnica prevesi na stran upravljavca.

Vgrajena zasebnost kot dodaten zaščitni ukrep

Primer 25: Dostop do mobilnih telefonskih številk uporabnikov in neuporabnikov aplikacije: „primerjaj in pozabi“

Osebni podatki posameznikov se obdelajo zaradi preverjanja, ali so v preteklosti že dali nedvoumno privolitev (to je „primerjaj in pozabi“ kot zaščitni ukrep).

Od razvijalca aplikacije se zahteva, da pridobi nedvoumno privolitev posameznikov, na katere se osebni podatki nanašajo, za obdelavo njihovih osebnih podatkov: na primer, razvijalec želi dostopati do celotnega elektronskega imenika uporabnikov aplikacije in zbrati vse podatke, skupaj z mobilnimi telefonskimi številkami kontaktov, ki ne uporabljajo aplikacije. Da to lahko stori, mora najprej presoditi, ali so imetniki mobilnih telefonskih številk v imenikih uporabnikov aplikacije dali nedvoumno privolitev (na podlagi člena 7(a)), da se njihovi podatki obdelajo.

Za to omejeno začetno obdelavo (to je kratkotrajni dostop za branje celotnega imenika uporabnika aplikacije) se razvijalec aplikacije lahko opre na člen 7(f) kot pravno podlago, če

[126] Glej za primerjavo *primer 7* zgoraj.

[127] Kot v *primerih 1 in 2* smo domnevali, da je objava točna in sorazmerna – pomanjkanje zaščitnih ukrepov in drugi dejavniki lahko spremenijo ravnovesje interesov glede na dejstva zadeve.

upošteva zaščitne ukrepe. Ti zaščitni ukrepi bi morali zajemati tehnične in organizacijske ukrepe za zagotovitev, da družba ta dostop uporablja le kot pomoč uporabniku, da ugotovi, kateri izmed njegovih kontaktov je že uporabnik in kateri je torej v preteklosti že dal nedvoumno privolitev družbi za zbiranje in obdelavo telefonskih številk v ta namen. Mobilne telefonske številke neuporabnikov se lahko zbirajo in uporabljajo le za strogo omejen cilj preverjanja, ali so dali nedvoumno privolitev za obdelavo svojih podatkov, takoj zatem pa jih je treba izbrisati.

Povezovanje osebnih podatkov prek spletnih storitev

Primer 26: Povezovanje osebnih podatkov prek spletnih storitev

Spletno podjetje, ki ponuja razne storitve, vključno z iskalnikom, souporabo videoposnetkov in navezovanjem stikov prek družbenih omrežij, pripravi pravilnik o zasebnosti, ki vsebuje klavzulo, ki mu omogoča, da „povezuje vse osebne podatke“, zbrane o vseh svojih uporabnikih v zvezi z različnimi storitvami, ki jih uporabljajo, ne da bi bilo opredeljeno obdobje hrambe podatkov. Po mnenju družbe to „zagotavlja najboljšo možno kakovost storitve“.

Družba oblikuje nekaj orodij, ki so na voljo različnim kategorijam uporabnikov, da lahko uveljavljajo svoje pravice (na primer izklop ciljnega oglaševanja, ugovor zoper nastavitev določene vrste piškotkov).

Vendar razpoložljiva orodja uporabnikom ne omogočajo dejanskega nadzora nad obdelavo njihovih podatkov: uporabniki ne morejo nadzirati posebnih povezav svojih podatkov prek spletnih storitev in ne morejo ugovarjati povezovanju podatkov o sebi. Na splošno obstaja neravnovesje med zakonitim interesom družbe in varstvom temeljnih pravic uporabnikov, zato se člen 7(f) ne sme uporabiti kot pravna podlaga za obdelavo. Primernejša podlaga bi bil člen 7(a), če so izpolnjeni pogoji za veljavno privolitev.