Oikeustapauskokoelma

UNIONIN TUOMIOISTUIMEN TUOMIO (ensimmäinen jaosto)

26 päivänä syyskuuta 2024*

Ennakkoratkaisupyyntö – Luonnollisten henkilöiden suojelu henkilötietojen käsittelyssä – Asetus (EU) 2016/679 – 57 artiklan 1 kohdan a ja f alakohta – Valvontaviranomaisen tehtävät – 58 artiklan 2 kohta – Korjaavat toimenpiteet – Hallinnollinen seuraamusmaksu – Valvontaviranomaisen harkintavalta – Rajat

Asiassa C-768 P,

jossa on kyse SEUT 267 artiklaan perustuvasta ennakkoratkaisupyynnöstä, jonka Verwaltungsgericht Wiesbaden (Wiesbadenin hallintotuomioistuin, Saksa) on esittänyt 10.12.2021 tekemällään päätöksellä, joka on saapunut unionin tuomioistuimeen 14.12.2021, saadakseen ennakkoratkaisun asiassa

TR

vastaan

Land Hessen,

UNIONIN TUOMIOISTUIN (ensimmäinen jaosto),

toimien kokoonpanossa: jaoston puheenjohtaja A. Arabadjiev sekä tuomarit T. von Danwitz, P. G. Xuereb, A. Kumin (esittelevä tuomari) ja I. Ziemele,

julkisasiamies: P. Pikamäe,

kirjaaja: Calot Escobar,

ottaen huomioon kirjallisessa käsittelyssä esitetyn,

ottaen huomioon huomautukset, jotka sille ovat esittäneet

– TR, edustajanaan F. Wittmaack, Rechtsanwalt,

– Land Hessen, edustajinaan M. Kottmann ja G. Ziegenhorn, Rechtsanwälte,

– Itävallan hallitus, asiamiehinään J. Schmoll ja T. Rappersberger,

– Portugalin hallitus, asiamiehinään P. Barros da Costa, J. Ramos ja C. Vieira Guerra,

* Oikeudenkäyntikieli: saksa.

– Romanian hallitus, asiamiehinään L.-E. Baţagoi ja E. Gane,

– Norjan hallitus, asiamiehinään S.-E. Jahr Dahl, L.-M. Moen Jünge ja M. Munthe-Kaas,

– Euroopan komissio, asiamiehinään A. Bouchagiar, M. Heller ja H. Kranenborg,

kuultuaan julkisasiamiehen 11.4.2024 pidetyssä istunnossa esittämän ratkaisuehdotuksen,

on antanut seuraavan

tuomion

1 Ennakkoratkaisupyyntö koskee luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27.4.2016 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (yleinen tietosuoja-asetus) (EUVL 2016, L 119, s. 1; jäljempänä yleinen tietosuoja-asetus) 57 artiklan 1 kohdan a ja f alakohdan, 58 artiklan 2 kohdan ja 77 artiklan 1 kohdan tulkintaa.

2 Ennakkoratkaisupyyntö on esitetty asiassa, jossa asianosaisina ovat TR ja Land Hessen (Hessenin osavaltio, Saksa) ja jossa on kyse siitä, että Hessischer Beauftragte für Datenschutz und Informationsfreiheit (Hessenin osavaltion tietosuojavaltuutettu ja tiedonvälityksen vapauden valtuutettu, jäljempänä HBDI) kieltäytyi ryhtymästä toimenpiteisiin Sparkasse X:ää (X:n säästöpankki, jäljempänä Sparkasse) vastaan.

Asiassa sovellettavat oikeussäännöt

3 Yleisen tietosuoja-asetuksen johdanto-osan 6, 7, 10, 129 ja 148 perustelukappaleessa todetaan seuraavaa:

”(6) Teknologian nopea kehitys ja globalisaatio ovat tuoneet henkilötietojen suojeluun uusia haasteita. Henkilötietoja jaetaan ja kerätään nyt merkittävän paljon enemmän. – –

(7) Tällainen kehitys edellyttää vahvaa ja johdonmukaisempaa tietosuojakehystä [Euroopan] unionissa, jota tuetaan tehokkaalla täytäntöönpanolla, sillä on tärkeää rakentaa luottamusta, jonka pohjalta digitaalitalous voi kehittyä koko sisämarkkinoiden alueella. – –

– –

(10) Jotta voitaisiin varmistaa yhdenmukainen ja korkeatasoinen luonnollisten henkilöiden suojelu ja poistaa henkilötietojen liikkuvuuden esteet unionissa, luonnollisten henkilöiden oikeuksien ja vapauksien suojelun tason näiden tietojen käsittelyssä olisi oltava vastaava kaikissa jäsenvaltioissa. – –

– –

(129) – – Valvontaviranomaisten valtuuksia olisi käytettävä unionin oikeudessa ja jäsenvaltioiden lainsäädännössä vahvistettujen asianmukaisten menettelytakeiden mukaisesti puolueettomasti, asianmukaisesti ja kohtuullisessa ajassa. Jokaisen toimenpiteen olisi erityisesti oltava tarkoituksenmukainen, tarpeellinen ja

oikeasuhteinen, jotta voidaan varmistaa tämän asetuksen noudattaminen siten, että otetaan huomioon kunkin yksittäisen tapauksen olosuhteet, kunnioitetaan jokaisen henkilön oikeutta tulla kuulluksi ennen kuin ryhdytään yksittäiseen toimenpiteeseen, joka vaikuttaisi häneen epäedullisesti, ja vältetään aiheuttamasta asianomaisille henkilöille tarpeettomia kustannuksia ja liiallisia haittoja. – –

– –

(148) Tämän asetuksen sääntöjen täytäntöönpanon vahvistamiseksi asetuksen säännösten rikkomisesta olisi määrättävä seuraamuksia, kuten hallinnollisia seuraamusmaksuja, valvontaviranomaisen tämän asetuksen mukaisesti määräämien asianmukaisten toimenpiteiden lisäksi tai niiden sijasta. Jos kyseessä on vähäinen rikkominen tai jos määrättävä seuraamusmaksu olisi kohtuuton rasitus luonnolliselle henkilölle, voidaan seuraamusmaksun sijasta antaa huomautus. Rikkomisen luonteeseen, vakavuuteen ja kestoon, sen tahallisuuteen, aiheutuneen vahingon lieventämiseksi toteutettuihin toimiin, vastuun asteeseen tai mahdollisiin vastaaviin aiempiin rikkomisiin, tapaan, jolla rikkominen tuli valvontaviranomaisen tietoon, rekisterinpitäjälle tai henkilötietojen käsittelijälle määrättyjen toimenpiteiden noudattamiseen, käytännesääntöjen noudattamiseen ja mahdollisiin muihin raskauttaviin tai lieventäviin tekijöihin olisi kuitenkin kiinnitettävä asianmukaista huomiota. – –”

4 Kyseisen asetuksen 5 artiklan sanamuoto on seuraava:

”1. Henkilötietojen suhteen on noudatettava seuraavia vaatimuksia:

a) niitä on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (’lainmukaisuus, kohtuullisuus ja läpinäkyvyys’);

b) ne on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla – – (’käyttötarkoitussidonnaisuus ’);

c) niiden on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään (’tietojen minimointi’);

d) niiden on oltava täsmällisiä ja tarvittaessa päivitettyjä – – (’täsmällisyys’);

e) ne on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten – – (’säilytyksen rajoittaminen’);

f) niitä on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus – – (’eheys ja luottamuksellisuus’).

2. Rekisterinpitäjä vastaa siitä, ja sen on pystyttävä osoittamaan se, että 1 kohtaa on noudatettu (’osoitusvelvollisuus’).”

5 Mainitun asetuksen 24 artiklan 1 kohdassa säädetään seuraavaa:

”Ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa.”

6 Saman asetuksen 33 artiklassa säädetään seuraavaa:

”1. Jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta 55 artiklan mukaisesti toimivaltaiselle valvontaviranomaiselle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. – –

– –

3. Edellä 1 kohdassa tarkoitetussa ilmoituksessa on vähintään

a) kuvattava henkilötietojen tietoturvaloukkaus, mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät;

b) ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa;

c) kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset;

d) kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

– –”

7 Yleisen tietosuoja-asetuksen 34 artiklan 1 kohdassa säädetään seuraavaa:

”Kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä.”

8 Yleisen tietosuoja-asetuksen VI luku, jonka otsikko on ”Riippumattomat valvontaviranomaiset”, käsittää asetuksen 51–59 artiklan.

9 Kyseisen asetuksen 51 artiklan 1 kohdan sanamuoto on seuraava:

”Kunkin jäsenvaltion on varmistettava, että yksi tai useampi riippumaton viranomainen on vastuussa tämän asetuksen soveltamisen valvonnasta luonnollisten henkilöiden perusoikeuksien ja -vapauksien suojaamiseksi käsittelyssä ja henkilötietojen vapaan liikkuvuuden helpottamiseksi unionissa, jäljempänä ’valvontaviranomainen’.”

10 Yleisen tietosuoja-asetuksen 57 artiklan, jonka otsikko on ”Tehtävät”, 1 kohdassa säädetään seuraavaa:

”Tämän asetuksen mukaisesti vahvistettuja muita tehtäviä rajoittamatta jokaisen valvontaviranomaisen on alueellaan

a) valvottava tämän asetuksen soveltamista ja täytäntöönpanoa;

– –

f) käsiteltävä rekisteröidyn tai 80 artiklan mukaisen elimen, järjestön tai yhdistyksen tekemiä valituksia ja tutkittava siinä määrin kuin se on asianmukaista valituksen kohdetta ja ilmoitettava valituksen tekijälle tutkinnan etenemisestä sekä tutkinnan tuloksista kohtuullisen ajan kuluessa, erityisesti jos asia edellyttää lisätutkimuksia tai koordinointia toisen valvontaviranomaisen kanssa;

– –”

11 Mainitun asetuksen 58 artiklan, jonka otsikko on ”Valtuudet”, 1 ja 2 kohdassa säädetään seuraavaa:

”1. Jokaisella valvontaviranomaisella on kaikki seuraavat tutkintavaltuudet:

a) määrätä rekisterinpitäjä ja henkilötietojen käsittelijä ja tarvittaessa rekisterinpitäjän tai henkilötietojen käsittelijän edustaja antamaan kaikki tehtäviensä suorittamiseksi tarvittavat tiedot;

– –

2. Jokaisella valvontaviranomaisella on kaikki seuraavat korjaavat toimivaltuudet:

a) varoittaa rekisterinpitäjää tai henkilötietojen käsittelijää siitä, että aiotut käsittelytoimet ovat todennäköisesti tämän asetuksen säännösten vastaisia;

b) antaa huomautus rekisterinpitäjälle tai henkilötietojen käsittelijälle, jos käsittelytoimet ovat olleet tämän asetuksen säännösten vastaisia;

c) määrätä rekisterinpitäjä tai henkilötietojen käsittelijä noudattamaan rekisteröidyn pyyntöjä, jotka koskevat tähän asetukseen perustuvien rekisteröidyn oikeuksien käyttöä;

d) määrätä rekisterinpitäjä tai henkilötietojen käsittelijä saattamaan käsittelytoimet tämän asetuksen säännösten mukaisiksi, tarvittaessa tietyllä tavalla ja tietyn määräajan kuluessa;

e) määrätä rekisterinpitäjä ilmoittamaan henkilötietojen tietoturvaloukkauksesta rekisteröidylle;

f) asettaa väliaikainen tai pysyvä rajoitus käsittelylle, mukaan lukien käsittelykielto;

– –

i) määrätä 83 artiklan nojalla hallinnollinen seuraamusmaksu tässä kohdassa tarkoitettujen toimenpiteiden lisäksi tai niiden asemesta kunkin yksittäisen tapauksen olosuhteista riippuen;

– –”

12 Mainitun asetuksen 77 artiklassa säädetään seuraavaa:

”1. Jokaisella rekisteröidyllä on oikeus tehdä kantelu valvontaviranomaiselle, erityisesti siinä jäsenvaltiossa, jossa hänen vakinainen asuinpaikkansa tai työpaikkansa on taikka jossa väitetty rikkominen on tapahtunut, jos rekisteröity katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan tätä asetusta, sanotun kuitenkaan rajoittamatta muita hallinnollisia muutoksenhakukeinoja tai oikeussuojakeinoja.

2. Valvontaviranomaisen, jolle kantelu on tehty, on ilmoitettava kantelun tekijälle sen etenemisestä ja ratkaisusta, mukaan lukien 78 artiklan mukaisten oikeussuojakeinojen mahdollisuudesta.”

13 Saman asetuksen 83 artiklan 1 ja 2 kohdassa säädetään seuraavaa:

”1. Jokaisen valvontaviranomaisen on varmistettava, että 4, 5 ja 6 kohdassa tarkoitettujen tämän asetuksen rikkomisesta määrättävien hallinnollisten seuraamusmaksujen määrääminen tämän artiklan mukaisesti on kussakin yksittäisessä tapauksessa tehokasta, oikeasuhteista ja varoittavaa.

2. Hallinnolliset seuraamusmaksut määrätään kunkin yksittäisen tapauksen olosuhteiden mukaisesti 58 artiklan 2 kohdan a–h ja j alakohdassa tarkoitettujen toimenpiteiden lisäksi tai niiden sijasta. Kun päätetään hallinnollisen seuraamusmaksun määräämisestä ja hallinnollisen seuraamusmaksun määrästä, kussakin yksittäisessä tapauksessa on otettava asianmukaisesti huomioon seuraavat seikat:

a) rikkomuksen luonne, vakavuus ja kesto huomioon ottaen kyseisen tietojenkäsittelyn luonne, laajuus tai tarkoitus, sekä niiden rekisteröityjen lukumäärä, joihin rikkomus vaikuttaa, ja heille aiheutuneen vahingon suuruus;

b) rikkomuksen tahallisuus tai tuottamuksellisuus;

c) rekisterinpitäjän tai henkilötietojen käsittelijän toteuttamat toimet rekisteröidyille aiheutuneen vahingon lieventämiseksi;

d) rekisterinpitäjän tai henkilötietojen käsittelijän vastuun aste, ottaen huomioon heidän 25 ja 32 artiklan nojalla toteuttamansa tekniset ja organisatoriset toimenpiteet;

e) rekisterinpitäjän tai henkilötietojen käsittelijän mahdolliset aiemmat vastaavat rikkomukset;

f) yhteistyön määrä valvontaviranomaisen kanssa rikkomuksen korjaamiseksi ja sen mahdollisten haittavaikutusten lieventämiseksi;

g) henkilötietoryhmät, joihin rikkomus vaikuttaa;

h) tapa, jolla rikkomus tuli valvontaviranomaisen tietoon, erityisesti se, ilmoittiko rekisterinpitäjä tai henkilötietojen käsittelijä rikkomuksesta ja missä laajuudessa;

i) jos kyseiselle rekisterinpitäjälle tai henkilötietojen käsittelijälle on aikaisemmin määrätty samasta asiasta 58 artiklan 2 kohdassa tarkoitettuja toimenpiteitä, näiden toimenpiteiden noudattaminen;

j) 40 artiklan mukaisten hyväksyttyjen käytännesääntöjen tai 42 artiklan mukaisten hyväksyttyjen sertifiointimekanismien noudattaminen; ja

k) mahdolliset muut tapaukseen sovellettavat raskauttavat tai lieventävät tekijät, kuten rikkomuksesta suoraan tai epäsuorasti saadut mahdolliset taloudelliset edut tai rikkomuksella vältetyt tappiot.”

Pääasia ja ennakkoratkaisukysymykset

14 Sparkasse on julkisoikeudellinen kunnallinen laitos, joka harjoittaa muun muassa pankki- ja luottotoimintaa. Se ilmoitti 15.11.2019 HBDI:lle henkilötietojen tietoturvaloukkauksesta yleisen tietosuoja-asetuksen 33 artiklan mukaisesti, koska eräs sen työntekijöistä oli useaan otteeseen tutustunut luvattomasti erään sen asiakkaista, TR:n, henkilötietoihin. Sparkasse ei ilmoittanut TR:lle hänen henkilötietojensa loukkaamisesta.

15 Saatuaan sattumalta tiedon siitä, että hänen henkilötietoihinsa oli tutustuttu perusteettomasti, TR teki 27.7.2020 kantelun HBDI:lle yleisen tietosuoja-asetuksen 77 artiklan nojalla. Kyseisessä kantelussa hän arvosteli sitä, ettei hänelle ollut ilmoitettu hänen henkilötietojensa loukkaamisesta, mikä oli kyseisen asetuksen 34 artiklan vastaista. Hän arvosteli myös Sparkassen lokitietojen säilyttämisaikaa, joka oli vahvistettu vain kolmeksi kuukaudeksi, sekä sen henkilöstön laajoja tietojen tarkastelua koskevia oikeuksia.

16 TR:n tekemän kantelun jälkeen HBDI kuuli Sparkassea kirjallisesti ja suullisesti sitä vastaan esitetystä arvostelusta. Kuulemisen aikana Sparkasse ilmoitti, ettei se ollut tehnyt ilmoitusta yleisen tietosuoja-asetuksen 34 artiklan nojalla, koska sen tietosuojavastaava oli katsonut, ettei TR:n oikeuksiin ja vapauksiin kohdistunut korkeaa riskiä. Kyseessä olevaa työntekijää vastaan oli nimittäin toteutettu kurinpitotoimenpiteitä, ja tämä oli vahvistanut kirjallisesti, ettei hän ollut kopioinut eikä säilyttänyt henkilötietoja, ettei hän ollut toimittanut niitä kolmansille osapuolille eikä hän tulisi tekemään niin tulevaisuudessa. Koska HBDI oli arvostellut lokitietojen liian lyhyttä säilytysaikaa, Sparkasse ilmoitti sille, että tätä kysymystä tarkasteltaisiin uudelleen.

17 HBDI ilmoitti TR:lle 3.9.2020 tekemällään päätöksellä, ettei Sparkasse ollut rikkonut yleisen tietosuoja-asetuksen 34 artiklaa, koska Sparkassen arviointi, jonka mukaan henkilötietojen tietoturvaloukkauksesta ei voinut aiheutua kyseisessä artiklassa tarkoitettua korkeaa riskiä hänen oikeuksilleen ja vapauksilleen, ei ollut ilmeisen virheellinen. Vaikka työntekijä oli tutustunut tietoihin, mikään ei nimittäin viitannut siihen, että hän olisi luovuttanut niitä kolmansille tai käyttänyt niitä TR:n vahingoksi. Lisäksi HBDI ilmoitti, että se oli kehottanut Sparkassea säilyttämään lokitietonsa jatkossa pidempään kuin kolmen kuukauden ajan. Lopuksi HBDI hylkäsi TR:n tekemän kantelun sen kysymyksen osalta, joka koskee Sparkassen työntekijöiden mahdollisuutta tarkastella henkilötietoja, ja korosti, että laajat tiedonsaantioikeudet voidaan lähtökohtaisesti myöntää, jos on varmaa, että jokainen käyttäjä on tietoinen edellytyksistä, joilla hän voi tarkastella tietoja. HBDI:n mukaan jokaisen tietojen tarkastelukerran periaatteellinen valvonta ei ole tarpeen.

18 TR nosti 3.9.2020 tehdystä päätöksestä kanteen ennakkoratkaisua pyytäneessä tuomioistuimessa, Verwaltungsgericht Wiesbadenissa (Wiesbadenin hallintotuomioistuin, Saksa), ja vaati, että kyseinen tuomioistuin velvoittaa HBDI:n ryhtymään toimenpiteisiin Sparkassea vastaan.

19 TR vetoaa kanteensa tueksi siihen, että HBDI ei käsitellyt hänen kanteluaan yleisen tietosuoja-asetuksen vaatimusten mukaisesti eli ottaen huomioon tosiseikkojen kokonaisuuden, ja toteaa lisäksi, että HBDI:n olisi pitänyt määrätä Sparkasselle hallinnollinen seuraamusmaksu, kun otetaan huomioon kyseisen asetuksen eri säännösten ja erityisesti sen 5 artiklan, 12 artiklan 3 kohdan, 15 artiklan 1 kohdan c alakohdan, 33 artiklan 1 kohdan c alakohdan ja 33 artiklan 3 kohdan rikkominen. TR:n mukaan tapauksessa, jossa rikkominen on todettu, tarkoituksenmukaisuusperiaatetta ei sovelleta, joten HBDI:llä ei ole harkintavaltaa päättää siitä, ryhtyykö se toimenpiteisiin vai ei, vaan korkeintaan vapaus valita toimenpiteet, jotka se toteuttaa.

20 Ennakkoratkaisua pyytänyt tuomioistuin pohtii tältä osin lähinnä sitä, onko siinä tapauksessa, että henkilötietojen suojaa koskevien säännösten rikkominen näytetään toteen, yleistä tietosuoja-asetusta tulkittava siten, että valvontaviranomaisen on toteutettava kyseisen asetuksen 58 artiklan 2 kohdan nojalla hallinnollisen seuraamusmaksun kaltaisia korjaavia toimenpiteitä, vai siten, että kyseisellä viranomaisella on harkintavaltaa, jonka nojalla se voi olosuhteiden mukaan pidättyä toteuttamasta tällaisia toimenpiteitä.

21 Ennakkoratkaisua pyytänyt tuomioistuin toteaa, että ensimmäinen tulkinta, jota TR kannattaa ja joka on esitetty myös osassa oikeuskirjallisuutta, perustuu siihen, että valvontaviranomaisella olevan toimivallan toteuttaa korjaavia toimenpiteitä tarkoituksena on palauttaa säännöstenmukainen tilanne silloin, kun tietojenkäsittelyllä loukataan kansalaisten oikeuksia. Yleisen tietosuoja-asetuksen 58 artiklan 2 kohta on näin ollen ymmärrettävä velvoittavaksi säännökseksi, jonka perusteella kansalaisella on oikeus vaatia viranomaistoimia silloin, kun yritys tai viranomainen on käsitellyt lainvastaisesti kansalaisen henkilötietoja tai muulla tavoin loukannut tämän oikeuksia. Kun tietoturvaloukkaus on todettu, valvontaviranomaisen on siis ryhdyttävä korjaaviin toimenpiteisiin, ja sillä on ainoastaan vapaus valita, minkä säädetyistä toimenpiteistä se toteuttaa.

22 Ennakkoratkaisua pyytänyt tuomioistuin epäilee kuitenkin tämän tulkinnan, jota se pitää liian laajana, perusteltavuutta ja on pikemminkin taipuvainen katsomaan, että valvontaviranomaisella on harkintavaltaa, jonka nojalla se voi tietyissä tapauksissa pidättäytyä korjaavan toimenpiteen toteuttamisesta ja erityisesti seuraamusmaksun määräämisestä tapauksessa, jossa rikkominen on näytetty toteen. Vaikka valvontaviranomaisella on yleisen tietosuoja-asetuksen 57 artiklan 1 kohdan f alakohdan nojalla velvollisuus tutkia kantelut huolellisesti ja tutkia kukin yksittäistapaus, sillä ei kuitenkaan ole velvollisuutta toteuttaa korjaavia toimenpiteitä kaikissa tilanteissa. Ennakkoratkaisua pyytäneen tuomioistuimen mukaan valvontaviranomaisella ei siis ole tällaista velvollisuutta silloin, kun henkilötietojen suojaa koskevia sääntöjä on rikottu menneisyydessä, mutta rekisterinpitäjä on toteuttanut toimenpiteitä, joiden perusteella voidaan olettaa, että tietosuojan loukkaus ei toistu.

23 Tässä tilanteessa Verwaltungsgericht Wiesbaden on päättänyt lykätä asian käsittelyä ja esittää unionin tuomioistuimelle seuraavan ennakkoratkaisukysymyksen:

”Onko [yleisen tietosuoja-asetuksen] 57 artiklan 1 kohdan a ja f alakohtaa sekä 58 artiklan 2 kohdan a–j alakohtaa, luettuna yhdessä 77 artiklan 1 kohdan kanssa, tulkittava siten, että siinä tapauksessa, että valvontaviranomainen toteaa, että tietojenkäsittely loukkaa rekisteröidyn oikeuksia, valvontaviranomainen on aina velvollinen ryhtymään kyseisen asetuksen 58 artiklan 2 kohdassa tarkoitettuihin toimenpiteisiin?”

Ennakkoratkaisupyynnön tutkittavaksi ottaminen

24 TR ei kiistä nimenomaisesti ennakkoratkaisupyynnön tutkittavaksi ottamista mutta väittää, että vastaus esitettyyn kysymykseen ei ole tarpeen pääasian ratkaisemiseksi. Hänen kanteessaan vaaditaan ainoastaan sitä, että ennakkoratkaisua pyytänyt tuomioistuin velvoittaa HBDI:n lausumaan sen käsiteltäväksi saatetussa kantelussa esitetyistä väitteistä tietosuoja-asetuksen 57 artiklan 1 kohdan f alakohdan mukaisesti, eikä sitä, että HBDI velvoitettaisiin käyttämään yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan mukaisia toimivaltuuksiaan.

25 Tässä yhteydessä on huomattava, että SEUT 267 artiklalla käyttöön otetussa unionin tuomioistuimen ja kansallisten tuomioistuinten välisessä yhteistyössä yksinomaan kansallisen tuomioistuimen, jossa asia on vireillä ja joka vastaa annettavasta ratkaisusta, tehtävänä on asian erityispiirteiden perusteella harkita, onko ennakkoratkaisu tarpeen asian ratkaisemiseksi ja onko sen unionin tuomioistuimelle esittämillä kysymyksillä merkitystä asian kannalta. Jos esitetyt kysymykset koskevat unionin oikeuden tulkintaa, unionin tuomioistuimen on näin ollen lähtökohtaisesti ratkaistava ne (tuomio 30.11.2023, Ministero dell’Instruzione ja INPS, C-270/22, EU:C:2023:933, 33 kohta oikeuskäytäntöviittauksineen).

26 Tästä seuraa, että olettamana on, että kansallisen tuomioistuimen sen säännöstön ja niiden tosiseikkojen perusteella, joiden määrittämisestä se vastaa ja joiden paikkansapitävyyden selvittäminen ei ole unionin tuomioistuimen tehtävä, esittämillä unionin oikeuden tulkintaan liittyvillä kysymyksillä on merkitystä asian ratkaisun kannalta. Unionin tuomioistuin voi jättää tutkimatta kansallisen tuomioistuimen esittämän pyynnön ainoastaan, jos on ilmeistä, että pyydetyllä unionin oikeuden tulkitsemisella ei ole mitään yhteyttä kansallisessa tuomioistuimessa käsiteltävän asian tosiseikkoihin tai kohteeseen, jos kyseinen ongelma on luonteeltaan hypoteettinen taikka jos unionin tuomioistuimella ei ole tiedossaan niitä tosiseikkoja ja oikeudellisia seikkoja, jotka ovat tarpeen, jotta se voisi antaa hyödyllisen vastauksen sille esitettyihin kysymyksiin (tuomio 30.11.2023, Ministero dell’Instruzione ja INPS, C-270/22, EU:C:2023:933, 34 kohta oikeuskäytäntöviittauksineen).

27 Nyt käsiteltävässä asiassa ennakkoratkaisua pyytänyt tuomioistuin korostaa, että TR on vedonnut oikeuteen, joka koskee sitä, että HBDI toteuttaa toimenpiteitä, ja väittänyt, että HBDI:llä oli velvollisuus määrätä seuraamusmaksu Sparkasselle.

28 Näin ollen ei ole ilmeistä, että pyydetyllä unionin oikeuden tulkitsemisella ei ole mitään yhteyttä kansallisessa tuomioistuimessa käsiteltävän asian tosiseikkoihin tai kohteeseen.

29 Ennakkoratkaisupyyntö voidaan näin ollen ottaa tutkittavaksi.

Ennakkoratkaisukysymyksen tarkastelu

30 Esitettyyn kysymykseen vastaamiseksi on aluksi muistutettava, että unionin oikeussäännön tulkinta edellyttää, että huomioon otetaan paitsi sen sanamuoto myös asiayhteys, johon se kuuluu, sekä sen toimen tavoitteet ja tarkoitus, jonka osa se on (tuomio 7.12.2023, SCHUFA Holding (Jäännösveloista vapauttaminen), C-26/22 ja C-64/22, EU:C:2023:958, 48 kohta oikeuskäytäntöviittauksineen).

31 On myös muistutettava, että Euroopan unionin perusoikeuskirjan 8 artiklan 3 kohdan ja yleisen tietosuoja-asetuksen 51 artiklan 1 kohdan ja 57 artiklan 1 kohdan a alakohdan mukaan kansalliset valvontaviranomaiset ovat vastuussa niiden unionin säännösten noudattamisen valvonnasta, jotka koskevat luonnollisten henkilöiden suojelua henkilötietojen käsittelyssä (tuomio 7.12.2023, SCHUFA Holding (Jäännösveloista vapauttaminen), C-26/22 ja C-64/22, EU:C:2023:958, 55 kohta oikeuskäytäntöviittauksineen).

32 Erityisesti yleisen tietosuoja-asetuksen 57 artiklan 1 kohdan f alakohdan nojalla jokaisen valvontaviranomaisen on alueellaan käsiteltävä kantelut, joita kyseisen asetuksen 77 artiklan 1 kohdan mukaan jokaisella rekisteröidyllä on oikeus tehdä, jos hän katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan kyseistä asetusta, ja tutkittava siinä määrin kuin se on asianmukaista kantelun kohdetta ja ilmoitettava kantelun tekijälle tutkinnan etenemisestä ja sen lopputuloksesta kohtuullisen ajan kuluessa. Valvontaviranomaisen asiana on tutkia tällainen kantelu kaikkea asianmukaista huolellisuutta noudattaen (ks. vastaavasti tuomio 7.12.2023, SCHUFA Holding (Jäännösveloista vapauttaminen), C-26/22 ja C-64/22, EU:C:2023:958, 56 kohta oikeuskäytäntöviittauksineen).

33 Yleisen tietosuoja-asetuksen 58 artiklan 1 kohdassa annetaan kullekin valvontaviranomaiselle kanteluiden käsittelemistä varten merkittävät tutkintavaltuudet. Jos tällainen viranomainen tutkintansa päätteeksi toteaa, että kyseisen asetuksen säännöksiä on rikottu, sen on reagoitava asianmukaisesti todetun puutteen korjaamiseksi, ja kaikkien toimenpiteiden on, kuten mainitun asetuksen johdanto-osan 129 perustelukappaleessa täsmennetään, oltava muun muassa tarkoituksenmukaisia, tarpeellisia ja oikeasuhteisia, jotta voidaan varmistaa mainitun asetuksen noudattaminen siten, että otetaan huomioon kunkin yksittäisen tapauksen olosuhteet. Tätä varten asetuksen 58 artiklan 2 kohdassa luetellaan korjaavat toimenpiteet, joita valvontaviranomainen voi käyttää (ks. vastaavasti tuomio 7.12.2023, SCHUFA Holding (Jäännösveloista vapauttaminen), C-26/22 ja C-64/22, EU:C:2023:958, 57 kohta oikeuskäytäntöviittauksineen).

34 Yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan nojalla valvontaviranomaisella on valtuudet muun muassa antaa huomautus rekisterinpitäjälle tai henkilötietojen käsittelijälle, jos käsittelytoimet ovat olleet kyseisen asetuksen säännösten vastaisia (b alakohta), tai määrätä rekisterinpitäjä tai henkilötietojen käsittelijä noudattamaan rekisteröidyn pyyntöjä, jotka koskevat kyseiseen asetukseen perustuvien rekisteröidyn oikeuksien käyttöä (c alakohta), määrätä rekisterinpitäjä tai henkilötietojen käsittelijä saattamaan käsittelytoimet saman asetuksen säännösten mukaisiksi tarvittaessa tietyllä tavalla ja tietyn määräajan kuluessa (d alakohta) tai määrätä yleisen tietosuoja-asetuksen 83 artiklan nojalla hallinnollinen seuraamusmaksu kyseisessä 58 artiklan 2 kohdassa tarkoitettujen toimenpiteiden lisäksi tai niiden asemesta kunkin yksittäisen tapauksen olosuhteista riippuen (i alakohta).

35 Kantelumenettely on tarkoitettu mekanismiksi, jolla suojellaan tehokkaasti rekisteröityjen oikeuksia ja etuja (tuomio 7.12.2023, SCHUFA Holding (Jäännösveloista vapauttaminen), C-26/22 ja C-64/22, EU:C:2023:958, 58 kohta).

36 Nyt käsiteltävässä asiassa ennakkoratkaisupyynnöstä ilmenee, että HBDI tutki aineellisesti pääasian kantajan sille tekemän valituksen ja ilmoitti tälle tutkinnan lopputuloksesta. Tarkemmin sanottuna HBDI vahvisti, että pääasian kantajan henkilötietoja on loukattu Sparkassessa siten, että eräs sen työntekijöistä oli tarkastellut niitä luvattomasti. HBDI kuitenkin hylkäsi pääasian kantajan tekemän kantelun Sparkassen henkilöstön tarkasteluoikeuksien osalta. Lisäksi se totesi, ettei asiassa ollut syytä ryhtyä toimenpiteisiin Sparkassea vastaan yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan nojalla.

37 Tältä osin on korostettava, että yleisessä tietosuoja-asetuksessa jätetään valvontaviranomaiselle harkintavaltaa sen suhteen, miten sen on korjattava todettu puute, koska sen 58 artiklan 2 kohdassa valvontaviranomaiselle annetaan toimivalta toteuttaa erilaisia korjaavia toimenpiteitä. Unionin tuomioistuin on jo todennut, että asianmukaisen ja tarpeellisen keinon valinta on valvontaviranomaisen tehtävä ja että sen on tehtävä tämä valinta konkreettisen tapauksen kaikki olosuhteet huomioon ottaen ja suoritettava kaikkea vaadittavaa huolellisuutta noudattaen tehtävänsä, joka on valvoa sitä, että tietosuoja-asetusta noudatetaan kaikilta osin (ks. vastaavasti tuomio 16.7.2020, Facebook Ireland ja Schrems, C-311/18 P, EU:C:2020:559, 112 kohta).

38 Tätä harkintavaltaa rajoittaa kuitenkin tarve varmistaa henkilötietojen suojelun yhdenmukainen ja korkea taso sääntöjen tiukalla soveltamisella, kuten yleisen tietosuoja-asetuksen johdanto-osan 7 ja 10 perustelukappaleesta ilmenee.

39 Erityisesti yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan i alakohdassa tarkoitettujen hallinnollisten seuraamusmaksujen osalta kyseisen asetuksen 83 artiklan 2 kohdasta ilmenee, että niitä määrätään kunkin yksittäisen tapauksen olosuhteiden mukaisesti kyseisen 58 artiklan 2 kohdassa tarkoitettujen muiden toimenpiteiden lisäksi tai niiden sijasta. Kyseisessä 83 artiklan 2 kohdassa täsmennetään lisäksi, että kun päätetään hallinnollisen seuraamusmaksun määräämisestä ja seuraamusmaksun määrästä, valvontaviranomaisen on kussakin yksittäisessä tapauksessa otettava asianmukaisesti huomioon kyseisen säännöksen a–k alakohdassa esitetyt seikat, kuten rikkomuksen luonne, vakavuus ja kesto.

40 Unionin lainsäätäjän säätämän seuraamusjärjestelmän avulla valvontaviranomaiset voivat näin ollen määrätä asianmukaisimpia ja perustelluimpia seuraamuksia kunkin tapauksen olosuhteiden mukaan (ks. vastaavasti tuomio 5.12.2023, Nacionalinis visuomenės sveikatos centras, C-683/21, EU:C:2023:949, 75 ja 78 kohta) ottaen samalla huomioon, kuten tämän tuomion 37 ja 38 kohdassa muistutetaan, tarpeen valvoa sitä, että tietosuoja-asetusta noudatetaan kaikilta osin, ja varmistaa henkilötietojen suojelun yhdenmukainen ja korkea taso sääntöjen tiukalla soveltamisella.

41 Näin ollen yleisen tietosuoja-asetuksen 58 artiklan 2 kohdasta tai sen 83 artiklasta ei voida päätellä, että valvontaviranomaisella olisi velvollisuus toteuttaa kaikissa tapauksissa silloin, kun se toteaa henkilötietojen tietoturvaloukkauksen, korjaava toimenpide ja erityisesti määrätä hallinnollinen seuraamusmaksu, koska sen velvollisuutena on vastaavissa olosuhteissa reagoida asianmukaisesti todetun puutteen korjaamiseksi. Kuten julkisasiamies totesi

ratkaisuehdotuksensa 81 kohdassa, kantelun tekijällä, jonka oikeuksia on loukattu, ei näin ollen ole subjektiivista oikeutta siihen, että valvontaviranomainen määrää rekisterinpitäjälle hallinnollisen seuraamusmaksun.

42 Valvontaviranomaisen on sitä vastoin puututtava asiaan, kun yhden tai useamman yleisen tietosuoja-asetuksen 58 artiklan 2 kohdassa säädetyn korjaavan toimenpiteen toteuttaminen on, kun otetaan huomioon kaikki konkreettisen tapauksen olosuhteet, asianmukaista, tarpeellista ja oikeasuhteista todetun puutteen korjaamiseksi ja kyseisen asetuksen täysimääräisen noudattamisen varmistamiseksi.

43 Tältä osin ei ole poissuljettua, että valvontaviranomainen voi poikkeuksellisesti ja yksittäistapauksen erityisolosuhteet huomioon ottaen jättää toteuttamatta korjaavan toimenpiteen, vaikka henkilötietojen tietoturvaloukkauksen on todettu tapahtuneen. Näin voisi olla muun muassa silloin, kun todettu rikkominen ei ole jatkunut, esimerkiksi silloin, kun rekisterinpitäjä, joka on lähtökohtaisesti toteuttanut yleisen tietosuoja-asetuksen 24 artiklassa tarkoitettuja tarvittavia teknisiä ja organisatorisia toimenpiteitä, on heti saatuaan tiedon kyseisestä rikkomisesta toteuttanut asianmukaiset ja tarpeelliset toimenpiteet, jotta kyseinen rikkominen lopetetaan eikä sitä enää toisteta, kun otetaan huomioon erityisesti kyseisen asetuksen 5 artiklan 2 kohdan ja 24 artiklan mukaiset rekisterinpitäjän velvollisuudet.

44 Tulkintaa, jonka mukaan valvontaviranomainen ei silloin, kun se toteaa henkilötietojen tietoturvaloukkauksen, ole kaikissa tapauksissa velvollinen toteuttamaan yleisen tietosuoja-asetuksen 58 artiklan 2 kohdassa tarkoitettua korjaavaa toimenpidettä, tukevat kyseisen asetuksen 58 artiklan 2 kohdan ja 83 artiklan tavoitteet.

45 Yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan tavoitteesta on todettava, että kyseisen asetuksen johdanto-osan 129 perustelukappaleesta ilmenee, että kyseisen säännöksen tavoitteena on sen varmistaminen, että henkilötietoja käsitellään kyseisen asetuksen mukaisesti ja että asetuksen rikkomista koskevat tilanteet palautetaan unionin oikeuden mukaisiksi kansallisten valvontaviranomaisten toimilla (tuomio 14.3.2024, Újpesti Polgármesteri Hivatal, C-46/23, EU:C:2024:239, 40 kohta).

46 Tästä seuraa, että korjaava toimenpide voidaan poikkeuksellisesti ja konkreettisen tapauksen erityisolosuhteet huomioon ottaen jättää toteuttamatta sillä edellytyksellä, että tilanne, jossa yleistä tietosuoja-asetusta on rikottu, on jo palautettu sääntöjenmukaiseksi ja rekisterinpitäjä varmistaa, että henkilötietojen käsittely on kyseisen asetuksen mukaista, ja että tällainen valvontaviranomaisen toimimatta jättäminen ei ole omiaan loukkaamaan tämän tuomion 38 kohdassa mainittua vaatimusta sääntöjen tiukasta soveltamisesta.

47 Yleisen tietosuoja-asetuksen 83 artiklan, joka koskee hallinnollisten seuraamusmaksujen määräämistä, tavoitteena on puolestaan kyseisen asetuksen johdanto-osan 148 perustelukappaleen sanamuodon mukaan kyseisen asetuksen sääntöjen täytäntöönpanon vahvistaminen. Mainitussa perustelukappaleessa todetaan kuitenkin myös, että jos kyseessä on mainitun asetuksen vähäinen rikkominen tai jos määrättävä seuraamusmaksu olisi kohtuuton rasitus luonnolliselle henkilölle, valvontaviranomaiset voivat pidättyä määräämästä hallinnollista seuraamusmaksua ja antaa sen sijasta huomautuksen (ks. vastaavasti tuomio 5.12.2023, Nacionalinis visuomenės sveikatos centras, C-683/21, EU:C:2023:949, 76 kohta).

48 Nyt käsiteltävässä asiassa ennakkoratkaisupyynnöstä ilmenee, että Sparkasse ilmoitti HBDI:lle yleisen tietosuoja-asetuksen 33 artiklan mukaisesti pääasian kantajan henkilötietojen loukkaamisesta, joka johtuu siitä, että eräs sen työntekijöistä oli tarkastellut henkilötietoja luvattomasti. Siinä todettiin lisäksi, että kyseistä työntekijää vastaan oli ryhdytty kurinpitotoimiin ja että lokitietojen säilytysaikaa tarkasteltaisiin uudelleen. Tässä tilanteessa HBDI pidättyi toteuttamasta yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan mukaista korjaavaa toimenpidettä ja erityisesti määräämästä hallinnollista seuraamusmaksua.

49 Koska valvontaviranomaisen tekemän kantelua koskevan päätöksen on oltava täysimääräisen tuomioistuinvalvonnan kohteena (tuomio 7.12.2023, SCHUFA Holding (Jäännösveloista vapauttaminen), C-26/22 ja C-64/22, EU:C:2023:958, 70 kohta), ennakkoratkaisua pyytäneen tuomioistuimen on selvitettävä, käsittelikö HBDI kyseessä olevaa kantelua kaikkea vaadittavaa huolellisuutta noudattaen ja toimiko HBDI pääasiassa kyseessä olevan päätöksen tehdessään yleisen tietosuoja-asetuksen 58 artiklan 2 kohdassa sille annetun harkintavallan rajoissa (ks. vastaavasti tuomio 7.12.2023, SCHUFA Holding (Jäännösveloista vapauttaminen), C-26/22 ja C-64/22, EU:C:2023:958, 68 ja 69 kohta oikeuskäytäntöviittauksineen).

50 Kaiken edellä esitetyn perusteella esitettyyn kysymykseen on vastattava, että yleisen tietosuoja-asetuksen 57 artiklan 1 kohdan a ja f alakohtaa, 58 artiklan 2 kohtaa ja 77 artiklan 1 kohtaa on tulkittava siten, että kun henkilötietojen tietoturvaloukkaus on todettu, valvontaviranomainen ei ole velvollinen toteuttamaan korjaavaa toimenpidettä ja erityisesti määräämään hallinnollista seuraamusmaksua kyseisen 58 artiklan 2 kohdan nojalla, jos tällainen toimenpide ei ole asianmukainen, tarpeellinen tai oikeasuhteinen todetun puutteen korjaamiseksi ja kyseisen asetuksen täysimääräisen noudattamisen varmistamiseksi.

Oikeudenkäyntikulut

51 Pääasian asianosaisten osalta asian käsittely unionin tuomioistuimessa on välivaihe kansallisessa tuomioistuimessa vireillä olevan asian käsittelyssä, minkä vuoksi kansallisen tuomioistuimen asiana on päättää oikeudenkäyntikulujen korvaamisesta. Oikeudenkäyntikuluja, jotka ovat aiheutuneet muille kuin näille asianosaisille huomautusten esittämisestä unionin tuomioistuimelle, ei voida määrätä korvattaviksi.

Näillä perusteilla unionin tuomioistuin (ensimmäinen jaosto) on ratkaissut asian seuraavasti:

Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27.4.2016 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (yleinen tietosuoja-asetus) 57 artiklan 1 kohdan a ja f alakohtaa, 58 artiklan 2 kohtaa ja 77 artiklan 1 kohtaa

on tulkittava siten, että

kun henkilötietojen tietoturvaloukkaus on todettu, valvontaviranomainen ei ole velvollinen toteuttamaan korjaavaa toimenpidettä ja erityisesti määräämään hallinnollista seuraamusmaksua kyseisen 58 artiklan 2 kohdan nojalla, jos tällainen toimenpide ei ole asianmukainen, tarpeellinen tai oikeasuhteinen todetun puutteen korjaamiseksi ja kyseisen asetuksen täysimääräisen noudattamisen varmistamiseksi.

Allekirjoitukset