Zadeva C-60/22

Povzetek predloga za sprejetje predhodne odločbe v skladu s členom 98(1) Poslovnika Sodišča

Datum vložitve:

1. februar 2022

Predložitveno sodišče:

Verwaltungsgericht Wiesbaden (Nemčija)

Datum predložitvene odločbe:

27. januar 2022

Tožeča stranka:

UZ

Tožena stranka:

Bundesrepublik Deutschland

Predmet postopka v glavni stvari

Pravo o varstvu podatkov – Uredba 2016/679 (Splošna uredba o varstvu podatkov) – Člen 5(2) – Odgovornost – Člen 17(1)(d) in člen 18(1)(b) – Zakonitost obdelave – Zahteva za izbris ali omejitev – Uporaba obdelanih podatkov

Predmet in pravna podlaga predloga za sprejetje predhodne odločbe

Razlaga prava Unije, člen 267 PDEU

Vprašanja za predhodno odločanje

1. Ali neobstoj odgovornosti oziroma opuščena ali nepopolna odgovornost upravljavca iz člena 5 Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov), na primer zaradi neobstoja

ali nepopolne evidence dejavnosti obdelave na podlagi člena 30 Splošne uredbe o varstvu podatkov ali neobstoja dogovora o skupnem postopku na podlagi člena 26 Splošne uredbe o varstvu podatkov, vodi do tega, da je obdelava podatkov nezakonita v smislu člena 17(1)(d) Splošne uredbe o varstvu podatkov in člena 18(1)(b) Splošne uredbe o varstvu podatkov, tako da ima posameznik, na katerega se nanašajo osebni podatki, pravico zahtevati izbris oziroma omejitev?

2. Če je odgovor na prvo vprašanje pritrdilen: ali obstoj pravice zahtevati izbris ali omejitev vodi do tega, da se obdelanih podatkov v sodnem postopku ne sme upoštevati? Vsaj takrat, ko posameznik, na katerega se nanašajo osebni podatki, ugovarja uporabi v sodnem postopku?

3. Če je odgovor na prvo vprašanje nikalen: ali upravljavčeva kršitev členov 5, 30 ali 26 Splošne uredbe o varstvu podatkov vodi do tega, da sme nacionalno sodišče pri vprašanju sodne uporabe obdelave podatkov podatke upoštevati le, če posameznik, na katerega se nanašajo osebni podatki, z uporabo izrecno soglaša?

Navedene določbe prava Unije

Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL 2016, L 119, str. 1), uvodna izjava 82, členi 5, 9, 17, 18, 26, 30, 94

Direktiva 2013/32/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o skupnih postopkih za priznanje ali odvzem mednarodne zaščite (UL 2013, L 180, str. 60), uvodna izjava 52

Listina Evropske unije o temeljnih pravicah, člena 7 in 8

Navedene nacionalne določbe

Bundesdatenschutzgesetz (zvezni zakon o varstvu podatkov; v nadaljevanju: BDSG) (BGBl. I, str. 2097), člen 43(3)

Kratka predstavitev dejanskega stanja in postopka

1 Tožeča stranka izpodbija zavrnilno odločbo Bundesamt für Migration und Flüchtlinge (zvezni urad za migracije in begunce, Nemčija) in predlaga, da se mu v skladu s členom 3 Asylgesetz (zakon o azilu; v nadaljevanju: AsylG) prizna status begunca. Odločba tožene stranke temelji na tako imenovanem elektronskem spisu zveznega urada MARIS, ki se ga tudi v okviru skupnega postopka na podlagi člena 26 sodišču posreduje prek elektronskega poštnega predala za sodne in upravne zadeve (EGVP). Glede vprašanj o celovitem posredovanju spisa se

[sodišče] sklicuje na vprašanja, ki so bila Sodišču že predložena (zadeva C-564/21).

2 Obstaja dvom, ali ima tožena stranka sploh evidenco o dejavnostih obdelave v smislu člena 30 Uredbe 2016/679 (Splošna uredba o varstvu podatkov) glede tako imenovanega elektronskega spisa MARIS oziroma ali je ta popolna. Prav tako ne obstaja noben dogovor oziroma zakonska ureditev v smislu člena 26 Splošne uredbe o varstvu podatkov glede postopka elektronskega posredovanja spisov in določitve odgovornosti v tem postopku. Predložitveno sodišče je te listine zahtevalo med postopkom. Tožena stranka pa je njihovo predložitev zavrnila med drugim z utemeljitvijo, da glede EGVP ne obstaja dogovor na podlagi člena 26 Splošne uredbe o varstvu podatkov.

Kratka predstavitev obrazložitve predloga za sprejetje predhodne odločbe

3 Postavlja se vprašanje, kako naj sodišče vsaj v primeru (formalne) nezakonitosti obdelave osebnih podatkov tožeče stranke pri toženi stranki ravna s temi podatki, saj se v skladu z Direktivo 2013/32 na podlagi nacionalnega prava v azilnih postopkih uporablja Splošna uredba o varstvu podatkov. Niti Asylgesetz (zakon o azilu) niti Verwaltungsgerichtsordnung (zakon o upravnem sporu) glede tega ne vsebujeta navedb.

4 V skladu z uvodno izjavo 52 Direktive 2013/32 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 ureja obdelavo osebnih podatkov, ki jo v azilnih postopkih v skladu s to direktivo izvajajo države članice. Direktiva 95/46 je bila v skladu s členom 94(1) Splošne uredbe o varstvu podatkov razveljavljena z učinkom od 25. maja 2018. Kljub temu se v skladu s členom 94(2) Splošne uredbe o varstvu podatkov sklicevanja na razveljavljeno Uredbo 95/46 štejejo kot sklicevanja na to uredbo. Zato se Splošna uredba o varstvu podatkov v celoti uporablja v postopkih za priznanje mednarodne zaščite.

5 Že v Direktivi 95/46 je bila predvidena dokumentacija avtomatskega postopka obdelave, tako imenovano uradno obveščanje na podlagi člena 18 te direktive. Vsebina uradnega obvestila iz člena 19 Direktive 95/46 je v bistvenem ustrezala sedanjemu členu 30 Splošne uredbe o varstvu podatkov, pri čemer se nova določba nanaša na vse oblike obdelave, torej tudi na zbirke podatkov.

6 V času veljavnosti Direktive 95/46 je tožena stranka v zvezi z elektronskim spisom MARIS razpolagala le z zelo rudimentarno evidenco obdelave kot uradno obveščanje v smislu Direktive 95/46 (člen 4e BDSG stara različica). Tedanja evidenca obdelave (uradno obveščanje) ni vsebovala posebne ureditve glede ravnanja s posebnimi vrstami osebnih podatkov iz člena 9 Splošne uredbe o varstvu podatkov (člen 8 Direktive 95/46). Tudi vse do današnjega dne naj ne bi bilo take posebne ureditve glede ravnanja s podatki iz člena 9 in 10 Splošne uredbe o varstvu podatkov. Na splošno se v elektronski spis MARIS namreč enako kot kazenske obsodbe, kot tako imenovane „običajne listine“, vnašajo

podatki v zvezi z zdravjem in podatki o verskem prepričanju. Posebna zaščita glede varnosti podatkov ni razvidna, razen da menda obstaja beleženje dostopov. Vendar pa je mogoče v spis prosilca za azil vpogledati tako iz vsake izpostave tožene stranke po vsej Nemčiji kot tudi iz same centrale.

7 Predložitveno sodišče ravno glede vodenja spisov in predložitve spisov sodišču resno dvomi, da tožena stranka upošteva zahteve iz člena 5(1) Splošne uredbe o varstvu podatkov na primer v povezavi s členoma 26 in 30 Splošne uredbe o varstvu podatkov. Kljub pozivu sodišča evidenca o dejavnostih obdelave ni bila predložena. Po odločitvi Sodišča glede odgovornosti iz člena 5(2) Splošne uredbe o varstvu podatkov namerava sodišče v zvezi s tem zaslišati vodjo pristojnega organa, torej tožene stranke.

8 Pred zaslišanjem pa je treba pojasniti, ali opustitev obveznosti iz Splošne uredbe o varstvu podatkov in s tem povezana nezakonitost obdelave podatkov vodi do sankcije, kot je izbris podatkov na podlagi člena 17(1)(d) Splošne uredbe o varstvu podatkov ali omejitve obdelave na podlagi člena 18(1)(b) Splošne uredbe o varstvu podatkov. To velja vsaj tedaj, ko to zahteva posameznik, na katerega se nanašajo osebni podatki, v tem primeru tožeča stranka. Sicer bi bilo sodišče namreč prisiljeno, da v okviru sodnega postopka sodeluje pri nezakoniti obdelavi podatkov. Organ bi lahko stalno nekaznovano kršil Splošno uredbo o varstvu podatkov.

9 V takem primeru bi lahko ukrepal le nadzorni organ na podlagi člena 58 Splošne uredbe o varstvu podatkov. Izrek upravne globe Bundesamt für Migration und Flüchtlinge (zvezni urad za migracije in begunce) pa po nacionalnem pravu ne bi prišel v poštev. V skladu s členom 43(3) BDSG, ki temelji na členu 83(7) Splošne uredbe o varstvu podatkov, se organom in drugim javnim službam ne izreka upravnih glob. Organ ne bi imel nobene spodbude, da bi ravnal zakonito. To bi imelo za posledico, da ne bi bile upoštevane niti zahteve iz Direktive 2013/32 niti zahteve iz Splošne uredbe o varstvu podatkov.

10 Sodišče Evropske unije je že odločilo, da mora v trenutku obdelave obstajati popolno „uradno obvestilo“ (danes: evidenca dejavnosti obdelave), včasih ni bilo tako (zadevi C-92/09 in C-93/09, sodba z dne 9. novembra 2011, ECLI:EU:C:2010:662, točka 95 in naslednje). V obravnavanem primeru je tožena stranka osebne podatke tožeče stranke obdelovala že od trenutka, ko je ta vložila prošnjo za azil (dne 7. maja 2019). Tako bi morala v tem trenutku vsaj na podlagi sodne prakse Sodišča obstajati popolna evidenca o dejavnostih obdelave glede spisa MARIS (in torej za azilni spis tožeče stranke). To pa ni tako.

11 Sodišče Evropske unije doslej niti na podlagi Direktive 95/46 niti na podlagi Splošne uredbe o varstvu podatkov ni odločilo, kaj velja v takem primeru. Če bi šteli, da mora upravljavec ali obdelovalec kot dokaz skladnosti s Splošno uredbo o varstvu podatkov voditi evidenco o dejavnostih obdelave, za katere je odgovoren (uvodna izjava 82 Splošne uredbe o varstvu podatkov), se postavi vprašanje,

kakšna je posledica opustitve organa, ki je odgovoren. Potem namreč ni mogoče upoštevati odgovornosti na podlagi člena 5 Splošne uredbe o varstvu podatkov.

12 Člen 83(5)(a) Splošne uredbe o varstvu podatkov sicer določa, da se lahko kršitve odgovornosti na podlagi člena 5 Splošne uredbe o varstvu podatkov kaznuje z upravnimi globami do 20.000.000 EUR. Tega pa – kot že navedeno – v skladu s členom 43(3) BSDG za zvezne organe ni mogoče uporabiti. Vsekakor pa člen 17(1)(d) Splošne uredbe o varstvu podatkov določa, da je treba nezakonito obdelane podatke brisati vsaj na zahtevo posameznika, na katerega se nanašajo osebni podatki.

13 Neobstoj evidence oziroma nepopolna evidenca dejavnosti obdelave vsaj ob upoštevanju člena 5 Splošne uredbe o varstvu podatkov po prepričanju predložitvenega sodišča vodi do „formalne“ nezakonitosti obdelave podatkov. Zato se postavlja vprašanje, ali v takem primeru kot sankcijo za opustitev na podlagi člena 5 Splošne uredbe o varstvu podatkov v povezavi s členom 30 Splošne uredbe o varstvu podatkov ne bilo treba opraviti izbrisa ali vsaj blokiranja podatkov. Sicer namreč, zaradi neobstoja možne sankcije, ne bi bilo mogoče učinkovito izvrševati Splošne uredbe o varstvu podatkov.

14 Konec koncev je – kolikor je znano – na primer Francoska republika v času veljavnosti člena 18 in naslednjih Direktive 95/46 v nacionalnem pravu določila, da v sodnih postopkih velja stroga zakonska prepoved uporabe tistih osebnih podatkov, ki niso bili zajeti v uradnem obveščanju odgovornega organa nadzornemu organu (nacionalna komisija za informatiko in svoboščine; v nadaljevanju: CNIL), saj je bila uporaba podatkov zaradi neobstoja dokumentacije nezakonita. Tako je v obravnavanem primeru do sankcije prišlo vsaj tako, da podatkov pri sodišču ni bilo dovoljeno obdelati in uporabiti. V času veljavnosti Splošne uredbe o varstvu podatkov naj bi tudi na Portugalskem in v drugih državah članicah neobstoj evidence dejavnosti obdelave vodil do prepovedi uporabe. V Zvezni republiki Nemčiji tak mehanizem v okviru prenosa Direktive 95/46 in tudi v času veljavnosti Splošne uredbe o varstvu podatkov ne obstaja. V tej državi je bil nasprotno postavljen temelj za „dopuščanje“ neobstoja uradnega obveščanja.

15 Tudi elektronsko posredovanje spisa in vlog tožene stranke je obdelava podatkov v smislu člena 4, točka 2, Splošne uredbe o varstvu podatkov, pri kateri je treba upoštevati načela obdelave podatkov na podlagi člena 5 Splošne uredbe o varstvu podatkov. Zato je mogoče tudi tu dvomiti v formalno zakonitost obdelave podatkov s posredovanjem tako imenovanega elektronskega zveznega spisa in vlog tožene stranke glede na posamezni način prenosa. Tudi tu ni evidence dejavnosti obdelave in ureditve o skupni odgovornosti. Obstaja sicer Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach z dne 24. novembra 2017 (uredba o okvirnih tehničnih pogojih elektronskega poslovanja in posebnem elektronskem poštnem predalu za sodne in upravne zadeve, BGBl. I, str. 3803, kot je bila spremenjena s členom 6 zakona z dne 5. oktobra 2021, BGBl. I, str. 4607).

Ureja posredovanje elektronskih dokumentov sodiščem [zveznih] dežel in zvezne države. Pri tem lahko najvišji organi zvezne države ali deželnih vlad za svoje področje pri javnopravnih službah preverijo identiteto organov ali pravnih oseb javnega prava, da bi jim dovolili dostop do Besonderes elektronisches Behördenpostfach (posebni uradni elektronski poštni predal) (tako imenovani BeBPo). Najvišji organi zvezne države ali več deželnih vlad lahko tudi skupaj za svoja področja določijo javnopravno službo. Kdo bi to dejansko bil, ni bilo določeno. Nazadnje za tem verjetno stoji tako imenovana Bund-Länder-Arbeitsgruppe der Justizministerien (zvezna in deželna delovna skupina pravosodnih ministrstev) (Bund-Länder-Kommission für Informationstechnik in der Justiz [BLK] Arbeitsgruppe IT-Standards in der Justiz, zvezna in deželna komisija za informacijsko tehniko v pravosodju [BLK] delovna skupina standardi IT v pravosodju). Kateri organ ali organi so odgovorni za evidenčno službo EGVP ali BeBPo ali celo potrebne strežniške strukture, ni znano in ni dokumentirano.

16 Prav tako ni nobenih ustreznih zakonskih ali siceršnjih pisnih pravil med sodišči in organi, kot bi bila potrebna na podlagi člena 26 Splošne uredbe o varstvu podatkov, da bi urejala odgovornosti. Celo v zveznih deželah, ki so po svoji uredbi izbrale model skupnega postopka, ni ustreznega prenosa, ki bi bil skladen z varstvom podatkov. V zvezni deželi Hessen je celo v uredbi določeno, da se elektronski poštni predal vodi izključno na strežnikih „podatkovnega centra“ pravosodja, torej pri Hessische Zentrale für Datenverarbeitung (centrala za obdelavo podatkov zvezne dežele Hessen; v nadaljevanju: HZD). Pri tem HZD ravno ni del pravosodja in je kvečjemu kot posrednik obdelovalec iz člena 28 Splošne uredbe o varstvu podatkov.

17 Znano je le, da naj bi bil dejansko Landesamt für Datensicherheit in Nordrhein-Westfalen (deželni urad za varstvo podatkov v zvezni deželi Severno Porenje – Vestfalija) kot „posrednik“ odgovoren za administracijo in obratovanje centralnega, čezmejnega registrskega strežnika S.A.F.E.. SAFE-ID naj bi bila nespremenljiva in naj bi jo bilo mogoče izdati le enkrat (glej v zvezi s tem SAFE – http://www.egvp.de/Drittprodukte/SAFE_Abbildungsvorschrift _SAFE_ID_Stand_Dez_2014.pdf). Poleg tega so poštni predali v EGVP označeni z enoznačno identifikacijsko številko (tako imenovano Govello-ID). Kolikor je predložitvenemu sodišču znano, naj bi bile te ID številke evidentirane pri evidenčni službi, ki jo upravlja zvezna dežela Severno Porenje - Vestfalija (IT-NRW). Kdo je v Zvezi zveznih dežel dejansko odgovoren za izdajo Govello-ID, s predpisi ni določeno.

18 Ni znano, na kateri pravni podlagi za varstvo podatkov temelji EGVP. Glede poizvedb o dogovoru iz člena 26 Splošne uredbe o varstvu podatkov je tožena stranka odklonila, da bi se o tem izjavila in ga predložila. Zato je tudi vprašljivo, ali se lahko zaradi neobstoja določbe o odgovornosti na podlagi člena 26 Splošne uredbe o varstvu podatkov prek tako imenovanega posebnega uradnega elektronskega poštnega predala izvede zakonito posredovanje. Zlasti tudi glede na podatkovno varnost, saj noben dokument ob prenosu ni šifriran.

19 Po mnenju predložitvenega sodišča ni odločilno, ali je treba v skladu s sedanjim pozitivnim pravom za posebni odvetniški elektronski poštni predal uporabiti šifriranje od konca do konca. Vsaj v zvezni deželi Hessen med posrednikom, HZD, in posameznim sodiščem – torej tudi Verwaltungsgericht Wiesbaden (upravno sodišče v Wiesbadnu, Nemčija) – ni šifriranja sporočil, ki jih je treba posredovati.

20 Vendar pa v obravnavanem primeru to ni pomembno, saj postopek ustreza postopku pošiljanja elektronske pošte. Sodišče je glede storitev elektronske pošte na internetu odločilo, da ne gre za komunikacijsko storitev, saj storitev ne zajema dostopa do interneta, ki ni v celoti ali pretežno sestavljen iz prenosa signalov po elektronskih komunikacijskih omrežjih in torej ni „elektronska komunikacijska storitev“ (sodba z dne 13. junija 2019, C-193/18, ECLI:EU:C:2019:498). Tako pri EGVP ne gre za storitev, za katero bi veljala Direktiva 2002/58/ES (člen 2(4) Splošne uredbe o varstvu podatkov). Zato velja Splošna uredba o varstvu podatkov s posledico, da je treba EGVP in priključene postopke zajeti v evidenco o dejavnostih obdelave in da se je treba dogovoriti o posamezni odgovornosti kot o postopku z več upravljavci na podlagi člena 26 Splošne uredbe o varstvu podatkov. Ne enega ne drugega v tem primeru ni. Zato obstaja dvom v zakonitost posredovanja podatkov.

21 Pri EGVP gre za postopek pravosodnih uprav, ki jih je treba pripisati drugi veji oblasti, izvršilni oblasti, in toženi stranki, ki je prav tako del izvršilne oblasti. Tako mora po prepričanju sodišča tožena stranka skrbeti za to, da je elektronski postopek za posredovanje vlog in spisov skladen s Splošno uredbo o varstvu podatkov.

22 Za predložitveno sodišče se zato v okviru pravosodne dejavnosti postavi vprašanje, kako je treba ravnati s podatki, ki so posredovani prek sistema EGVP-prek tako imenovanega uradnega poštnega predala, če postopek EGVP in s tem povezana obdelava podatkov kot taka nista skladna s Splošno uredbo o varstvu podatkov.

23 Predložitveno sodišče mora v okviru pravosodne dejavnosti upoštevati in spoštovati Splošno uredbo o varstvu podatkov.

24 Sodišče nima nobenega vpliva na zakonitost obdelave podatkov pravosodne uprave, saj je ta zunaj „sodne dejavnosti“ pri drugi veji oblasti, izvršilni oblasti. Predložitveno sodišče pa mora upoštevati in spoštovati evropsko pravo. Če ga udeleženci postopka kršijo, verjetno sodna uporaba podatkov ne bi bila dopustna, saj sodišče sicer sodeluje pri nezakoniti obdelavi podatkov. V obravnavanem primeru je otežujoče še, da tožena stranka glede na dosedanjo korespondenco verjetno (namerno) krši zahteve evropskega prava.

25 Prav tako ne gre za primer, v katerem bi bili z uporabo podatkov s strani sodišča na podlagi člena 17(3)(e) Splošne uredbe o varstvu podatkov upravičeni uveljavljanje, izvajanje ali obramba pravnih zahtevkov tožene stranke. Podatki

sicer toženi stranki služijo za izpolnjevanje pravne obveznosti na podlagi prava Unije ali države članice, ki velja za upravljavca, ali za izvajanje naloge v javnem interesu ali pri izvajanju javne oblasti, ki je bila dodeljena upravljavcu, člen 17(3)(b) Splošne uredbe o varstvu podatkov. S tem pa bi hkrati legalizirali trajno ravnanje v nasprotju z varstvom podatkov.

26 Zato so predložena vprašanja posebnega pomena, ko gre za uporabo Splošne uredbe o varstvu podatkov v sodnih postopkih. Spodkopan bi bil cilj iz člena 1(2) Splošne uredbe o varstvu podatkov, da se varuje temeljne pravice in svoboščine posameznikov ter zlasti njihovo pravico do varstva osebnih podatkov.

27 Zato bi bila vsaj za primer, da bi bil odgovor na prvo vprašanje nikalen, potrebna odločitev posameznika, na katerega se osebni podatki nanašajo ali bolje izrecno soglasje posameznika, na katerega se osebni podatki nanašajo – v obravnavanem primeru tožeče stranke –, da bi se smelo njegove podatke kljub formalno nezakoniti obdelavi uporabiti v sodnem postopku.

28 To pa bi imelo za posledico, da v primeru zavrnitve ne bi bilo dovoljeno obdelati (uporabiti) pred sodiščem podatkov, ki so bili obdelani pri toženi stranki in ki jih ta predloži v obliki tako imenovanega uradnega elektronskega spisa MARIS. To bi imelo dalje za posledico, da do naknadne izpolnitve obveznosti dokumentacije ne bi več obstajala podlaga za odločitev. Prvotno odločbo tožene stranke bi morali vedno odpraviti. Odločitve o uveljavljanem statusu azila ne bi bilo mogoče sprejeti, dokler ne bi bile izpolnjene zahteve glede dokumentacije .