Mål C-60/22

Sammanfattning av begäran om förhandsavgörande enligt artikel 98.1 i rättegångsreglerna för Europeiska unionens domstol

Datum för ingivande:

1 februari 2022

Domstol som begär förhandsavgörande:

Verwaltungsgericht Wiesbaden (Tyskland)

Datum för beslut att begära förhandsavgörande:

27 januari 2022

Sökande:

UZ

Motpart:

Förbundsrepubliken Tyskland

Saken i det nationella målet

Dataskydd – Förordning 2016/679 (allmän dataskyddsförordning) – Artikel 5.2 – Ansvarsskyldighet – Artikel 17.1 d) och artikel 18.1 b) – Laglig behandling av personuppgifter – Utövande av rätten till radering eller begränsning – Användning av de behandlade uppgifterna

Syfte med och rättslig grund för begäran om förhandsavgörande

Tolkning av unionsrätten, artikel 267 i FEUF

Frågor som har hänskjutits för förhandsavgörande

1) Leder en personuppgiftsansvarigs bristfälliga, ofullständiga eller underlåtna uppfyllelse av sin ansvarsskyldighet enligt artikel 5 i Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän

dataskyddsförordning, GDPR), till exempel på grund av ett bristfälligt eller ofullständigt register över behandling enligt artikel 30 i GDPR eller en bristfälligt arrangemang om ett gemensamt förfarande enligt artikel 26 i GDPR, till att behandlingen av personuppgifter är olaglig enligt artikel 17.1 d) och artikel 18.1 b) i GDPR och att den registrerade har en rätt till radering eller begränsning?

2) Om fråga 1 besvaras jakande: innebär en rätt till radering eller begränsning att de behandlade personuppgifterna inte ska beaktas i ett domstolsförfarande? I vart fall om den registrerade motsätter sig användandet av uppgifterna i domstolsförfarandet?

3) Om fråga 1 besvaras nekande: leder en personuppgiftsansvarigs överträdelse av artikel 5, 30 eller 26 i GDPR – med avseende på användningen av behandlade personuppgifter i domstolsförfaranden – till att en nationell domstol endast får beakta personuppgifterna om den registrerade uttryckligen samtycker till användandet?

Anförda unionsbestämmelser

Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning, GDPR) (EUT L 119, 4.5.2016, s. 1), skäl 82, artikel 5, 9, 17, 18, 26, 30, 94.

Europaparlamentets och rådets direktiv 2013/32/EU av den 26 juni 2013 om gemensamma förfaranden för att bevilja och återkalla internationellt skydd (EUT L 180, 29.6.2013, s. 60), skäl 52

Europeiska unionens stadga om de grundläggande rättigheterna, artikel 7 och 8

Anförd nationell lagstiftning

Bundesdatenschutzgesetz (den federala dataskyddslagen, BDSG) (Bundesgesetzblatt del I s. 2097), 43 § tredje stycket

Kortfattad redogörelse för de faktiska omständigheterna och förfarandet i det nationella målet

1 UZ bestrider ett avslagsbeslut meddelat av Bundesamt für Migration und Flüchtlinge (den federala migrations- och flyktingsmyndigheten) i Förbundsrepubliken Tyskland och begär ett positivt beslut om flyktingstatus enligt 3 § Asylgesetz (asyllagen, AsylG). Förbundsrepubliken Tysklands beslut baseras på en elektronisk akt kallad MARIS, som också översänds via ett gemensamt förfarande enligt artikel 26 till domstolens elektroniska domstols- och

administrationsbrevlåda (EGVP). Gällande frågan om den fullständiga översändningen av akten hänvisas till de frågor som redan har hänskjutits till domstolen (mål C 564/21).

2 Det råder tvivel huruvida ett register över behandling enligt artikel 30 i förordning 2016/679 (allmän dataskyddsförordning, GDPR) beträffande den så kallade elektroniska MARIS-akten över huvud taget eller i sin helhet finns tillgängligt hos Förbundsrepubliken Tyskland. Det finns inte heller något arrangemang eller lagstiftning i enlighet med artikel 26 i GDPR beträffande förfarandet för elektronisk översändning av akter och fastställandet av vem som bär ansvaret i ett sådant förfarande. Dessa handlingar begärdes in av den hänskjutande domstolen under förfarandets gång. Förbundsrepubliken Tyskland har dock vägrat att lämna ut handlingarna bland annat med motiveringen att det inte finns något arrangemang i enlighet med artikel 26 beträffande EGVP.

Kortfattad redogörelse för skälen till att förhandsavgörande begärs

3 Frågan som uppstår är hur den hänskjutande domstolen åtminstone vid en (formell) rättsstridighet beträffande Förbundsrepubliken Tysklands behandling av UZ:s personuppgifter ska hantera personuppgifterna eftersom GDPR enligt direktiv 2013/32 är tillämplig på asylförfaranden enligt nationell lagstiftning. Varken asyllagen eller förvaltningsprocesslagen innehåller några uttalanden om detta.

4 Enligt skäl 52 i direktiv 2013/32 ska behandlingen av personuppgifter i asylföranden i medlemsstaterna ske enligt Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter. Direktiv 95/46 upphävdes enligt artikel 94.1 i GDPR från och med den 25 maj 2018. Enligt artikel 94.2 i GDPR ska dock hänvisningar till det upphävda direktivet 95/46 tolkas som hänvisningar till GDPR. GDPR tillämpas således fullt ut för förfaranden om rätt till internationellt skydd.

5 Redan i direktiv 95/46 föreskrevs en dokumentation av behandlingar på automatisk väg, en så kallad anmälan, enligt artikel 18. Enligt artikel 19 i direktiv 95/46 motsvarade innehållet i anmälan i huvudsak den nu gällande artikel 30 i GDPR. Enligt artikel 30 i GDPR gäller den nya standarden alla former av behandling, inklusive register.

6 När direktiv 95/46 ännu var i kraft hade Förbundsrepubliken Tyskland beträffande den elektroniska MARIS-akten endast tillgång till ett mycket outvecklat behandlingsregister för anmälningar enligt direktiv 95/46 (4 § BDSG). Det dåvarande behandlingsregistret (anmälan) innehöll inga särskilda regler för hanteringen av särskilda kategorier av personuppgifter enligt artikel 9 i GDPR (artikel 8 i direktiv 95/46). Särskilda bestämmelser för hantering av personuppgifter enligt artikel 9 och 10 i GDPR existerar än idag inte. Hälso- och religionsrelaterade personuppgifter ingår precis som brottmålsdomar i allmänhet i

den elektroniska MARIS-akten så som ”normala handlingar”. Det framgår inte att det skulle finnas ett särskilt skydd för datasäkerhet, förutom att det troligen finns en åtkomstloggning. Det är dock möjligt att få åtkomst till en asylsökandes akt i svarandens lokalkontor i hela Tyskland samt från centralmyndigheten.

7 Särskilt gällande handläggningen av ärendet och inlämnandet av akten till domstolen hyser den hänskjutande domstolen betydande tvivel huruvida Förbundsrepubliken Tyskland uppfyller kraven som ställs i artikel 5.1 i GDPR, jämförd med till exempel artikel 26 och 30 i GDPR. Trots den hänskjutande domstolens uppmaning har registret över behandling inte lämnats in. Den hänskjutande domstolen har för avsikt att höra myndighetschefen vid det ansvariga organet, alltså Förbundsrepubliken Tyskland, med avseende på dennes ansvarsskyldighet enligt artikel 5.2 i GDPR efter EU-domstolens avgörande.

8 Innan en förhandling måste det dock klargöras om en underlåtenhet att uppfylla skyldigheterna enligt GDPR och den därmed förbundna rättsstridigheten av behandlingen av personuppgifterna kommer att resultera i en sanktion såsom radering enligt artikel 17.1 d) i GDPR eller begränsning av behandlingen enligt artikel 18.1 b) i GDPR. I vart fall om den registrerade – i detta fall UZ – begär det. Annars skulle den hänskjutande domstolen vara tvungen att delta i en olaglig databehandling inom ramen för domstolsförfarandet. Myndigheten skulle ständigt kunna bryta mot GDPR utan sanktioner.

9 I ett sådant fall kan enligt artikel 58 i GDPR endast tillsynsmyndigheten agera. Antagandet av en sanktionsavgift mot den federala migrations- och flyktingsmyndigheten skulle dock inte komma i fråga enligt nationell lagstiftning. Enligt 43 § tredje stycket BDSG, som grundas på artikel 83.7 i GDPR, påförs lokala myndigheter och andra offentliga organ inga sanktionsavgifter. Det finns inget incitament för myndigheten att agera lagligt. Konsekvensen av detta är att varken bestämmelserna i direktiv 2013/32 eller bestämmelserna i GDPR följs.

10 EU-domstolen har redan slagit fast att ”anmälan” (idag: register över behandling) måste vara fullständig vid tidpunkten för behandlingen, dock inte innan dess (målen C 92/09 och C 93/09, dom av den 9 november 2011, ECLI:EU:C:2010:662, punkterna 95 ff.). I det nationella målet har UZ:s personuppgifter behandlats av Förbundsrepubliken Tyskland sedan den tidpunkt då han lämnade in sin asylansökan (den 7 maj 2019). Således borde enligt EU-domstolens praxis ett fullständigt register över behandling angående MARIS-akten (och även för UZ:s asylakt) ha funnits tillgängligt åtminstone vid denna tidpunkt. Så är inte fallet.

11 Vad som gäller i förevarande fall har EU-domstolen varken prövat enligt direktiv 95/46 eller enligt GDPR. Med utgångspunkten att den personuppgiftsansvarige eller personuppgiftsbiträdet bör föra register över behandling som sker under deras ansvar för att påvisa att GDPR följs (skäl 82 GDPR), uppkommer frågan vilka konsekvenser som det ansvariga organets underlåtenhet får, eftersom ansvarsskyldigheten enligt artikel 5 i GDPR inte kan uppfyllas.

12 Artikel 83.5 a) i GDPR föreskriver förvisso att en överträdelse av ansvarsskyldigheten enligt artikel 5 i GDPR kan bestraffas med administrativa sanktionsavgifter upp till 20 000 000 euro. Men som redan har redogjorts för är detta enligt 43 § BDSG inte tillämpligt på federala myndigheter. Däremot regleras det i artikel 17.1 d) i GDPR att olagligt behandlade personuppgifter ska raderas på begäran av den registrerade.

13 Det bristfälliga eller ofullständiga registret över behandling leder åtminstone med ledning av artikel 5 i GDPR till den hänskjutande domstolens övertygelse om att behandlingen av personuppgifterna ”formellt” är olaglig. Därför uppkommer frågan om, i ett sådant fall, en sanktion för en underlåtenhet av skyldigheten enligt artikel 5 i GDPR, jämförd med artikel 30 i GDPR, inte måste medföljа en radering eller åtminstone en blockering av personuppgifterna. I annat fall, i avsaknad av en möjlig sanktion, kan GDPR inte genomföras effektivt.

14 Såvitt känt har till exempel Frankrike med stöd av artikel 18 och följande artiklar i direktiv 95/46 reglerat i nationell rätt att det vid rättsliga förfaranden finns ett strikt lagligt förbud mot användandet av personuppgifter i domstolsförfaranden som inte har rapporterats genom anmälan av den ansvariga myndigheten till tillsynsmyndigheten (CNIL) eftersom användandet av personuppgifterna i brist av dokumentation är olagligt. Det innebär att det förekom åtminstone en sanktion, det vill säga att personuppgifterna inte fick behandlas och användas av domstolen. Även i Portugal och andra medlemsstater borde avsaknaden av ett register över behandling vid tillämpningen av GDPR leda till ett förbud mot användandet. Det är en mekanism som inte finns i Förbundsrepubliken Tyskland, varken inom ramen för genomförandet av direktivet 95/46 eller under den tid som GDPR varit kraft. Snarare lades grundstenen här för att ”tolerera” avsaknaden av anmälan.

15 Även den elektroniska överföringen av akten och UZ:s inlagor utgör en behandling av personuppgifter enligt artikel 4.2 i GDPR, som ska ske med beaktande av principerna för behandling av personuppgifter enligt artikel 5 i GDPR. Här föreligger visst tvivel om den formella lagligheten av behandlingen av personuppgifter genom överföringen av den så kallade elektroniska akten och UZ:s inlagor via respektive överföringskanal. Också här saknas ett register över behandling och en bestämmelse om gemensamt ansvar. Förvisso finns förordningen om de tekniska ramvillkoren för elektronisk juridisk kommunikation och den särskilda elektroniska myndighetsbrevlådan (Elektronischer-Rechtsverkehr-Verordnung – ERVV) av den 24 november 2017 (Bundesgesetzblatt del I s. 3803, ändrad genom artikel 6 i lagen av den 5 oktober 2021, Bundesgesetzblatt del I s. 4607). Förordningen reglerar överföringen av elektroniska dokument till domstolar. De högsta federala myndigheterna i Tyskland eller delstatsregeringarna kan kontrollera identiteten på myndigheter eller offentligrättsliga juridiska personer inom deras område genom att ge dem åtkomst till den särskilda elektroniska myndighetsbrevlådan (så kallad BeBPo). De högsta federala myndigheterna i Tyskland, eller flera delstatsregeringar, kan också gemensamt utse ett offentligrättsligt organ för sina områden. Vem som faktiskt är utsedd har inte reglerats. I slutändandan faller ansvaret antagligen på

den federala och de delstatliga justitieministrarnas arbetsgrupp (kommissionen [BLK] för informationsteknologi i rättsväsendet, arbetsgrupp för IT-standarden i rättsväsendet). Vilken eller vilka myndigheter som är ansvariga för EVGP eller BeBPos registertjänst eller ens för den nödvändiga serverstrukturen är varken känt eller dokumenterat.

16 Det finns inte heller några motsvarande lagstadgade eller andra skriftliga arrangemang mellan domstolar och myndigheter, vilket skulle krävas enligt artikel 26 i GDPR för att reglera ansvaret. Även i delstaterna, som genom förordning har valt modellen med ett gemensamt förfarande, saknas ett motsvarande genomförande i överensstämmelse med dataskyddsnormerna. I Hessen föreskrivs det till och med i förordningen att den elektroniska brevlådan endast får hanteras på servrarna tillhörande rättsväsendets ”datacentral”, alltså på det hessiska centret för behandling av personuppgifter (Hessische Zentrale für Datenverarbeitung, HZD). HZD är inte en del av rättsväsendet och är i bästa fall att anse som ett förmedlande personuppgiftsbiträde enligt artikel 28 i GDPR.

17 Det enda som är känt är att Nordrhein-Westfalens myndighet för datasäkerhet (Landesamt für Datensicherheit) bör vara ansvarig som ”förmedlare” för administrationen och driften av den centrala, delstatsöverskridande registerservern S.A.F.E. Ett SAFE-ID bör vara beständigt och endast tilldelas en gång (se SAFE – http://www.egvp.de/Drittprodukte/SAFE_Abbildungsvorschrift _SAFE_ID_Stand_Dez_2014.pdf). Dessutom identifieras brevlådor i EGVP genom ett unikt identifikationsnummer (så kallat Govello ID). Såvitt känt för den hänskjutande domstolen bör dessa ID:n registreras i en registertjänst som underhålls av Nordrhein-Westfalen (IT NRW). Vem som faktiskt är ansvarig för att utfärda Govello ID är inte reglerat.

18 Det är inte känt på vilken dataskyddsrättslig grund EGVP bygger. Vad gäller frågan om ett arrangemang enligt artikel 26 i GDPR har Förbundsrepubliken Tyskland vägrat att lämna en förklaring eller att presentera ett sådant arrangemang. I detta avseende är det också tveksamt om en laglig överföring kan ske via den så kallade särskilda elektroniska myndighetsbrevlådan på grund av bristande fastställande av ansvar i enlighet med artikel 26 i GDPR. Detta gäller även med avseende på datasäkerheten, eftersom inget av dokumenten krypteras under överföringen.

19 Huruvida det enligt gällande rätt ska användas totalsträckskryptering för den särskilda elektroniska advokatbrevlådan är inte avgörande enligt den hänskjutande domstolen. Åtminstone i Hessen finns det ingen kryptering av de meddelanden som överförs mellan förmedlaren HZD och respektive domstol – i förevarande fall förvaltningsdomstolen i Wiesbaden.

20 Det blir dock inte gällande här eftersom förfarandet motsvarar ett e-postförfarande. När det gäller den internetbaserade Gmail-tjänsten har EU-domstolen slagit fast att den inte är en kommunikationstjänst eftersom tjänsten inte förmedlar någon internetåtkomst som inte helt eller huvudsakligen utgörs av

överföring av signaler i elektroniska kommunikationsnät och därför inte utgör en ”elektronisk kommunikationstjänst” (dom av den 13 juni 2019, C 193/18, ECLI:EU:C:2019:498). Detta innebär att EGVP inte är en tjänst som faller under direktiv 2002/58/EG (artikel 2.4 i GDPR). GDPR gäller därför, vilket innebär att EGVP och de tillhörande förfarandena ska registreras i ett register över behandling och att respektive ansvar måste bestämmas genom ett arrangemang med flera ansvariga enligt artikel 26 i GDPR. Allt detta saknas i förevarande fall. Därför finns det frågetecken kring lagligheten av dataöverföringen.

21 EGVP är ett förfarande för rättsväsendet som hör under den verkställande makten. Förbundsrepubliken Tyskland är också en del av den verkställande makten. Förbundsrepubliken Tyskland måste därför, för att övertyga den hänskjutande domstolen, säkerställa att det elektroniska förfarandet för dataöverföring av inlagor och akter är förenligt med GDPR.

22 Den hänskjutande domstolen ställer sig i samband med sin dömande verksamhet därför frågan hur de uppgifter som tillhandahålls via EGVP-systemet via den så kallade myndighetsbrevlådan ska hanteras, om EGVP-förfarandet och den tillhörande databehandlingen som sådan inte överensstämmer med GDPR.

23 Den hänskjutande domstolen måste iaktta och följa GDPR i samband med sin dömande verksamhet.

24 Det har ingen inverkan på lagligheten av rättsväsendets behandling av personuppgifter eftersom detta ligger utanför den ”rättsliga verksamheten” i den verkställande makten. Den hänskjutande domstolen måste dock iaktta och följa europarätten. Om de som är involverade i förfarandet åsidosätter detta, bör dataanvändningen inte vara tillåten i domstol, eftersom domstolen annars skulle delta i en olaglig behandling av personuppgifter. I det aktuella fallet förvärras det av att Förbundsrepubliken Tyskland med hänsyn till den tidigare korrespondensen sannolikt (medvetet) brutit mot de europarättsliga kraven.

25 Det är inte heller fråga om en situation som skulle motivera en rättslig användning via artikel 17.3 e) i GDPR för att fastställa, göra gällande eller försvara rättsliga anspråk från Förbundsrepubliken Tyskland. Förvisso tjänar Förbundsrepubliken Tysklands personuppgifter till att uppfylla en rättslig förpliktelse som kräver behandling enligt unionsrätten eller enligt en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av eller för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige, artikel 17.3 i GDPR. Samtidigt skulle detta dock permanent legalisera en åtgärd som bryter mot dataskyddslagstiftningen.

26 Frågorna som hänskjuts är därför av särskild betydelse när det gäller tillämpningen av GDPR i domstolsprocesser. Målet enligt artikel i 1.2 GDPR, att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, skulle motverkas.

27 I detta avseende bör det krävas den registrerades – i detta fall UZ:s – godkännande eller ännu hellre vederbörandes uttryckliga samtycke till att dennes personuppgifter får användas i ett domstolsförfarande trots en formellt sett olaglig behandling av personuppgifterna, åtminstone för det fall att fråga 1 besvaras nekande.

28 Detta skulle dock också innebära att om UZ inte ger sitt samtycke till en användning av de personuppgifter som behandlas av Förbundsrepubliken Tyskland och som läggs fram i form av den så kallade elektroniska MARIS-akten, så skulle personuppgifterna inte få behandlas (användas) i domstolen. Det skulle också innebära att det inte skulle finnas något beslutsunderlag förrän dokumentationskraven är uppfyllda. Förbundsrepubliken Tysklands ursprungliga beslut skulle behöva upphävas. Ett avgörande om den påstådda asylstatusen skulle inte vara möjligt förrän dokumentationskraven uppfylls.