



Rättsfallssamlingen

DOMSTOLENS DOM (stora avdelningen)

den 5 december 2023*

”Begäran om förhandsavgörande – Skydd av personuppgifter – Förordning (EU) 2016/679 – Artikel 4.2 och 4.7 – Begreppen ’behandling’ och ’personuppgiftsansvarig’ – Utveckling av en mobil it-applikation – Artikel 26 – Gemensamt personuppgiftsansvar – Artikel 83 – Påförande av administrativa sanktionsavgifter – Villkor – Krav på att överträdelsen ska ha skett uppsåtligt eller av oaktsamhet – Den personuppgiftsansvariges ansvar för personuppgiftsbehandling som utförs av ett personuppgiftsbiträde”

I mål C-683/21,

angående en begäran om förhandsavgörande enligt artikel 267 FEUF, framställd av Vilniaus apygardos administracinis teismas (Regionala förvaltningsdomstolen i Vilnius, Litauen) genom beslut av den 22 oktober 2021, som inkom till domstolen den 12 november 2021, i målet

Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos

mot

Valstybinė duomenų apsaugos inspekcija,

ytterligare deltagare i rättegången:

UAB ”IT sprendimai sėkmei”,

Lietuvos Respublikos sveikatos apsaugos ministerija,

meddelar

DOMSTOLEN (stora avdelningen)

sammansatt av ordföranden K. Lenaerts, vice-ordföranden L. Bay Larsen, avdelningsordförandena A. Arabadjiev, C. Lycourgos, E. Regan, T. von Danwitz, Z. Csehi och O. Spineanu-Matei samt domarna M. Ilešič, J.-C. Bonichot, L.S. Rossi, A. Kumin, N. Jääskinen (referent), N. Wahl och M. Gavalec,

generaladvokat: N. Emiliou,

justitiesekreterare: handläggaren C. Strömholm,

* Rättegångsspråk: litauiska.

efter det skriftliga förfarandet och förhandlingen den 17 januari 2023,

med beaktande av de yttranden som avgetts av:

- Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos, genom G. Aleksienė,
- Valstybinė duomenų apsaugos inspekcija, genom R. Andrijauskas,
- Litauens regering, genom V. Kazlauskaitė-Švenčionienė, i egenskap av ombud,
- Nederländernas regering, genom C.S. Schillemans, i egenskap av ombud,
- Europeiska unionens råd, genom R. Liudvinavičiūtė och K. Pleśniak, båda i egenskap av ombud,
- Europeiska kommissionen, genom A. Bouchagiar, H. Kranenborg och A. Steiblytė, samtliga i egenskap av ombud,

och efter att den 4 maj 2023 ha hört generaladvokatens förslag till avgörande,

följande

Dom

- 1 Begäran om förhandsavgörande avser tolkningen av artikel 4.2 och 4.7 samt artiklarna 26.1 och 83.1 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 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) (EUT L 119, 2016, s. 1 och rättelser i EUT L 127, 2018, s. 2 och EUT L 74, 2021, s. 35) (nedan kallad dataskyddsförordningen).
- 2 Begäran har framställts i ett mål mellan Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (Nationella folkhälsomyndigheten vid hälsoministeriet, Litauen) (nedan kallad folkhälsomyndigheten) och Valstybinė duomenų apsaugos inspekcija (Nationella dataskyddinspektionen, Litauen) (nedan kallad dataskyddstillsynsmyndigheten). Målet rör ett beslut genom vilket dataskyddstillsynsmyndigheten påförde folkhälsomyndigheten administrativa sanktionsavgifter med stöd av artikel 83 i dataskyddsförordningen för överträdelser av artiklarna 5, 13, 24, 32 och 35 i denna förordning.

Tillämpliga bestämmelser

Unionsrätt

3 I skälen 9, 10, 11, 13, 26, 74, 79, 129 och 148 i dataskyddsförordningen anges följande:

”(9) ... Skillnader i nivån på skyddet av fysiska personers rättigheter och friheter, särskilt rätten till skydd av personuppgifter, vid behandling av personuppgifter i olika medlemsstater kan förhindra det fria flödet av personuppgifter över hela [Europeiska] unionen. Dessa skillnader kan därför utgöra ett hinder för att bedriva ekonomisk verksamhet på unionsnivå, de kan snedvrída konkurrensen och hindra myndigheterna att fullgöra sina skyldigheter enligt unionsrätten. ...

(10) För att säkra en enhetlig och hög skyddsnivå för fysiska personer och för att undanröja hindren för flödena av personuppgifter inom unionen bör nivån på skyddet av fysiska personers rättigheter och friheter vid behandling av personuppgifter vara likvärdig i alla medlemsstater. En konsekvent och enhetlig tillämpning av bestämmelserna om skydd av fysiska personers grundläggande rättigheter och friheter vid behandling av personuppgifter bör säkerställas i hela unionen. ...

(11) Ett effektivt skydd av personuppgifter över hela unionen förutsätter att de registrerades rättigheter förstärks och specificeras och att de personuppgiftsansvarigas och personuppgiftsbiträdenas skyldigheter vid behandling av personuppgifter klargörs, samt att det finns likvärdiga befogenheter för övervakning och att det säkerställs att reglerna för skyddet av personuppgifter efterlevs och att sanktionerna för överträdelser är likvärdiga i medlemsstaterna.

...

(13) För att säkerställa en enhetlig nivå för skyddet av fysiska personer över hela unionen och undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden behövs en förordning som skapar rättslig säkerhet och öppenhet för ekonomiska aktörer, däribland mikroföretag samt små och medelstora företag, och som ger fysiska personer i alla medlemsstater samma rättsligt verkställbara rättigheter och skyldigheter samt ålägger personuppgiftsansvariga och personuppgiftsbiträden ansvar, så att övervakningen av behandling av personuppgifter blir enhetlig, sanktionerna i alla medlemsstater likvärdiga och samarbetet mellan tillsynsmyndigheterna i olika medlemsstater effektivt. ...

...

(26) Principerna för dataskyddet bör gälla all information som rör en identifierad eller identifierbar fysisk person. Personuppgifter som har pseudonymiserats och som skulle kunna tillskrivas en fysisk person genom att kompletterande uppgifter används bör anses som uppgifter om en identifierbar fysisk person. ... Principerna för dataskyddet bör därför inte gälla för anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person, eller för personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar. Denna förordning berör därför inte behandling av sådan anonym information, vilket inbegriper information för statistiska ändamål eller forskningsändamål.

...

- (74) Personuppgiftsansvariga bör åläggas ansvaret för all behandling av personuppgifter som de utför eller som utförs på deras vägnar. Personuppgiftsansvariga bör särskilt vara skyldiga att vidta lämpliga och effektiva åtgärder och kunna visa att behandlingen är förenlig med denna förordning, även vad gäller åtgärdernas effektivitet. Man bör inom dessa åtgärder beakta behandlingens art, omfattning, sammanhang och ändamål samt risken för fysiska personers rättigheter och friheter.

...

- (79) Skyddet av de registrerades rättigheter och friheter samt de personuppgiftsansvarigas och personuppgiftsbiträdenas ansvar kräver ett tydligt fastställande av vem som bär ansvaret enligt denna förordning, bland annat när personuppgiftsansvariga gemensamt fastställer ändamål och medel för en behandling tillsammans med andra personuppgiftsansvariga eller när en behandling utförs på en personuppgiftsansvarigs vägnar.

...

- (129) För att denna förordning ska övervakas och verkställas på ett enhetligt sätt i hela unionen bör tillsynsmyndigheterna i alla medlemsstater ha samma uppgifter och effektiva befogenheter, bland annat undersökningsbefogenheter, korrigerande befogenheter och befogenheter att ålägga sanktioner ... Tillsynsmyndigheternas befogenheter bör utövas opartiskt, rättvist och inom rimlig tid i överensstämmelse med lämpliga rättssäkerhetsgarantier i unionsrätten och i medlemsstaternas nationella rätt. Framför allt bör varje åtgärd vara lämplig, nödvändig och proportionell för att säkerställa efterlevnad av denna förordning, med beaktande av omständigheterna i varje enskilt fall, samt respektera varje persons rätt att bli hörd innan några enskilda åtgärder som påverkar honom eller henne negativt vidtas och vara utformad så att onödiga kostnader och alltför stora olägenheter för de berörda personerna undviks. Undersökningsbefogenheten när det gäller tillträde till lokaler bör utövas i enlighet med särskilda krav i medlemsstaternas nationella processrätt, såsom kravet på att inhämta förhandstillstånd från rättsliga myndigheter. Varje rättsligt bindande åtgärd som vidtas av tillsynsmyndigheten bör vara skriftlig, klar och entydig, innehålla information om vilken tillsynsmyndighet som har utfärdat åtgärden och datum för utfärdandet, vara undertecknad av tillsynsmyndighetens chef eller en av dess ledamöter efter dennes bemyndigande samt innehålla en motivering till åtgärden och en hänvisning till rätten till ett effektivt rättsmedel. Detta bör inte utesluta ytterligare krav enligt medlemsstaternas nationella processrätt. Antagande av ett rättsligt bindande beslut innebär att det kan bli föremål för domstolsprövning i den medlemsstat till vilken den tillsynsmyndighet som antog beslutet hör.

...

- (148) För att stärka verkställigheten av denna förordning bör det utdömas sanktioner, inbegripet administrativa sanktionsavgifter, för överträdelser av denna förordning utöver eller i stället för de lämpliga åtgärder som tillsynsmyndigheten vidtar i enlighet med denna förordning. Vid en mindre överträdelse eller om den sanktionsavgift som sannolikt skulle utdömas skulle innebära en oproportionell börda för en fysisk person får en reprimand utfärdas i stället för sanktionsavgifter. Vederbörlig hänsyn bör dock tas till överträdelsens karaktär, svårighetsgrad och varaktighet och huruvida den har skett uppsåtligen, vilka

åtgärder som vidtagits för att lindra skadan, graden av ansvar eller eventuella tidigare överträdelser av relevans, det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, efterlevnad av åtgärder som förordnats mot den personuppgiftsansvarige eller personuppgiftsbiträdet, tillämpning av en uppförandekod och eventuella andra försvårande eller förmildrande faktorer. Påförandet av sanktioner, inbegripet administrativa sanktionsavgifter, bör omfattas av lämpliga rättssäkerhetsgarantier i överensstämmelse med de allmänna principerna inom unionsrätten och Europeiska unionens stadga om de grundläggande rättigheterna, vilket inbegriper ett effektivt rättsligt skydd och korrekt rättsligt förfarande.”

4 I artikel 4 i dataskyddsförordningen föreskrivs följande:

”I denna förordning avses med

1. *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,

2. *behandling*: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,

...

5. *pseudonymisering*: behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person,

...

7. *personuppgiftsansvarig*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt,

8. *personuppgiftsbiträde*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

...”

- 5 Artikel 26 i dataskyddsförordningen har rubriken ”Gemensamt personuppgiftsansvariga”, och där föreskrivs följande i punkt 1:

”Om två eller fler personuppgiftsansvariga gemensamt fastställer ändamålen med och medlen för behandlingen ska de vara gemensamt personuppgiftsansvariga. Gemensamt personuppgiftsansvariga ska under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt denna förordning, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artiklarna 13 och 14, genom ett inbördes arrangemang, såvida inte de personuppgiftsansvarigas respektive skyldigheter fastställs genom unionsrätten eller en medlemsstats nationella rätt som de personuppgiftsansvariga omfattas av. Inom ramen för arrangemanget får en gemensam kontaktpunkt för de registrerade utses.”

- 6 Artikel 28 i dataskyddsförordningen har rubriken ”Personuppgiftsbiträden”, och där föreskrivs följande i punkt 10:

”Om ett personuppgiftsbiträde överträder denna förordning genom att fastställa ändamålen med och medlen för behandlingen, ska personuppgiftsbiträdet anses vara personuppgiftsansvarig med avseende på den behandlingen, utan att det påverkar tillämpningen av artiklarna 82, 83 och 84.”

- 7 Artikel 58 i dataskyddsförordningen har rubriken ”Befogenheter”, och där föreskrivs följande i punkt 2:

”Varje tillsynsmyndighet ska ha samtliga följande korrigerande befogenheter

a) Utfärda varningar till en personuppgiftsansvarig eller personuppgiftsbiträdet om att planerade behandlingar sannolikt kommer att bryta mot bestämmelserna i denna förordning.

b) Utfärda reprimander till en personuppgiftsansvarig eller personuppgiftsbiträdet om behandling bryter mot bestämmelserna i denna förordning.

...

d) Förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att se till att behandlingen sker i enlighet med bestämmelserna i denna förordning och om så krävs på ett specifikt sätt och inom en specifik period.

...

f) Införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, behandling.

...

i) Påföra administrativa sanktionsavgifter i enlighet med artikel 83 utöver eller i stället för de åtgärder som avses i detta stycke, beroende på omständigheterna i varje enskilt fall.

...”

8 Artikel 83 i dataskyddsförordningen har rubriken "Allmänna villkor för påförande av administrativa sanktionsavgifter", och där föreskrivs följande:

"1. Varje tillsynsmyndighet ska säkerställa att påförande av administrativa sanktionsavgifter i enlighet med denna artikel för sådana överträdelser av denna förordning som avses i punkterna 4, 5 och 6 i varje enskilt fall är effektivt, proportionellt och avskräckande.

2. Administrativa sanktionsavgifter ska, beroende på omständigheterna i det enskilda fallet, påföras utöver eller i stället för de åtgärder som avses i artikel 58.2 a–h och j. Vid beslut om huruvida administrativa sanktionsavgifter ska påföras och om beloppet för de administrativa sanktionsavgifterna i varje enskilt fall ska vederbörlig hänsyn tas till följande:

- a) Överträdelsens karaktär, svårighetsgrad och varaktighet med beaktande av den aktuella uppgiftsbehandlings karaktär, omfattning eller syfte samt antalet berörda registrerade och den skada som de har lidit.
- b) Om överträdelsen skett med uppsåt eller genom oaktsamhet.
- c) De åtgärder som den personuppgiftsansvarige eller personuppgiftsbiträdet har vidtagit för att lindra den skada som de registrerade har lidit.
- d) Graden av ansvar hos den personuppgiftsansvarige eller personuppgiftsbiträdet med beaktande av de tekniska och organisatoriska åtgärder som genomförts av dem i enlighet med artiklarna 25 och 32.
- e) Eventuella relevanta tidigare överträdelser som den personuppgiftsansvarige eller personuppgiftsbiträdet gjort sig skyldig till.
- f) Graden av samarbete med tillsynsmyndigheten för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter.
- g) De kategorier av personuppgifter som påverkas av överträdelsen.
- h) Det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, särskilt huruvida och i vilken omfattning den personuppgiftsansvarige eller personuppgiftsbiträdet anmälde överträdelsen.
- i) När åtgärder enligt artikel 58.2 tidigare har förordnats mot den berörda personuppgiftsansvarige eller personuppgiftsbiträdet vad gäller samma sakfråga, efterlevnad av dessa åtgärder.
- j) Tillämpandet av godkända uppförandekoder i enlighet med artikel 40 eller godkända certifieringsmekanismer i enlighet med artikel 42.
- k) Eventuell annan försvårande eller förmildrande faktor som är tillämplig på omständigheterna i fallet, såsom ekonomisk vinst som görs eller förlust som undviks, direkt eller indirekt, genom överträdelsen.

3. Om en personuppgiftsansvarig eller ett personuppgiftsbiträde, med avseende på en och samma eller sammankopplade uppgiftsbehandlingar, uppsåtligen eller av oaktsamhet överträder flera av

bestämmelserna i denna förordning får den administrativa sanktionsavgiftens totala belopp inte överstiga det belopp som fastställs för den allvarligaste överträdelsen.

4. Vid överträdelser av följande bestämmelser ska det i enlighet med punkt 2 påföras administrativa sanktionsavgifter på upp till 10 000 000 [euro] eller, om det gäller ett företag, på upp till 2 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

a) Personuppgiftsansvarigas och personuppgiftsbiträdens skyldigheter enligt artiklarna 8, 11, 25–39, 42 och 43.

...

5. Vid överträdelser av följande bestämmelser ska det i enlighet med punkt 2 påföras administrativa sanktionsavgifter på upp till 20 000 000 [euro] eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

a) De grundläggande principerna för behandling, inklusive villkoren för samtycke, enligt artiklarna 5, 6, 7 och 9.

b) Registrerades rättigheter enligt artiklarna 12–22.

...

d) Alla skyldigheter som följer av medlemsstaternas lagstiftning som antagits på grundval av kapitel IX.

...

6. Vid underlåtenhet att rätta sig efter ett föreläggande från tillsynsmyndigheten i enlighet med artikel 58.2 ska det i enlighet med punkt 2 i den här artikeln påföras administrativa sanktionsavgifter på upp till 20 000 000 [euro] eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

7. Utan att det påverkar tillsynsmyndigheternas korrigerande befogenheter enligt artikel 58.2 får varje medlemsstat fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och organ som är inrättade i medlemsstaten.

8. Tillsynsmyndighetens utövande av sina befogenheter enligt denna artikel ska omfattas av lämpliga rättssäkerhetsgarantier i enlighet med unionsrätten och medlemsstaternas nationella rätt, inbegripet effektiva rättsmedel och rättssäkerhet.

...”

- 9 Artikel 84 i dataskyddsförordningen har rubriken ”Sanktioner”, och där föreskrivs följande i punkt 1:

”Medlemsstaterna ska fastställa regler om andra sanktioner för överträdelser av denna förordning, särskilt för överträdelser som inte är föremål för administrativa sanktionsavgifter enligt artikel 83, och vidta alla nödvändiga åtgärder för att säkerställa att de genomförs. Dessa sanktioner ska vara effektiva, proportionella och avskräckande.”

Litauisk rätt

- 10 I artikel 29.3 i *Viešųjų pirkimų įstatymas* (lagen om offentlig upphandling) anges vissa omständigheter under vilka en upphandlande myndighet antingen har rätt eller skyldighet att dra tillbaka en upphandling eller projekttävling som den inlett, vilket kan ske när som helst innan kontraktet (eller föravtalet) har ingåtts eller vinnaren i projekttävlingen har utsetts.
- 11 I artikel 72.2 i lagen om offentlig upphandling anges vilka förhandlingssteg som den upphandlande myndigheten ska gå igenom i ett förhandlat förfarande utan föregående annonsering.

Målet vid den nationella domstolen och tolkningsfrågorna

- 12 I samband med covid-19-pandemin gav Lietuvos Respublikos sveikatos apsaugos ministras (Republiken Litauens hälsominister), genom ett första beslut av den 24 mars 2020, direktören för folkhälsomyndigheten i uppdrag att omedelbart vidta åtgärder för att införskaffa ett datasystem för registrering och uppföljning – för epidemiologiska ändamål – av uppgifter om personer som exponerats för det virus som orsakar covid-19.
- 13 Genom e-postmeddelande den 27 mars 2020 kontaktades bolaget UAB ”IT sprendimai sėkmei” (nedan kallat bolaget ITSS) av en person som uppgav sig företräda folkhälsomyndigheten. Denna person (nedan kallad A.S.) underrättade bolaget om att myndigheten hade beslutat att ge det i uppdrag att utveckla en mobil applikation som skulle uppfylla nyss nämnda ändamål (nedan kallad den aktuella mobilappen eller appen). A.S. skickade därefter e-postmeddelanden till bolaget ITSS, med folkhälsomyndighetens direktör som mottagare i kopia, om olika aspekter rörande utvecklingen av mobilappen.
- 14 Under förhandlingarna mellan bolaget ITSS och folkhälsomyndigheten, skickade inte bara A.S., utan även andra anställda vid folkhälsomyndigheten e-postmeddelanden till bolaget angående formuleringen av de frågor som skulle ställas till användarna i den aktuella mobilappen.
- 15 Vid utvecklingen av appen utarbetades en policy för skydd av personuppgifter, där bolaget ITSS och folkhälsomyndigheten utsågs som personuppgiftsansvariga.
- 16 Den aktuella mobilappen, i vilken bolaget ITSS och folkhälsomyndigheten nämndes, fanns tillgänglig för nedladdning i onlinebutiken Google Play Store från och med den 4 april 2020 och i onlinebutiken Apple App Store från och med den 6 april 2020. Appen var i drift till och med den 26 maj 2020.

- 17 Mellan den 4 april 2020 och den 26 maj 2020 använde sig 3 802 personer av appen. Under denna tid lämnade användarna de uppgifter om sig själva som begärdes av appen, såsom identitetsnummer, geografiska koordinater (latitud och longitud), land, stad, kommun, postnummer, gatunamn, fastighetsnummer, efternamn, förnamn, personlig kod, telefonnummer och adress.
- 18 Genom ett andra beslut av den 10 april 2020 beslutade Republiken Litauens hälsominister att ge folkhälsomyndighetens direktör i uppgift att vidta åtgärder för att förvärva den aktuella mobilappen från bolaget ITSS och det fanns planer på att göra detta med stöd av artikel 72.2 i lagen om offentlig upphandling. Detta bolag tilldelades dock aldrig något upphandlingskontrakt där det framgick att folkhälsomyndigheten officiellt förvärvade appen.
- 19 Folkhälsomyndigheten kontaktade nämligen bolaget den 15 maj 2020 och bad det att inte på något sätt nämna myndigheten i den aktuella mobilappen. Genom skrivelse av den 4 juni 2020 underrättade folkhälsomyndigheten dessutom bolaget om att det saknades medel för att finansiera förvärvet av appen och att myndigheten därför, med stöd av artikel 29.3 i lagen om offentlig upphandling, hade beslutat att avsluta det förfarande som inletts i syfte att genomföra förvärvet.
- 20 Den 18 maj 2020 inledde dataskyddstillsynsmyndigheten en utredning om behandling av personuppgifter. Utredningen visade att personuppgifter hade samlats in med hjälp av den aktuella mobilappen. Av utredningen framgick vidare att vissa användare hade valt att använda den aktuella mobilappen för tillsynsändamål under den obligatoriska självisolering som infördes till följd av covid-19-pandemin och att dessa användare hade besvarat frågor som innebar behandling av personuppgifter. Enligt utredningen lämnade användarna nämligen personuppgifter när de svarade på frågor som ställdes i appen. Dessa uppgifter avsåg bland annat den berörda personens hälsotillstånd och hans eller hennes efterlevnad av reglerna för självisolering.
- 21 Genom beslut av den 24 februari 2021 påförde dataskyddstillsynsmyndigheten folkhälsomyndigheten administrativa sanktionsavgifter på 12 000 euro med stöd av artikel 83 i dataskyddsförordningen. Som skäl för beslutet angavs att folkhälsomyndigheten hade åsidosatt artiklarna 5, 13, 24, 32 och 35 i denna förordning. Genom samma beslut påfördes även bolaget ITSS, i egenskap av gemensam personuppgiftsansvarig, administrativa sanktionsavgifter på 3 000 euro.
- 22 Folkhälsomyndigheten överklagade detta beslut till den hänskjutande domstolen, Vilniaus apygardos administracinis teismas (Regionala förvaltningsdomstolen i Vilnius, Litauen), och gjorde gällande att bolaget ITSS ensamt skulle anses vara personuppgiftsansvarig, i den mening som avses i artikel 4.7 i dataskyddsförordningen. Bolaget ITSS gjorde för sin del gällande att det hade agerat i egenskap av personuppgiftsbiträde, i den mening som avses i artikel 4.8 i dataskyddsförordningen, på uppdrag av folkhälsomyndigheten. Enligt bolaget var folkhälsomyndigheten ensam personuppgiftsansvarig.
- 23 Den hänskjutande domstolen har anfört att bolaget ITSS skapade den aktuella mobilappen och att folkhälsomyndigheten lämnade råd till bolaget om innehållet i de frågor som skulle ställas till användarna i appen. Det föreligger dock inte något upphandlingskontrakt mellan folkhälsomyndigheten och bolaget ITSS. Folkhälsomyndigheten har dessutom varken samtyckt eller lämnat tillstånd till att den aktuella mobilappen skulle göras tillgänglig för nedladdning via olika onlinebutiker.

- 24 Den hänskjutande domstolen har vidare angett att syftet med att skapa den aktuella mobilappen var att genomföra det mål som folkhälsomyndigheten hade satt upp, nämligen att hantera covid-19-pandemin genom att skapa ett it-verktyg, och att det var förutsett att personuppgifter skulle behandlas för detta ändamål. Vad gäller bolaget ITSS roll har det enligt den hänskjutande domstolen aldrig varit tal om att bolaget skulle haft några andra syften än att få betalt för den it-produkt det hade tagit fram.
- 25 Den hänskjutande domstolen har även påpekat att det under dataskyddstillsynsmyndighetens utredning fastställdes att det litauiska bolaget Juvare Lithuania, som hanterade it-systemet för tillsynsändamål och kontroll av smittsamma sjukdomar som riskerar att sprida sig, skulle erhålla kopior av de personuppgifter som samlats in via den aktuella mobilappen. Enligt den hänskjutande domstolen användes dessutom fingerade uppgifter för att testa appen. De enda uppgifter som var verkliga var telefonnumren till bolagets anställda.
- 26 Det är mot denna bakgrund som Vilniaus apygardos administracinis teismas (Regionala förvaltningsdomstolen i Vilnius) har beslutat att vilandeförklara målet och att ställa följande tolkningsfrågor till EU-domstolen:
- ”1. Kan begreppet ’personuppgiftsansvarig’ i artikel 4.7 i dataskyddsförordningen tolkas på så sätt att den som planerar att genom offentlig upphandling anskaffa ett verktyg för insamling av uppgifter (en mobil it-applikation) även ska anses vara personuppgiftsansvarig, oberoende av att något upphandlingskontrakt inte har ingåtts och att den framtagna it-produkten (mobilapplikationen), för vars anskaffning ett upphandlingsförfarande användes, inte har levererats?
 2. Kan begreppet ’personuppgiftsansvarig’ i artikel 4.7 i dataskyddsförordningen tolkas på så sätt att en upphandlande myndighet, som inte har förvärvat äganderätten till den framtagna it-applikationen och inte har tagit den i besittning, även ska anses vara personuppgiftsansvarig när den slutliga versionen av applikationen innehåller hänvisningar eller länkar till denna myndighet och/eller när myndigheten anges som personuppgiftsansvarig i den i applikationen angivna policyn för skydd av personuppgifter, vilken inte har godkänts eller erkänts officiellt av den aktuella myndigheten?
 3. Ska begreppet ’personuppgiftsansvarig’ i artikel 4.7 i dataskyddsförordningen tolkas på så sätt att även den som inte har utfört någon faktisk behandling av personuppgifter, i den mening som avses i artikel 4.2 i dataskyddsförordningen, och/eller som inte har lämnat något tydligt tillstånd eller samtycke till sådan behandling, ska anses vara personuppgiftsansvarig? Är det av betydelse för tolkningen av begreppet ’personuppgiftsansvarig’ att den it-produkt med hjälp av vilken behandlingen av personuppgifter har skett har tagits fram i enlighet med det av den upphandlande myndigheten formulerade uppdraget?
 4. Om det är relevant för tolkningen av begreppet ’personuppgiftsansvarig’ att fastställa vilken faktisk behandling av personuppgifter som har skett, ska då artikel 4.2 i dataskyddsförordningen (’behandling av personuppgifter’) tolkas på så sätt att den även omfattar fall där kopior av personuppgifter har använts för att testa it-systemen under förfarandet för anskaffning av mobilapplikationen?

5. Kan gemensamt personuppgiftsansvar enligt artiklarna 4.7 och 26.1 i dataskyddsförordningen enbart tolkas på så sätt att det innefattar frivilligt samordnade åtgärder för att bestämma ändamål och medel för behandlingen av personuppgifter, eller kan detta begrepp även tolkas på så sätt att gemensamt personuppgiftsansvar även omfattar fall där det inte finns något tydligt 'arrangemang' som avser ändamål och medel för behandlingen av personuppgifter och/eller åtgärderna inte har samordnats mellan de berörda organen? Är en omständighet som hänför sig till utvecklingsstadiet för ett medel för behandling av personuppgifter (en it-applikation), under vilket personuppgifter har behandlats, och till syftet med att utveckla en sådan applikation av rättslig betydelse för tolkningen av begreppet gemensamt personuppgiftsansvar? Kan ett 'inbördes arrangemang' mellan gemensamt personuppgiftsansvariga enbart förstås som ett tydligt och definierat fastställande av villkoren för det gemensamma personuppgiftsansvaret?
6. Ska bestämmelsen i artikel 83.1 i dataskyddsförordningen om att 'administrativa sanktionsavgifter ska vara effektiva, proportionella och avskräckande' tolkas på så sätt att den även omfattar fall som aktualiserar ansvarsutkrävande av 'den personuppgiftsansvarige' när utvecklaren i samband med framtagandet av en it-produkt även utför åtgärder som innebär behandling av personuppgifter, och medför otillbörliga åtgärder innebärande personuppgiftsbehandling som vidtas av personuppgiftsbiträdet alltid automatiskt ett rättsligt ansvar för den personuppgiftsansvarige? Ska denna bestämmelse tolkas på så sätt att den även innefattar ett strikt ansvar för den personuppgiftsansvarige?"

Prövning av tolkningsfrågorna

Den första, den andra och den tredje frågan

- 27 Den hänskjutande domstolen har ställt den första, den andra och den tredje frågan, vilka ska prövas tillsammans, för att få klarhet i huruvida artikel 4.7 i dataskyddsförordningen ska tolkas på så sätt att ett organ som har gett ett företag i uppdrag att utveckla en mobil it-applikation kan anses vara personuppgiftsansvarig, i den mening som avses i denna bestämmelse, även i ett fall där detta organ inte självt har utfört behandlingar av personuppgifter och inte uttryckligen har gett sitt samtycke till att konkreta åtgärder som innebär behandling av personuppgifter utförs eller till att mobilapplikationen görs tillgänglig för allmänheten och inte heller har förvärvat applikationen.
- 28 EU-domstolen gör i denna del följande bedömning. I artikel 4.7 i dataskyddsförordningen ges en vid definition av begreppet "personuppgiftsansvarig". Med begreppet avses fysiska eller juridiska personer, offentliga myndigheter, institutioner eller andra organ som ensamma eller tillsammans med andra "bestämmer ändamålen och medlen för behandlingen" av personuppgifter.
- 29 Syftet med denna vida definition är att i överensstämmelse med dataskyddsförordningens syfte säkerställa ett effektivt skydd för fysiska personers grundläggande fri- och rättigheter och, i synnerhet, en hög skyddsnivå för envars rätt till skydd av de personuppgifter som rör honom eller henne (se, för ett liknande resonemang, dom av den 29 juli 2019, Fashion ID, C-40/17, EU:C:2019:629, punkt 66, och dom av den 28 april 2022, Meta Platforms Ireland, C-319/20, EU:C:2022:322, punkt 73 och där angiven rättspraxis).
- 30 Domstolen har redan slagit fast att en fysisk eller juridisk person som för egna syften utövar inflytande över behandlingen av personuppgifter, och därigenom deltar i bestämmandet av ändamål och medel för behandlingen, kan anses vara personuppgiftsansvarig vid behandling av

de aktuella personuppgifterna. I detta avseende krävs det inte att ändamålen och medlen för behandlingen bestäms genom skriftliga riktlinjer eller instruktioner från den personuppgiftsansvarige (se, för ett liknande resonemang, dom av den 10 juli 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, punkterna 67 och 68) och inte heller att den personuppgiftsansvarige är formellt utsedd till sådan.

- 31 För att fastställa om ett organ, såsom folkhälsomyndigheten, kan anses vara personuppgiftsansvarig, i den mening som avses i artikel 4.7 i dataskyddsförordningen, måste således en prövning göras av om detta organ, för egna syften, faktiskt har utövat inflytande över bestämmandet av ändamålen och medlen för behandlingen av de aktuella personuppgifterna.
- 32 Vad beträffar det nu aktuella fallet kan följande konstateras. Med förbehåll för de kontroller som det ankommer på den hänskjutande domstolen att göra, framgår det av handlingarna i målet att den aktuella mobilappen skapades på begäran av folkhälsomyndigheten och att detta syftade till att genomföra det mål som folkhälsomyndigheten hade satt upp, nämligen att hantera covid-19-pandemin genom att skapa ett it-verktyg för registrering och uppföljning av uppgifter om personer som exponerats för det virus som orsakar covid-19. Folkhälsomyndigheten hade förutsett att appanvändarnas personuppgifter skulle behandlas för detta ändamål. Av beslutet om hänskjutande framgår vidare att parametrarna för appen, som till exempel vilka frågor som skulle ställas till användarna och hur de skulle formuleras, anpassades till folkhälsomyndighetens behov och att myndigheten spelade en aktiv roll vid fastställandet av nämnda parametrar.
- 33 Vid sådana förhållanden får folkhälsomyndigheten i princip anses ha deltagit rent faktiskt i bestämmandet av ändamålen och medlen för personuppgiftsbehandlingen.
- 34 Däremot finner EU-domstolen att det i sig endast skulle kunna anses vara relevant att folkhälsomyndigheten angavs som personuppgiftsansvarig i den policy för skydd av personuppgifter som upprättades för den aktuella mobilappen och att det fanns länkar till myndigheten i appen om det visades att myndigheten, uttryckligen eller underförstått, samtyckt till att denna uppgift angavs i policyn eller till att appen innehöll dessa länkar.
- 35 Vad vidare gäller det som den hänskjutande domstolen har anfört som skäl till att den ställt de tre första tolkningsfrågorna – det vill säga att folkhälsomyndigheten inte själv behandlade personuppgifter, att det inte förelåg något kontrakt mellan myndigheten och bolaget ITSS, att myndigheten aldrig förvärvade den aktuella mobilappen eller att den inte lämnat sitt samtycke till att appen gjordes tillgänglig för nedladdning via olika onlinebutiker – finner EU-domstolen att dessa omständigheter inte utesluter att folkhälsomyndigheten kan anses vara ”personuppgiftsansvarig”, i den mening som avses i artikel 4.7 i dataskyddsförordningen.
- 36 Det framgår nämligen av artikel 4.7 jämförd med skäl 74 i dataskyddsförordningen att ett organ som uppfyller villkoret i nämnda artikel 4.7 ska anses vara personuppgiftsansvarig inte bara vid all behandling av personuppgifter som organet självt utför, utan även vid sådan behandling som utförs för dess räkning.
- 37 Här måste dock påpekas att folkhälsomyndigheten inte anses vara personuppgiftsansvarig vid den behandling av personuppgifter som skett till följd av att den aktuella mobilappen gjordes tillgänglig för allmänheten, om myndigheten uttryckligen hade motsatt sig ett sådant tillgängliggörande innan detta skedde. Det ankommer på den hänskjutande domstolen att

kontrollera om så var fallet. Om det är så att folkhälsomyndigheten uttryckligen motsatt sig detta, kan det nämligen inte anses att den aktuella behandlingen av personuppgifter utfördes för myndighetens räkning.

- 38 Mot bakgrund av det ovan anförda ska den första, den andra och den tredje frågan besvaras enligt följande. Artikel 4.7 i dataskyddsförordningen ska tolkas på så sätt att ett organ som har gett ett företag i uppdrag att utveckla en mobil it-applikation, och som i samband med detta har deltagit i bestämmandet av ändamål och medel för den behandling av personuppgifter som utförs via denna applikation, kan anses vara personuppgiftsansvarig i den mening som avses i denna bestämmelse, även i ett fall där detta organ inte självt har utfört behandlingar av personuppgifter och inte uttryckligen har gett sitt samtycke till att konkreta åtgärder som innebär behandling av personuppgifter utförs eller till att mobilapplikationen görs tillgänglig för allmänheten och inte heller har förvärvat applikationen. Detta gäller dock inte om nämnda organ innan applikationen gjordes tillgänglig för allmänheten uttryckligen motsatte sig tillgängliggörandet och den behandling av personuppgifter som skett till följd av detta.

Den femte frågan

- 39 Den hänskjutande domstolen har ställt den femte frågan, som ska prövas härnäst, för att få klarhet i huruvida artiklarna 4.7 och 26.1 i dataskyddsförordningen ska tolkas på så sätt att det är en förutsättning för att två organ ska kunna anses vara gemensamt personuppgiftsansvariga att det finns ett inbördes arrangemang mellan dessa organ som avser bestämmande av ändamål och medel för behandlingen av de aktuella personuppgifterna eller att det finns ett inbördes arrangemang som fastställer villkoren för det gemensamma personuppgiftsansvaret.
- 40 EU-domstolen gör i denna del följande bedömning. Enligt artikel 26.1 i dataskyddsförordningen ska det anses vara fråga om "gemensamt personuppgiftsansvariga" om två eller fler personuppgiftsansvariga gemensamt bestämmer ändamål och medel för behandlingen.
- 41 Detta innebär, såsom framgår av domstolens praxis, att för att en fysisk eller juridisk person ska kunna betraktas som gemensamt personuppgiftsansvarig måste denna person självständigt uppfylla villkoren i definitionen av begreppet "personuppgiftsansvarig" i artikel 4.7 i dataskyddsförordningen (se, för ett liknande resonemang, dom av den 29 juli 2019, Fashion ID, C-40/17, EU:C:2019:629, punkt 74).
- 42 Den omständigheten att det finns ett gemensamt ansvar behöver dock inte nödvändigtvis innebära att de olika aktörer som medverkar vid en behandling av personuppgifter har ett likvärdigt ansvar. Tvärtom kan dessa aktörer vara involverade i olika skeden av behandlingen och i olika utsträckning, så att graden av ansvar för var och en av dem ska bedömas med beaktande av alla relevanta omständigheter i det enskilda fallet (dom av den 5 juni 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, punkt 43). För att flera aktörer ska anses ha ett gemensamt ansvar för en och samma behandling krävs inte heller att var och en av dem har tillgång till de aktuella personuppgifterna (dom av den 10 juli 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, punkt 69 och där angiven rättspraxis).
- 43 Såsom generaladvokaten har påpekat i punkt 38 i sitt förslag till avgörande kan ett deltagande i att bestämma ändamål och medel för en behandling av personuppgifter ta sig olika former, eftersom deltagandet kan följa såväl av ett gemensamt beslut fattat av två eller flera organ som av sådana

organs samstämmiga beslut. I det sistnämnda fallet krävs dock att besluten kompletterar varandra, så att vart och ett av dem har en påtaglig inverkan på bestämmandet av ändamålen och medlen för behandlingen.

- 44 Däremot kan det inte krävas att det föreligger ett inbördes arrangemang i form av en formell överenskommelse mellan de personuppgiftsansvariga om ändamål och medel för behandlingen.
- 45 Av artikel 26.1 i dataskyddsförordningen, jämförd med skäl 79 i samma förordning, framgår visserligen att gemensamt personuppgiftsansvariga är skyldiga att, genom ett inbördes arrangemang, under öppna former fastställa sitt respektive ansvar för att fullgöra skyldigheterna enligt förordningen. Förekomsten av ett sådant inbördes arrangemang utgör emellertid inte en förutsättning för att två eller flera organ ska kunna anses vara gemensamt personuppgiftsansvariga, utan en skyldighet som artikel 26.1 ålägger gemensamt personuppgiftsansvariga, när det väl fastställts att de har denna ställning. Denna skyldighet syftar till att säkerställa att gemensamt personuppgiftsansvariga uppfyller de krav som ställs på dem enligt dataskyddsförordningen. Det nu sagda innebär att redan den omständigheten att flera organ har deltagit i bestämmandet av ändamål och medel för en behandling av personuppgifter innebär att organen får ställning som gemensamt personuppgiftsansvariga.
- 46 Av det ovan anförda följer att den femte frågan ska besvaras enligt följande. Artiklarna 4.7 och 26.1 i dataskyddsförordningen ska tolkas på så sätt att det inte är en förutsättning för att två organ ska kunna anses vara gemensamt personuppgiftsansvariga att det finns ett inbördes arrangemang mellan dessa organ som avser bestämmande av ändamål och medel för behandlingen av de aktuella personuppgifterna och inte heller att det finns ett inbördes arrangemang som fastställer villkoren för det gemensamma personuppgiftsansvaret.

Den fjärde frågan

- 47 Den hänskjutande domstolen har ställt den fjärde frågan för att få klarhet i huruvida artikel 4.2 i dataskyddsförordningen ska tolkas på så sätt att det ska anses utgöra ”behandling”, i den mening som avses i denna bestämmelse, att använda personuppgifter vid funktions- och systemtester av en mobil applikation.
- 48 EU-domstolen gör i denna del följande bedömning. Såsom framgår av punkt 25 ovan är omständigheterna i förevarande fall sådana att det litauiska bolag som hanterade it-systemet för spårning och kontroll av smittsamma sjukdomar som riskerar att sprida sig skulle erhålla kopior av de personuppgifter som samlats in via den aktuella mobilappen. Vid funktions- och systemtestning av appen användes fingerade uppgifter. De enda uppgifter som var verkliga var telefonnummer till anställda vid nämnda bolag.
- 49 I detta avseende vill domstolen för det första påpeka följande. I artikel 4.2 i dataskyddsförordningen definieras begreppet ”behandling” som ”[varje] åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej”. I bestämmelsen finns en icke uttömmande uppräkningslista, som inleds med uttrycket ”såsom”, där det ges exempel på vad som utgör behandling, däribland insamling, tillhandahållande och användning av personuppgifter.
- 50 Det framgår således av ordalydelsen i denna bestämmelse, bland annat av uttrycket ”[varje] åtgärd”, att unionslagstiftaren har avsett att ge begreppet ”behandling” en vidsträckt innebörd (se, för ett liknande resonemang, dom av den 24 februari 2022, Valsts ieņēmumu dienests

(Behandling av personuppgifter för skatteändamål), C-175/20, EU:C:2022:124, punkt 35) och att skälen till att en åtgärd eller en kombination av åtgärder vidtas saknar betydelse vid bedömningen av huruvida åtgärden eller åtgärdskombinationen ska anses utgöra "behandling", i den mening som avses i artikel 4.2 i dataskyddsförordningen.

- 51 Frågan huruvida personuppgifter används för it-tester eller för något annat ändamål påverkar således inte bedömningen av huruvida den aktuella åtgärden ska anses utgöra "behandling", i den mening som avses i artikel 4.2 i dataskyddsförordningen.
- 52 För det andra ska det emellertid påpekas att det endast är behandling som avser "personuppgifter" som utgör "behandling", i den mening som avses i artikel 4.2 i dataskyddsförordningen.
- 53 I artikel 4.1 i dataskyddsförordningen preciseras i detta avseende att begreppet "personuppgifter" ska förstås som "varje upplysning som avser en identifierad eller identifierbar fysisk person", det vill säga som avser "en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet".
- 54 Den omständighet som den hänskjutande domstolen har hänvisat till i sin fjärde fråga, nämligen att det rör sig om "kopior av personuppgifter", innebär inte i sig att dessa kopior inte ska anses utgöra personuppgifter, i den mening som avses i artikel 4.1 i dataskyddsförordningen, under förutsättning att kopiorna faktiskt innehåller upplysningar som avser en identifierad eller identifierbar fysisk person.
- 55 Det ska dock konstateras att fingerade uppgifter inte utgör personuppgifter, i den mening som avses i artikel 4.1 i dataskyddsförordningen. Sådana uppgifter avser nämligen inte en identifierad eller identifierbar fysisk person, utan en person som inte existerar.
- 56 Detsamma gäller anonyma eller anonymiserade uppgifter som används för it-tester.
- 57 Det följer nämligen av skäl 26 i dataskyddsförordningen och av själva definitionen av begreppet personuppgifter i artikel 4.1 i förordningen att detta begrepp inte omfattar "anonym information, nämligen information som inte hänför sig till en identifierad eller identifierbar fysisk person", och inte heller "personuppgifter som anonymiserats på ett sådant sätt att den registrerade inte eller inte längre är identifierbar".
- 58 Det ska däremot påpekas att det framgår av artikel 4.5 jämförd med skäl 26 i dataskyddsförordningen att personuppgifter som endast har pseudonymiserats och som skulle kunna tillskrivas en fysisk person genom att kompletterande uppgifter används ska anses som uppgifter om en identifierbar fysisk person, på vilka principerna om dataskydd är tillämpliga.
- 59 Av det ovan anförda följer att den fjärde frågan ska besvaras enligt följande. Artikel 4.2 i dataskyddsförordningen ska tolkas på så sätt det ska anses utgöra "behandling", i den mening som avses i denna bestämmelse, att använda personuppgifter vid funktions- och systemtester av en mobil applikation. Detta gäller dock inte om de aktuella personuppgifterna har anonymiserats på ett sådant sätt att den person som berörs av uppgifterna inte, eller inte längre, är identifierbar eller om det rör sig om fingerade uppgifter som inte avser en verklig fysisk person.

Den sjätte frågan

- 60 Den hänskjutande domstolen har ställt den sjätte frågan för att få klarhet i huruvida artikel 83 i dataskyddsförordningen ska tolkas på så sätt att administrativa sanktionsavgifter kan påföras med stöd av denna bestämmelse endast om det visas att den personuppgiftsansvarige uppsåtligen eller av oaktsamhet har begått någon av de överträdelser som avses i punkterna 4–6 i denna artikel och på så sätt att en sådan sanktionsavgift kan påföras en personuppgiftsansvarig med avseende på personuppgiftsbehandling som ett personuppgiftsbiträde utfört för dennes räkning.
- 61 EU-domstolen gör i denna del följande bedömning. Vad först gäller frågan huruvida administrativa sanktionsavgifter kan påföras med stöd av artikel 83 i dataskyddsförordningen endast om det visas att den personuppgiftsansvarige eller personuppgiftsbiträdet uppsåtligen eller av oaktsamhet har begått någon av de överträdelser som avses i punkterna 4–6 i denna artikel, kan det konstateras att det av artikel 83.1 framgår att sanktionsavgifter som påförs med stöd av den artikeln ska vara effektiva, proportionerliga och avskräckande. I artikel 83 i dataskyddsförordningen preciseras däremot inte uttryckligen att sådana överträdelser kan beivras med sanktionsavgifter endast om de har begåtts uppsåtligen eller i vart fall av oaktsamhet.
- 62 Den litauiska regeringen och Europeiska unionens råd har av detta dragit slutsatsen att unionslagstiftaren har avsett att ge medlemsstaterna ett visst handlingsutrymme vid genomförandet av artikel 83 i dataskyddsförordningen, som innebär att de kan införa bestämmelser med innebörd att administrativa sanktionsavgifter ska kunna påföras med stöd av denna bestämmelse utan att det behöver visas att den överträdelse av dataskyddsförordningen för vilken sanktionsavgift påförs har begåtts uppsåtligen eller av oaktsamhet.
- 63 En sådan tolkning av artikel 83 i dataskyddsförordningen kan inte godtas.
- 64 Det ska därvid påpekas att enligt artikel 288 FEUF har bestämmelser i förordningar i allmänhet omedelbara verkningar i de nationella rättsordningarna utan att de nationella myndigheterna behöver införa tillämpningsbestämmelser. För att vissa bestämmelser i förordningar ska kunna genomföras kan det dock krävas att medlemsstaterna inför tillämpningsbestämmelser (se, för ett liknande resonemang, dom av den 28 april 2022, *Meta Platforms Ireland*, C-319/20, EU:C:2022:322, punkt 58 och där angiven rättspraxis).
- 65 Så är bland annat fallet med dataskyddsförordningen, där vissa bestämmelser ger medlemsstaterna en möjlighet att införa nationella tilläggsregler, som är strängare eller avvikande i förhållande till förordningen, och som ger dem ett handlingsutrymme för hur dessa bestämmelser i förordningen ska genomföras (dom av den 28 april 2022, *Meta Platforms Ireland*, C-319/20, EU:C:2022:322, punkt 57).
- 66 På samma sätt gäller att det i avsaknad av särskilda processuella regler i dataskyddsförordningen ankommer på varje medlemsstat att i sin rättsordning fastställa – under förutsättning att likvärdighetsprincipen och effektivitetsprincipen iakttas – de processuella regler som gäller för taleformer som syftar till att säkerställa skyddet av de rättigheter som enskilda har enligt förordningen (se, för ett liknande resonemang, dom av den 4 maj 2023, *Österreichische Post* (Ideell skada på grund av behandling av personuppgifter), C-300/21, EU:C:2023:370, punkterna 53 och 54 och där angiven rättspraxis).

- 67 Det finns emellertid ingenting i ordalydelsen av artikel 83.1–83.6 i dataskyddsförordningen som talar för att unionslagstiftaren haft för avsikt att ge medlemsstaterna ett handlingsutrymme vad gäller de materiella krav som en tillsynsmyndighet ska iaktta när den beslutar att påföra en personuppgiftsansvarig administrativa sanktionsavgifter för någon av de överträdelser som avses i punkterna 4–6 i artikel 83.
- 68 Av artikel 83.7 i dataskyddsförordningen framgår visserligen att varje medlemsstat får fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras myndigheter och andra offentliga organ som är etablerade i medlemsstaten. Vidare framgår av artikel 83.8 jämförd med skäl 129 i förordningen att tillsynsmyndighetens utövande av sina befogenheter enligt denna artikel ska omfattas av lämpliga processuella skyddsregler i enlighet med unionsrätten och medlemsstaternas nationella rätt, inbegripet effektiva rättsmedel och rättssäkerhet.
- 69 Det ska dock konstateras att den omständigheten att förordningen således innebär en möjlighet för medlemsstaterna att införa undantagsregler som gäller i förhållande till där etablerade myndigheter och andra offentliga organ samt regler om vilka krav som ställs på det förfarande som tillsynsmyndigheterna ska följa när de avser att påföra administrativa sanktionsavgifter, inte på något sätt innebär att medlemsstaterna även har rätt att, utöver sådana undantagsregler och regler om krav på förfarandet, införa regler om vilka materiella krav som måste vara uppfyllda för att en personuppgiftsansvarig ska kunna hållas ansvarig och påföras administrativa sanktionsavgifter med stöd av artikel 83 i förordningen. Härtill kommer att den omständigheten att unionslagstiftaren har varit noga med att uttryckligen ange att medlemsstaterna har en möjlighet att införa sådana undantagsregler och regler om krav på förfarandet, men däremot inte angett något om en möjlighet att införa regler om materiella krav av nyss nämnt slag, visar att unionslagstiftaren inte har avsett att ge medlemsstaterna något handlingsutrymme i det avseendet.
- 70 Denna bedömning vinner även stöd av en jämförelse av artiklarna 83 och 84 i dataskyddsförordningen. Av artikel 84.1 i förordningen framgår nämligen att medlemsstaterna fortsatt har befogenhet att fastställa regler om ”andra sanktioner” för överträdelser av förordningen, ”särskilt för överträdelser som inte är föremål för administrativa sanktionsavgifter enligt artikel 83”. Vid en sådan jämförelse av nämnda bestämmelser framgår således att denna befogenhet inte omfattar att fastställa regler om vilka materiella krav som måste vara uppfyllda för att sådana administrativa sanktionsavgifter ska kunna påföras. Dessa krav omfattas således enbart av unionsrätten.
- 71 Vad gäller dessa krav ska det påpekas att artikel 83.2 i dataskyddsförordningen innehåller en uppräknning av vilka faktorer som en tillsynsmyndighet ska beakta vid beslut om att påföra en personuppgiftsansvarig administrativa sanktionsavgifter. Av led b) i bestämmelsen framgår att en av de faktorer som ska beaktas är ”[o]m överträdelsen skett med uppsåt eller genom oaktsamhet”. Någon hänvisning till en möjlighet att hålla en personuppgiftsansvarig ansvarig utan att överträdelsen skett varken uppsåtligt eller av oaktsamhet görs däremot inte i någon av de faktorer som räknas upp i artikel 83.2 i dataskyddsförordningen.
- 72 Artikel 83.2 i dataskyddsförordningen måste dessutom läsas tillsammans med punkt 3 i samma artikel, som reglerar vad som ska gälla i fall där det är fråga om flera överträdelser av denna förordning. Den bestämmelsen har följande lydelse: ”Om en personuppgiftsansvarig eller ett personuppgiftsbiträde, med avseende på en och samma eller sammankopplade

uppgiftsbehandlings, uppsåtliga eller av oaktsamhet överträder flera av bestämmelserna i denna förordning får den administrativa sanktionsavgiftens totala belopp inte överstiga det belopp som fastställs för den allvarligaste överträdelsen”.

- 73 Det följer således av ordalydelsen i artikel 83.2 i dataskyddsförordningen att det endast är i fall där en personuppgiftsansvarig har åsidosatt bestämmelserna i förordningen genom ett vållande, det vill säga uppsåtliga eller av oaktsamhet, som det kan bli aktuellt att påföra den personuppgiftsansvarige administrativa sanktionsavgifter med stöd av denna artikel.
- 74 En sådan tolkning vinner stöd av den allmänna systematiken i och syftet med dataskyddsförordningen.
- 75 För det första har unionslagstiftaren infört en sanktionsordning som innebär att tillsynsmyndigheterna ges möjlighet att påföra de sanktioner som är mest lämpliga beroende på omständigheterna i varje enskilt fall.
- 76 I artikel 58 i dataskyddsförordningen, som reglerar vilka befogenheter tillsynsmyndigheterna ska ha, anges nämligen i punkt 2 i) att dessa myndigheter får påföra administrativa sanktionsavgifter med stöd av artikel 83 i förordningen ”utöver eller i stället för” andra i artikel 58.2 angivna korrigerande åtgärder, såsom varningar, reprimander eller förelägganden. På samma sätt anges i skäl 148 i dataskyddsförordningen att vid mindre överträdelser eller om den troliga sanktionsavgiften skulle innebära en oproportionerlig börda för en fysisk person får tillsynsmyndigheterna utfärda en reprimand i stället för att påföra en sanktionsavgift.
- 77 För det andra framgår det särskilt av skäl 10 i dataskyddsförordningen att förordningens bestämmelser bland annat syftar till att säkerställa en enhetlig och hög skyddsnivå för fysiska personer vid behandling av personuppgifter inom unionen och till att säkerställa att bestämmelserna om skydd av fysiska personers grundläggande fri- och rättigheter vid behandling av personuppgifter tillämpas på ett konsekvent och enhetligt sätt i hela unionen. I skälen 11 och 129 i dataskyddsförordningen talas dessutom just om vikten av att se till att förordningen tillämpas på ett konsekvent sätt och i samband med detta framhålls behovet av att säkerställa att tillsynsmyndigheterna har likvärdiga befogenheter i fråga om övervakning och tillsyn av efterlevnaden av bestämmelserna om skydd av personuppgifter och att de kan påföra likvärdiga sanktioner vid överträdelser av förordningen.
- 78 Genom att det finns en sanktionsordning som gör det möjligt att påföra administrativa sanktionsavgifter enligt artikel 83 i dataskyddsförordningen – om de särskilda omständigheterna i det enskilda fallet är sådana att detta är befogat – skapas ett incitament för personuppgiftsansvariga och personuppgiftsbiträden att följa bestämmelserna i förordningen. Administrativa sanktionsavgifter bidrar genom sin avskräckande verkan till att stärka skyddet för fysiska personer vid behandling av personuppgifter och utgör därför en nyckelfaktor för att säkerställa att dessa personers rättigheter iakttas, vilket ligger i linje med förordningens syfte att säkerställa en hög skyddsnivå för fysiska personer vid behandling av personuppgifter.
- 79 Unionslagstiftaren har dock inte ansett att det för att säkerställa en sådan hög skyddsnivå behöver införas en bestämmelse om att administrativa sanktionsavgifter kan påföras även i fall där överträdelsen inte skett vare sig uppsåtliga eller av oaktsamhet. Med hänsyn till att dataskyddsförordningen syftar till att uppnå en både likvärdig och enhetlig skyddsnivå och att det för detta ändamål krävs att förordningen tillämpas på ett konsekvent sätt i hela unionen, skulle det strida mot detta ändamål att tillåta medlemsstaterna att införa en sådan ordning för påförande av

administrativa sanktionsavgifter enligt artikel 83 i förordningen. En sådan valfrihet skulle dessutom kunna snedvrída konkurrensen mellan ekonomiska aktörer inom unionen, vilket skulle strida mot de mål som unionslagstiftaren gett uttryck för bland annat i skälen 9 och 13 i förordningen.

- 80 Det nu sagda innebär följande. Artikel 83 i dataskyddsförordningen utgör hinder för att administrativa sanktionsavgifter påförs för någon av de överträdelser som avses i punkterna 4–6 i samma artikel utan att det behöver visas att den personuppgiftsansvarige har begått överträdelsen uppsåtligen eller av oaktsamhet. Det krävs således att överträdelsen har begåtts genom ett vållande för att administrativa sanktionsavgifter ska kunna påföras.
- 81 Vad därvid gäller frågan huruvida en överträdelse har begåtts uppsåtligen eller av oaktsamhet, och därigenom kan beivras med administrativa sanktionsavgifter enligt artikel 83 i dataskyddsförordningen, vill EU-domstolen även påpeka att personuppgiftsansvariga kan påföras sanktionsavgifter för ett agerande som omfattas av dataskyddsförordningens tillämpningsområde om de inte kan anses ha varit okunniga om att deras agerande utgjorde en överträdelse, oavsett om de varit medvetna om att de åsidosatte bestämmelserna i dataskyddsförordningen (se, analogt, dom av den 18 juni 2013, *Schenker & Co. m.fl.*, C-681/11, EU:C:2013:404, punkt 37 och där angiven rättspraxis, dom av den 25 mars 2021, *Lundbeck/kommissionen*, C-591/16 P, EU:C:2021:243, punkt 156, och dom av den 25 mars 2021, *Arrow Group och Arrow Generics/kommissionen*, C-601/16 P, EU:C:2021:244, punkt 97).
- 82 Om den personuppgiftsansvarige är en juridisk person gäller vidare att det för att artikel 83 i dataskyddsförordningen ska kunna tillämpas inte krävs ett aktivt handlande från den juridiska personens ledningsorgan eller ens att detta känt till överträdelsen (se, analogt, dom av den 7 juni 1983, *Musique Diffusion française m.fl./kommissionen*, 100/80–103/80, EU:C:1983:158, punkt 97, och dom av den 16 februari 2017, *Tudapetrol Mineralölerzeugnisse Nils Hansen/kommissionen*, C-94/15 P, EU:C:2017:124, punkt 28 och där angiven rättspraxis).
- 83 EU-domstolen övergår därefter till att pröva frågan huruvida en personuppgiftsansvarig kan påföras administrativa sanktionsavgifter med stöd av artikel 83 i dataskyddsförordningen med avseende på personuppgiftsbehandling som ett personuppgiftsbiträde utfört. Enligt definitionen i artikel 4.8 i dataskyddsförordningen avses med personuppgiftsbiträde ”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning”.
- 84 Såsom anförts i punkt 36 ovan gäller att en personuppgiftsansvarig är ansvarig inte bara för all personuppgiftsbehandling som denne själv utför, utan även för behandling som utförs för dennes räkning. Detta innebär att den personuppgiftsansvarige kan påföras administrativa sanktionsavgifter med stöd av artikel 83 i dataskyddsförordningen i ett fall där det förekommit otillåten behandling av personuppgifter och där det inte är den personuppgiftsansvarige själv, utan ett personuppgiftsbiträde som denne har anlitat, som har utfört nämnda behandling för den personuppgiftsansvariges räkning.
- 85 Den personuppgiftsansvariges ansvar för ett personuppgiftsbiträdes handlande kan dock inte anses omfatta även fall där personuppgiftsbiträdet har behandlat personuppgifter för sina egna ändamål. Detta ansvar omfattar inte heller fall där personuppgiftsbiträdet har behandlat personuppgifter i strid med den ram eller de former för behandlingen som den personuppgiftsansvarige bestämt eller på ett sådant sätt att den personuppgiftsansvarige inte

rimligen kan anses ha samtyckt till behandlingen. Enligt artikel 28.10 i dataskyddsförordningen ska nämligen i ett sådant fall personuppgiftsbiträdet anses vara personuppgiftsansvarig vid behandling av nyss nämnt slag.

- 86 Av det ovan anförda följer att den sjätte frågan ska besvaras enligt följande. Artikel 83 i dataskyddsförordningen ska tolkas på så sätt att administrativa sanktionsavgifter kan påföras med stöd av denna bestämmelse endast om det visas att den personuppgiftsansvarige uppsåtligt eller av oaktsamhet har begått någon av de överträdelser som avses i punkterna 4–6 i denna artikel och på så sätt att administrativa sanktionsavgifter kan påföras en personuppgiftsansvarig med avseende på personuppgiftsbehandling som ett personuppgiftsbiträde utfört för dennes räkning. Detta gäller dock inte om personuppgiftsbiträdet i samband med detta har utfört personuppgiftsbehandlingar för sina egna ändamål eller har behandlat personuppgifter i strid med den ram eller de former för behandlingen som den personuppgiftsansvarige bestämt eller på ett sådant sätt att den personuppgiftsansvarige inte rimligen kan anses ha samtyckt till behandlingen.

Rättegångskostnader

- 87 Eftersom förfarandet i förhållande till parterna i det nationella målet utgör ett led i beredningen av samma mål, ankommer det på den hänskjutande domstolen att besluta om rättegångskostnaderna. De kostnader för att avge yttrande till domstolen som andra än nämnda parter har haft är inte ersättningsgilla.

Mot denna bakgrund beslutar domstolen (stora avdelningen) följande:

- 1) Artikel 4.7 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 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)**

ska tolkas på följande sätt:

Ett organ som har gett ett företag i uppdrag att utveckla en mobil it-applikation, och som i samband med detta har deltagit i bestämmandet av ändamål och medel för den behandling av personuppgifter som utförs via denna applikation, kan anses vara personuppgiftsansvarig i den mening som avses i denna bestämmelse, även i ett fall där detta organ inte självt har utfört behandlingar av personuppgifter och inte uttryckligen har gett sitt samtycke till att konkreta åtgärder som innebär behandling av personuppgifter utförs eller till att mobilapplikationen görs tillgänglig för allmänheten och inte heller har förvärvat applikationen. Detta gäller dock inte om nämnda organ innan applikationen gjordes tillgänglig för allmänheten uttryckligen motsatte sig tillgängliggörandet och den behandling av personuppgifter som skett till följd av detta.

- 2) Artiklarna 4.7 och 26.1 i förordning 2016/679**

ska tolkas på följande sätt:

Det inte är en förutsättning för att två organ ska kunna anses vara gemensamt personuppgiftsansvariga att det finns ett inbördes arrangemang mellan dessa organ

som avser bestämmande av ändamål och medel för behandlingen av de aktuella personuppgifterna och inte heller att det finns ett inbördes arrangemang som fastställer villkoren för det gemensamma personuppgiftsansvaret.

3) Artikel 4.2 i förordning 2016/679

ska tolkas på följande sätt:

Det ska anses utgöra ”behandling”, i den mening som avses i denna bestämmelse, att använda personuppgifter vid funktions- och systemtester av en mobil applikation. Detta gäller dock inte om de aktuella personuppgifterna har anonymiserats på ett sådant sätt att den person som berörs av uppgifterna inte, eller inte längre, är identifierbar eller om det rör sig om fingerade uppgifter som inte avser en verklig fysisk person.

4) Artikel 83 i förordning 2016/679

ska tolkas på följande sätt:

Administrativa sanktionsavgifter kan påföras med stöd av denna bestämmelse endast om det visas att den personuppgiftsansvarige uppsåtligen eller av oaktsamhet har begått någon av de överträdelser som avses i punkterna 4–6 i denna artikel.

Administrativa sanktionsavgifter kan påföras en personuppgiftsansvarig med avseende på personuppgiftsbehandling som ett personuppgiftsbiträde utfört för dennes räkning. Detta gäller dock inte om personuppgiftsbiträdet i samband med detta har utfört personuppgiftsbehandlingar för sina egna ändamål eller har behandlat personuppgifter i strid med den ram eller de former för behandlingen som den personuppgiftsansvarige bestämt eller på ett sådant sätt att den personuppgiftsansvarige inte rimligen kan anses ha samtyckt till behandlingen.

Underskrifter