

Sag C-60/22

Sammendrag af anmodning om præjudiciel afgørelse i henhold til artikel 98, stk. 1, i Domstolens procesreglement

Dato for indlevering:

1. februar 2022

Forelæggende ret:

Verwaltungsgericht Wiesbaden (Tyskland)

Afgørelse af:

27. januar 2022

Sagsøger:

UZ

Sagsøgt:

Forbundsrepublikken Tyskland

Hovedsagens genstand

Databeskyttelsesret – forordning 2016/679 (generel forordning om databeskyttelse) – artikel 5, stk. 2 – ansvarlighed – artikel 17, stk. 1, litra d), og artikel 18, stk. 1, litra b) – behandlingens lovlighed – ret til sletning eller begrænsning – udnyttelse af de behandlede oplysninger

Genstand og retsgrundlag for anmodningen om præjudiciel afgørelse

Fortolkning af EU-retten, artikel 267 TEUF

Præjudicielle spørgsmål

- 1) Medfører en dataansvarligs manglende eller undladte eller ufuldstændige udvisning af ansvarlighed i henhold til artikel 5 i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF

(generel forordning om databeskyttelse, databeskyttelsesforordningen), f.eks. ved en manglende eller ufuldstændig fortegnelse over behandlingsaktiviteterne i henhold til databeskyttelsesforordningens artikel 30 eller en manglende ordning om en fælles procedure i henhold til databeskyttelsesforordningens artikel 26, at behandlingen af oplysninger er ulovlig som omhandlet i databeskyttelsesforordningens artikel 17, stk. 1, litra d), og artikel 18, stk. 1, litra b), således at den registrerede har ret til at få slettet eller begrænset oplysningerne?

- 2) Såfremt det første spørgsmål besvares bekræftende: Medfører eksistensen af en ret til sletning eller begrænsning, at de behandlede oplysninger ikke skal tages i betragtning under en retssag? Gælder dette i hvert fald i tilfælde, hvor den registrerede rejser indsigelse mod udnyttelse under en retssag?
- 3) Såfremt det første spørgsmål besvares benægtende: Medfører en dataansvarligs overtrædelse af databeskyttelsesforordningens artikel 5, 30 eller 26, at en national ret med hensyn til spørgsmålet om retslig udnyttelse af behandlingen af oplysninger kun må tage oplysningerne i betragtning, såfremt den registrerede udtrykkeligt giver samtykke til udnyttelsen?

Anførte EU-retlige forskrifter

Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT 2016, L 119, s. 1), 82. betragtning, artikel 5, 9, 17, 18, 26, 30 og 94

Europa-Parlamentets og Rådets direktiv 2013/32/EU af 26. juni 2013 om fælles procedurer for tildeling og fratagelse af international beskyttelse (EUT 2013, L 180 s. 60), 52. betragtning

Den Europæiske Unions charter om grundlæggende rettigheder, artikel 7 og 8

Anførte nationale forskrifter

Bundesdatenschutzgesetz BDSG (forbundslov om databeskyttelse) (BGBl. I, s. 2097), § 43, stk. 3

Kort fremstilling af de faktiske omstændigheder og retsforhandlingerne i hovedsagen

- 1 Sagsøgeren har klaget over et afslag fra Bundesamt für Migration und Flüchtlinge (forbundskontoret for migration og flygtninge) og har nedlagt påstand om tildeling af flytningestatus i henhold til § 3 i Asylgesetz (AsylG) (asylloven). Sagsøgtes afgørelse er baseret på de elektroniske sagsakter i den såkaldte Bundesamtakte

MARIS (forbundskontorets sagsakter i det elektroniske dokumentstyringssystem Migrations- Asyl, Reintegrations-. Integrations-System, forkortet MARIS), som ligeledes som led i en fælles procedure i henhold til artikel 26 fremsendes til retten via Elektronisches Gericht- und Verwaltungspostfach (retternes og forvaltningens elektroniske postkassesystem (herefter »EGVP«). For så vidt angår spørgsmålene vedrørende den fuldstændige fremsendelse af sagsakterne henvises til de spørgsmål, der allerede er forelagt Domstolen (sag C-564/21).

- 2 Der hersker tvivl om, hvorvidt der hos sagsøgte overhovedet eller i fuldstændig form foreligger en fortegnelse over behandlingsaktiviteterne som omhandlet i artikel 30 i forordning 2016/679 (generel forordning om databeskyttelse, herefter: »databeskyttelsesforordningen«) for så vidt angår de såkaldte elektroniske MARIS-sagsakter. Der foreligger heller ingen ordning eller lovbestemmelse som omhandlet i databeskyttelsesforordningens artikel 26 for så vidt angår proceduren for elektronisk fremsendelse af sagsakter og fastsættelse af ansvaret i denne procedure. Den forelæggende ret har under retssagen udbedt sig disse dokumenter. Sagsøgte har dog nægtet at fremlægge dokumenterne, bl.a. med den begrundelse, at der for så vidt angår EGVP ikke foreligger nogen ordning i henhold til databeskyttelsesforordningens artikel 26.

Kort fremstilling af begrundelsen for forelæggelsen

- 3 Spørgsmålet er, hvorledes retten, i det mindste i tilfælde af at der foreligger en (formel) ulovlighed i forbindelse med sagsøgtes behandling af sagsøgerens personoplysninger, skal håndtere disse oplysninger, da databeskyttelsesforordningen i henhold til direktiv 2013/32 finder anvendelse på asylsager i henhold til national ret. Hverken asylloven eller Verwaltungsgerichtsordnung (lov om forvaltningsretspleje) indeholder bestemmelser herom.
- 4 I henhold til 52. betragtning til direktiv 2013/32 gælder Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger for medlemsstaternes behandling af personoplysninger i forbindelse med asylsager. I henhold til databeskyttelsesforordningens artikel 94, stk. 1, blev direktiv 95/46 ophævet med virkning fra 25. maj 2018. I henhold til databeskyttelsesforordningens artikel 94, stk. 2, gælder henvisninger til det ophævede direktiv 95/46 som henvisninger til denne forordning. Følgelig finder databeskyttelsesforordningen fuldt ud anvendelse på procedurer for tildeling af international beskyttelse.
- 5 Allerede direktiv 95/46 fastsatte bestemmelser om dokumentation af elektroniske databehandlinger, den såkaldte anmeldelse i henhold til dette direktivs artikel 18. Indholdet af anmeldelsen i henhold til artikel 19 i direktiv 95/46 svarede i det væsentlige til databeskyttelsesforordningens nuværende artikel 30, idet den nye retsregel omfatter alle former for behandling, dvs. også registre.

- 6 Mens direktiv 95/46 var gældende, rådede sagsøgte kun over en meget rudimentær behandlingsfortegnelse som anmeldelse som omhandlet i direktiv 95/46 [databeskyttelseslovens § 4 e)] vedrørende de elektroniske MARIS-sagsakter. Den daværende behandlingsfortegnelse (anmeldelsen) indeholdt ingen særlige bestemmelser om håndteringen af særlige kategorier af personoplysninger i henhold til databeskyttelsesforordningens artikel 9 (artikel 8 i direktiv 95/46). Sådanne særlige bestemmelser om håndteringen af oplysninger i henhold til databeskyttelsesforordningens artikel 9 og 10 ses stadig ikke at foreligge. Helbredsoplysninger og oplysninger om religiøs overbevisning optages nemlig i lighed med straffedomme generelt som såkaldte »normale bilag« i de elektroniske MARIS-sagsakter. Der fremgår ingen særlig beskyttelse af datasikkerheden, bortset fra, at adgang formentlig logges. Der vil dog være adgang til en asylansøgers sag både fra alle sagsøgte landekontorer i hele Tyskland og fra selve centralen.
- 7 Netop hvad angår førelse af sagsmapper og fremlæggelse af sagens bilag for retten nærer den forelæggende ret i væsentligt omfang tvivl om, hvorvidt sagsøgte har overholdt bestemmelserne i databeskyttelsesforordningens artikel 5, stk. 1, sammenholdt med f.eks. databeskyttelsesforordningens artikel 26 og 30. Fortegnelsen over behandlingsaktiviteterne er i strid med rettens påbud ikke blevet fremlagt. Når Domstolens afgørelse foreligger, er det således hensigten at afhøre lederen af den ansvarlige myndighed, altså sagsøgte, vedrørende den pågældendes ansvarlighed i henhold til databeskyttelsesforordningens artikel 5, stk. 2.
- 8 Før en afhøring skal det imidlertid afklares, om undladelsen af at opfylde forpligtelser i henhold til databeskyttelsesforordningen og dermed en ulovlig behandling af oplysninger medfører en sanktion som sletning af oplysninger i henhold til databeskyttelsesforordningens artikel 17, stk. 1, litra d), eller en begrænsning af behandlingen i henhold til databeskyttelsesforordningens artikel 18, stk. 1, litra b). Dette må i det mindste være tilfældet, såfremt den registrerede, i den foreliggende sag sagsøgeren, anmoder herom. I modsat fald ville retten nemlig i forbindelse med retssagen være tvunget til at tage del i en ulovlig behandling af oplysninger. Myndigheden ville kunne overtræde databeskyttelsesforordningen, uden at der på noget tidspunkt pålægges sanktioner.
- 9 I et sådant tilfælde ville kun tilsynsmyndigheden i henhold til databeskyttelsesforordningens artikel 58 kunne gribe ind. I henhold til national ret ville Bundesamt für Migration und Flüchtliche (forbundskontoret for migration og flygtninge) dog ikke kunne idømmes en administrativ bøde. I henhold til databeskyttelseslovens § 43, stk. 3, der er baseret på databeskyttelsesforordningens artikel 83, stk. 7, pålægges der ikke offentlige myndigheder og andre offentlige organer administrative bøder. Der ville ikke være nogen tilskyndelse for myndigheden til ikke at handle ulovligt. Dette ville medføre, at hverken bestemmelserne i direktiv 2013/32 eller databeskyttelsesforordningen selv ville blive overholdt.

- 10 Domstolen har allerede truffet afgørelse om, at »anmeldelsen« (i dag fortegnelsen over behandlingsaktiviteter) skal foreligge fuldstændigt på tidspunktet for behandlingen, men ikke tidligere (sag C-92/09 og C-93/09, dom af 9.11.2011, ECLI:EU:C:2010:662, præmis 95 ff.). I disse sager blev sagsøgerens personoplysninger allerede behandlet af sagsøgte fra det tidspunkt, hvor sagsøgeren havde indgivet sin asylansøgning (den 7.5.2019). Dermed skulle der i det mindste ifølge Domstolens praksis på dette tidspunkt have foreligget en fuldstændig fortegnelse over behandlingsaktiviteterne vedrørende MARIS-sagsakterne (og dermed for sagsøgerens asylsag). Dette er imidlertid ikke tilfældet.
- 11 Hvad der gælder i dette tilfælde, har Domstolen hidtil hverken truffet afgørelse om i henhold til direktiv 95/46 eller i henhold til databeskyttelsesforordningen. Tages der udgangspunkt i, at den dataansvarlige eller databehandleren for at påvise overholdelse af databeskyttelsesforordningen bør føre fortegnelser over behandlingsaktiviteter under sit ansvar (82. betragtning til databeskyttelsesforordningen) opstår spørgsmålet, hvilken konsekvens en undladelse fra det ansvarlige organs side har. I dette tilfælde kan ansvarligheden i henhold til databeskyttelsesforordningens artikel 5 nemlig ikke opfyldes.
- 12 Databeskyttelsesforordningens artikel 83, stk. 5, litra a), bestemmer ganske vist, at en overtrædelse af ansvarligheden i henhold til databeskyttelsesforordningens artikel 5 kan straffes med administrative bøder på op til 20 000 000 EUR. Denne bestemmelse finder dog – som allerede anført – i henhold til databeskyttelseslovens § 43, stk. 3, ikke anvendelse på forbundsmyndigheder. Databeskyttelsesforordningens artikel 17, stk. 1, litra d), bestemmer dog, at ulovligt behandlede oplysninger skal slettes, i det mindste hvis den registrerede anmoder herom.
- 13 Den manglende eller ufuldstændige fortegnelse over behandlingsaktiviteter medfører i det mindste i lyset af databeskyttelsesforordningens artikel 5 efter den forelæggende rets opfattelse, at behandlingen af oplysninger udgør en »formel« ulovlighed. Spørgsmålet er derfor, om ikke oplysningerne i et sådant tilfælde som sanktion for en undladelse i henhold til databeskyttelsesforordningens artikel 5 sammenholdt med databeskyttelsesforordningens artikel 30 skal slettes eller i det mindste gøres utilgængelige. I modsat fald ville databeskyttelsesforordningen nemlig på grund af fraværet af en mulig sanktion ikke kunne håndhæves effektivt.
- 14 I hvert fald havde – så vidt vides – f.eks. den franske republik, da artikel 18 ff. i direktiv 95/46 var i kraft, i national ret bestemt, at der i forbindelse med retssager gælder et strengt lovforbud mod anvendelse af de personlige oplysninger, som ikke var registreret gennem det ansvarlige organs anmeldelse til tilsynsmyndigheden (CNIL), da det var ulovligt at anvende oplysningerne uden dokumentation. Dermed fandtes der i dette tilfælde i det mindste en sanktion som følge af, at oplysningerne ikke måtte behandles og anvendes af retten. I henhold til databeskyttelsesforordningen skal den manglende fortegnelse over behandlingsaktiviteter også i Portugal og i andre medlemsstater medføre et forbud

mod udnyttelse. En mekanisme, som ikke findes i Forbundsrepublikken Tyskland i forbindelse med gennemførelsen af direktiv 95/46 og heller ikke under databeskyttelsesforordningen. Tværtimod blev grundstenen til at »tåle« den manglende anmeldelse lagt her.

- 15 Den elektroniske fremsendelse af sagen og sagsøgte processkrifter udgør ligeledes en behandling af oplysninger som omhandlet i databeskyttelsesforordningens artikel 4, nr. 2), som skal overholde principperne for behandling af oplysninger i henhold til databeskyttelsesforordningens artikel 5. Der hersker derfor også i denne forbindelse tvivl om, hvorvidt behandlingen af oplysninger formelt sker lovligt, når forbundskontorets såkaldte elektroniske sagsakter og sagsøgte processkrifter fremsendes gennem den pågældende distributionskanal. Heller ikke i dette tilfælde foreligger der en fortegnelse over behandlingsaktiviteter og en ordning vedrørende det fælles ansvar. Ganske vist findes bekendtgørelsen Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (bekendtgørelse om de tekniske rammebetingelser for den elektroniske udveksling af retsdokumenter og om myndighedernes særlige elektroniske postkasse) af 24.11.2017 (BGBl. I, s. 3803, som ændret ved artikel 6 i lov af 5.10.2021, BGBl. I, s. 4607). Den regulerer fremsendelsen af elektroniske dokumenter til delstaternes og forbundsstatens domstole. I denne forbindelse kan forbundsstatens eller delstatsregeringernes øverste myndigheder på deres område for så vidt angår offentligretlige organer kontrollere offentlige myndigheders eller offentligretlige juridiske personers identitet med henblik på at give disse adgang til Besonderes Elektronisches Behördenpostfach (myndighedernes særlige elektroniske postkasse) (den såkaldte BeBPo). Forbundsstatens øverste myndigheder eller flere delstatsregeringer kan ligeledes udpege et fælles offentligretligt organ for deres områder. Hvem dette rent faktisk er, er ikke fastlagt. I sidste ende er det vel justitsministeriernes såkaldte Bund-Länder-Arbeitsgruppe (Bund-Länder-Kommission für Informationstechnik in der Justiz [BLK] Arbeitsgruppe IT-Standards in der Justiz) (Forbundsstatens og delstaternes arbejdsgruppe (Forbundsstatens og delstaternes kommission for informationsteknologi i retsvæsenet, Arbejdsgruppen for IT-standarder i retsvæsenet)), der står bag. Det vides ikke og er ikke dokumenteret, hvilken myndighed eller hvilke myndigheder der er ansvarlige for EGVP's eller BeBPo's bibliotekstjeneste endsige for den nødvendige serverstruktur.
- 16 Der findes heller ingen lovbestemmelser herom eller andre skriftlige bestemmelser mellem domstolene og myndighederne, således som det kræves i henhold til databeskyttelsesforordningens artikel 26 med henblik på at fordele ansvaret. Selv i delstater, der i henhold til deres bekendtgørelse har valgt modellen med den fælles procedure, er gennemførelsen ikke sket i overensstemmelse med databeskyttelsesreglerne. I delstaten Hessen bestemmes det endda i bekendtgørelsen, at den elektroniske postkasse udelukkende føres på retsvæsenets »datacentral«, dvs. hos Hessische Zentrale für Datenverarbeitung (HZD) (Delstaten Hessens Center for Behandling af Oplysninger, herefter »HZD«). Men

HZD hører netop ikke under retsvæsenet og er i bedste fald i sin egenskab af mellemmand databehandler i henhold til databeskyttelsesforordningens artikel 28.

- 17 Det vides kun, at Landersamt für Datensicherheit (den regionale myndighed for datasikkerhed) i delstaten Nordrhein-Westfalen faktisk som »mellemmand« skal være ansvarlig for administrationen og driften af den centrale, tværnationale registerserver SA.F.E. Et SAFE-ID skal ikke kunne ændres og skal kun kunne tildeles én gang (jf. i denne forbindelse SAFE – http://www.egvp.de/Drittprodukte/SAFE_Abbildungsvorschrift_SAFE_ID_Stand_Dez_2014.pdf). Desuden navngives postkasser i EGVP-systemet ved hjælp af et entydigt identifikationsnummer (såkaldt Govello-ID). Så vidt den forelæggende ret ved, er disse ID-numre registreret hos en bibliotekstjeneste, som ajourføres af Nordrhein-Westfalen (IT-NRW). Hvem der faktisk er ansvarlig for tildelingen af Govello-ID i forbundsstatdelstatssammenhæng er ikke reguleret.
- 18 Det vides ikke, på hvilket databeskyttelsesretlige grundlag EGVP er baseret. For så vidt angår forespørgslen om en ordning i henhold til databeskyttelsesforordningens artikel 26, har sagsøgte nægtet at udtale sig herom og at fremlægge denne. I denne henseende er det også spørgsmålet, hvorvidt der kan ske lovlig fremsendelse via den såkaldte BeBPo, når ansvaret i henhold til databeskyttelsesforordningens artikel 26 ikke er fastlagt. Dette gælder også i forhold til datasikkerheden, da ingen af dokumenterne er krypteret under fremsendelsen.
- 19 Om der i henhold til gældende positiv ret skal anvendes en end-to-end-kryptering for så vidt angår den særlige elektroniske advokatpostkasse, er efter den forelæggende rets opfattelse ikke afgørende. I det mindste i delstaten Hessen foretages der ingen kryptering af de meddelelser, der fremsendes mellem mellemmanden, HZD, og den pågældende ret – dvs. også Verwaltungsgericht Wiesbaden (forvaltningsdomstolen i Wiesbaden).
- 20 Det er imidlertid ikke afgørende i denne sag, for proceduren svarer til en mailprocedure. Hvad angår den webbaserede G-mailtjeneste har Domstolen truffet afgørelse om, at der ikke er tale om en kommunikationstjeneste, da tjenesten ikke omfatter en adgang til internettet, der ikke udelukkende eller overvejende består i en overføring af signaler via elektroniske kommunikationsnet, og derfor ikke er en »elektronisk kommunikationstjeneste« (dom af 13.6.2019, C-193/18, ECLI:EU:C:2019:498). Det følger heraf, at EGVP ikke er en tjeneste, der er omfattet af direktiv 2002/58/EF (databeskyttelsesforordningens artikel 2, stk. 4). Derfor finder databeskyttelsesforordningen anvendelse med den konsekvens, at EGVP og de dertil knyttede procedurer skal registreres i en fortegnelse over behandlingsaktiviteter, og at det respektive ansvar skal aftales som procedurer med mange dataansvarlige i henhold til databeskyttelsesforordningens artikel 26. Ingen af kravene er opfyldt i den foreliggende sag. Dermed hersker der tvivl om, hvorvidt overførslen af oplysninger er lovlig.

- 21 EGVP er en procedure under domstolenes forvaltningsorganer, der henhører under den anden statsmagt, den udøvende magt, og under sagsøgte, som ligeledes er en del af den udøvende magt. Dermed skal sagsøgte drage omsorg for og godtgøre for retten, at den elektroniske procedure til brug for overførsel af oplysninger og overførsel af processkrifter og sagsakter er i overensstemmelse med databeskyttelsesforordningen.
- 22 For den forelæggende ret er spørgsmålet derfor, når domstolen handler i sin egenskab af domstol, hvorledes de oplysninger, som leveres gennem EGVP-systemet via den såkaldte myndighedspostkasse skal håndteres, såfremt EGVP-proceduren og den dertil knyttede behandling af oplysninger som sådan ikke er i overensstemmelse med databeskyttelsesforordningen.
- 23 Den forelæggende ret er forpligtet til at overholde og følge databeskyttelsesforordningen, når den handler i sin egenskab af domstol.
- 24 Den har ingen indflydelse på lovligheden af den behandling af oplysninger, som domstolens forvaltningsorgans foretager, da denne behandling uden for »domstolens handlen i egenskab af domstol« henhører under den anden magt, den udøvende magt. Den forelæggende ret er imidlertid forpligtet til at overholde og respektere EU-retten. Såfremt procesdeltagere overtræder EU-retten, kan rettens anvendelse af oplysningerne formentlig ikke ske lovligt, da retten i så fald tager del i en ulovlig behandling af oplysninger. I den foreliggende sag er det i denne forbindelse en skærpende omstændighed, at sagsøgte i betragtning af den hidtidige korrespondance vel (bevidst) overtræder EU-retlige bestemmelser.
- 25 Ej heller er der tale om et tilfælde, som kan begrunde, at sagsøgtes anvender oplysningerne under en retssag til i henhold til databeskyttelsesforordningens artikel 17, stk. 3, litra e) at fastlægge, forsvare eller gøre retskrav gældende. Oplysningerne skal ganske vist gøre det muligt for sagsøgte at overholde en retlig forpligtelse, der kræver behandling i henhold til EU-retten eller medlemsstaternes nationale ret, og som den dataansvarlige er underlagt, eller for at udføre en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, databeskyttelsesforordningens artikel 17, stk. 3, litra b). Men dermed ville en handling, som er i strid med databeskyttelseslovgivningen, samtidig være varigt legaliseret.
- 26 Følgelig er de forelagte spørgsmål af særlig betydning, når der er tale om gennemførelsen af databeskyttelsesforordningen under en retssag. Formålet i henhold til databeskyttelsesforordningens artikel 1, stk. 2, som er at fremme fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger, ville blive undergravet.
- 27 I denne henseende ville det i det mindste for det tilfælde, at det første spørgsmål benægtes, formentlig være nødvendigt at indhente den registreredes beslutning eller rettere den registreredes – i denne sag sagsøgerens – udtrykkelige samtykke

til, at dennes oplysninger må anvendes under retssagen på trods af en formelt ulovlig behandling.

- 28 Dette ville imidlertid også medføre, at de oplysninger, som sagsøgte har behandlet, og som denne fremlægger i form af de såkaldte elektroniske MARIS-sagsakter, i tilfælde af et afslag, ikke må behandles (anvendes) af retten. Dette ville endvidere medføre, at der ikke længere foreligger noget beslutningsgrundlag, før kravene til dokumentation efterfølgende er opfyldt. Sagsøgtes oprindelige afgørelse bør altid annulleres. Det ville ikke være muligt at træffe afgørelse om den asyl-status, der gøres gældende, før kravene til dokumentation efterfølgende er opfyldt.

ARBEJDSDOKUMENT