

Lieta C-61/22

**Lūguma sniegt prejudiciālu nolēmumu kopsavilkums saskaņā ar Tiesas
Reglamenta 98. panta 1. punktu**

Iesniegšanas datums:

2022. gada 1. februāris

Iesniedzējtiesa:

Verwaltungsgericht Wiesbaden (Vācija)

Datums, kurā pieņemts iesniedzējtiesas nolēmums:

2022. gada 13. janvāris

Pieteicējs:

RL

Atbildētāja:

Landeshauptstadt Wiesbaden

Pamatlietas priekšmets

Pirkstu nospiedumu noņemšana un to saglabāšana personas apliecībās – Regulas (ES) 2019/1157 3. panta 5. punkts – Spēkā esamība – Regulas pieņemšanas procedūra – Eiropas Savienības Pamattiesību hartas 7. un 8. pants – Vispārīgās datu aizsardzības regulas 35. panta 10. punkts

Lūguma sniegt prejudiciālu nolēmumu priekšmets un tiesiskais pamats

Regulas (ES) 2019/1157 3. panta 5. punkta spēkā esamība, LESD 267. pants

Prejudiciālais jautājums

Vai pienākums noņemt pirkstu nospiedumus un tos saglabāt personas apliecībā atbilstoši Eiropas Parlamenta un Padomes Regulas (ES) 2019/1157 (2019. gada 20. jūnijs) par Savienības pilsoņu personas apliecību un Savienības pilsoņiem un viņu ģimenes locekļiem, kuri izmanto tiesības brīvi pārvietoties, izsniegto

uzturēšanās dokumentu drošības uzlabošanu (OV L 188, 12.07.2019., 67. lpp.) 3. panta 5. punktam ir pretrunā augstāka ranga Savienības tiesību normām, it īpaši

- a) LESD 77. panta 3. punktam,
- b) Pamattiesību hartas 7. un 8. pantam,
- c) Vispārīgās datu aizsardzības regulas 35. panta 10. punktam,

un līdz ar to šā iemesla dēļ nav spēkā?

Piemērojamās Savienības tiesību normas

Eiropas Savienības Pamattiesību hartas 7., 8. un 52 pants;

Līguma par Eiropas Savienības darbību 21., 77. un 289. pants;

Eiropas Parlamenta un Padomes Regulas (ES) 2019/1157 (2019. gada 20. jūnijs) par Savienības pilsoņu personas apliecību un Savienības pilsoņiem un viņu ģimenes locekļiem, kuri izmanto tiesības brīvi pārvietoties, izsniegto uzturēšanās dokumentu drošības uzlabošanu 2., 17., 18., 19., 21., 22., 40. un 41. apsvērumus un 3. un 11. pants;

Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) 9. un 35. pants.

Piemērojamās valsts tiesību normas

Gesetz über Personalausweise und den elektronischen Identitätsnachweis [Personas apliecību un elektronisko identitātes apliecinājumu likums] (*Personalausweisgesetz* [Personas apliecību likums] – *PAuswG*) 5. un 9. pants.

Īss pamatlietas faktisko apstākļu un tiesvedības izklāsts

1. Pieteicējs lūdza izsniegt viņam personas apliecību bez pirkstu nospiedumu noņemšanas. Atbildētāja šo lūgumu noraidīja, jo *Personalausweisgesetz* (turpmāk tekstā – *PAuswG*) 5. panta 9. punktā, kas pamatots ar Regulu (ES) 2019/1157, ir paredzēta obligāta divu pirkstu nospiedumu noņemšana.
2. Regula (ES) 2019/1157 ir spēkā kopš 2021. gada 2. augusta. Regulas (ES) 2019/1157 3. panta 5. punktā ir noteikts, ka dalībvalstu izsniegtajās personas apliecībās iestrādā datu nesēju, kas ietver apliecības turētāja sejas attēlu un divus pirkstu nospiedumus sadarbspējīgos digitālos formātos. Arī Vācijas tiesību aktos tika iekļauts regulējums, kas paredz pirkstu nospiedumu saglabāšanu personas

apliecībā(*PAuswG* 5. panta 9. punkts), turklāt, kā liecina likuma anotācija, Vācijas likumdevējs uzskatīja, ka pirkstu nospiedumi ir jānoņem atbilstoši Regulas (ES) 2019/1157 3. panta 5. punktam.

- 3 Pieteicējs 2021. gada 30. novembrī lūdza izsniegt viņam jaunu personas apliecību bez pirkstu nospiedumiem, jo viņa vecās personas apliecības mikroshēma esot bojāta. Šādas jaunas personas apliecības izsniegšana tika atteikta, jo kopš 2021. gada 2. augusta pirkstu nospiedumu noņemšana esot obligāta. Turklāt pieteicējam neesot tiesību prasīt jaunas personas apliecības izdošanu, jo viņam jau esot derīgs personu apliecinošs dokuments. Personas apliecība esot derīga arī tad, ja mikroshēma ir bojāta.
- 4 Saskaņā ar Vācijas tiesību aktiem par personas apliecību izsniegšanu atbildīgā iestāde darbojas arī kā apdraudējuma novēršanas iestāde. Tomēr tieši personas apliecību izsniegšanai un ar to saistīto datu apstrādei ir piemērojama nevis Direktīva (ES) 2016/680, bet gan, kā minēts Regulas (ES) 2019/1157 40. apsvērumā, Vispārīgā datu aizsardzības regula (turpmāk tekstā – VDAR). Tādēļ nav tā, ka šajā lietā *Oberbürgermeister* [pilsētas domes priekšsēdētājs] rīkotos autonomi interpretējamo Eiropas tiesību aktos reglamentētajā apdraudējuma novēršanas jomā. Saskaņā ar Direktīvas (ES) 2016/680 1. panta 1. punktu un 2. panta 1. punktu šī direktīva ir piemērojama vienīgi tad, kad iestādes veic darbības, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu kriminālsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu. Pasu un personas apliecību izsniegšana šajā jomā neietilpst.

Īss lūguma sniegt prejudiciālu nolēmumu pamatojuma izklāsts

- 5 Sprieduma taisīšanai ir nepieciešams prejudiciālais nolēmums. Ja Regulas (ES) 2019/1157 3. panta 5. punkts ir pretrunā augstāka ranga Savienības tiesību normām, pieteicējam ir tiesības saņemt personas apliecību bez pirkstu nospiedumu noņemšanas (*PAuswG* 9. panta 1. punkta pirmais teikums). *PAuswG* 5. panta 9. punktā ietvertais valsts tiesiskais regulējums tad būtu nepamatots, jo tas būtu pretrunā Savienības tiesību normām.
- 6 Pat ja no *PAuswG* 28. panta 3. punkta izriet, ka pieteicēja vecā personas apliecība joprojām ir derīga – lai gan tās mikroshēma ir bojāta – pieteicējam vismaz pases 10 gadus ilgā derīguma termiņa beigās ir jāiesniedz pieteikums par jaunas personas apliecības izsniegšanu. Turklāt saskaņā ar *PAuswG* 6. panta 2. punktu pieteicējs jaunas personas apliecības pieteikumu var iesniegt pirms personas apliecības termiņa beigām, ja viņš var norādīt uz tiesiski pamatotām interesēm saņemt jaunu apliecību. Bojātas mikroshēmas gadījumā personas identifikācija tiešsaistē vairs nav iespējama. Nav iespējams izmantot arī automātisko robežkontroles funkciju. Šie ierobežojumi tās izmantošanā ir uzskatāmi par tiesiski pamatotām interesēm saņemt jaunu apliecību.

- 7 Iesniedzējtiesai ir šaubas par to, vai Regulas (ES) 2019/1157 3. panta 5. punkts ir saderīgs ar citām Savienības tiesību normām. Šīs šaubas ir balstītas uz to, ka Regula (ES) 2019/1157 tika pieņemta parastajā likumdošanas procedūrā, apsvērumiem par Regulas (ES) 2019/1157 3. panta 5. punkta saderību ar Eiropas Savienības Pamattiesību hartas (turpmāk tekstā – Harta) 7. un 8. pantu un to, ka nav pieņemts novērtējuma lēmums atbilstoši VDAR 35. panta 10. punktam.
- 8 Minētā tiesa ir pārliecināta, ka Regula (ES) 2019/1157 būtu bijusi jāpieņem LESD 77. pantā izklāstītajā īpašajā likumdošanas procedūrā.
- 9 LESD 289. pants ietver nošķirumu starp parasto likumdošanas procedūru un īpašo likumdošanas procedūru. Regula (ES) 2019/1157 ir pamatota ar LESD 21. panta 2. punktu, un tā tika pieņemta parastajā likumdošanas procedūrā. Saskaņā ar LESD 21. panta 2. punktu Eiropas Parlaments un Padome saskaņā ar parasto likumdošanas procedūru var pieņemt noteikumus, lai sekmētu tiesības brīvi pārvietoties, ja izrādās, ka minētā mērķa sasniegšanai vajadzīga Savienības rīcība, bet Līgumi nav piešķirušī šim nolūkam vajadzīgās pilnvaras.
- 10 LESD 77. panta 3. punkta pirmais teikums ietver vēl vienu kompetenci formulējošu normu, kas citastarp attiecas uz personas apliecību regulējumu. Saskaņā ar šo normu Padome saskaņā ar īpašu likumdošanas procedūru var pieņemt noteikumus par pasēm, personas apliecībām, uzturēšanās atļaujām vai līdzīgiem dokumentiem, ja Savienības pasākumi izrādās nepieciešami, lai sekmētu tiesības brīvi pārvietoties, ja vien Līgumos nav paredzētas citas pilnvaras. Padome pēc apspriešanās ar Eiropas Parlamentu lēmumu pieņem vienprātīgi. Līdz ar šo nepieciešamo vienprātību dalībvalstīm šajā jomā ir atstāta maksimāli iespējama suverenitāte.
- 11 LESD 77. pants atbilst agrākā EKL (EK līguma) 62. pantam. Pieņemot Regulu (EK) Nr. 2252/2004, kuras 1. panta 2. punktā ir noteikts, ka pasēs tiek iekļauti pirkstu nospiedumi, likumdevējs pamatojās uz EKL 62. pantu. Eiropas Savienības Tiesa 2013. gada 17. oktobra spriedumā *Schwarz* (C-291/12, EU:C:2013:670) ir nospriedusi, ka EKL 62. panta 2. punkta a) apakšpunkts bija uzskatāms par atbilstīgu tiesisko pamatu Regulas (EK) Nr. 2252/2004, it īpaši tās 1. panta 2. punkta, pieņemšanai.
- 12 LESD 77. panta 3. punktā noteiktā kompetence prevalē pār LESD 21. panta 2. punktu, jo 77. panta 3. punkts kā satura ziņā speciālāka norma ietver augstākas prasības pret likumdošanas procedūru, un LESD 21. panta 2. punkts ir piemērojams vienīgi tad, ja Līgumos attiecībā uz mērķa sekmēt tiesības brīvi pārvietoties sasniegšanu nav paredzētas nekādas citas pilnvaras. Regula (ES) 2019/1157 gan neattiecas uz Šengenas *acquis* pilnveidošanu, tomēr tās nolūks – tāpat kā Regulai (EK) 2252/2004 – ir saskaņot drošības elementus un ieviest biometriskos identifikatorus, kas ir svarīgs solis jaunu elementu izmantošanā, ņemot vērā turpmāko attīstību Eiropas mērogā. Tādējādi – tāpat kā Regulas (EK) 2252/2004 gadījumā – ir paaugstināma dokumentu (šajā gadījumā – nevis pasu, bet personas apliecību) drošības pakāpe.

- 13 Ņemot vērā visu iepriekš izklāstīto, tiesa uzskata, ka, lai īstenotu Regulas (ES) 2019/1157 un līdz ar to arī šīs regulas 3. panta 5. punkta iedarbīgu pieņemšanu, būtu bijusi jāievēro LESD 77. panta 3. punktā paredzētā īpašā likumdošanas procedūra.
- 14 Turklāt satura ziņā pastāv šaubas par to, vai pirkstu nospiedumu noņemšana un to saglabāšana personas apliecībā atbilst Hartas 7. un 8. pantam.
- 15 Saskaņā ar Hartas 7. pantu ikvienai personai ir tiesības uz savas privātās un ģimenes dzīves, dzīvokļa un saziņas neaizskaramību. No Hartas 8. panta izriet ikvienas personas tiesības uz savu personas datu aizsardzību.
- 16 Eiropas Savienības Tiesa jau 2013. gada 17. oktobra spriedumā *Schwarz* (C-291/12, EU:C:2013:670, 27. un 30. punkts), , atsaucoties uz ECT spriedumu, 2008. gada 4. decembris *S. un Marper*/Apvienotā Karaliste (*Reports of judgments and decisions* 2008-V, 213. lpp., 68. un 84. punkts) ir konstatējusi, ka valsts iestāžu veiktā pirkstu nospiedumu noņemšana un to saglabāšana pasēs, kas paredzēta Regulas (EK) Nr. 2252/2004 1.panta 2. punktā, ir tiesību uz privātās dzīves neaizskaramību un personas datu aizsardzību aizskārums. Pirkstu nospiedumi ir personas dati, jo tie objektīvi satur unikālu informāciju par fiziskajām personām un ļauj tās precīzi identificēt. Tās pašas pamattiesības ir aizskartas arī, veicot pirkstu nospiedumu noņemšanu un to saglabāšanu personas apliecībās.
- 17 Iesniedzējtiesai ir šaubas par to, vai pirkstu nospiedumu noņemšana un līdz ar to Hartas 7. un 8. pantā nostiprināto tiesību aizskārums, it īpaši ņemot vērā Hartas 52. pantu un 8. panta 2. punktu, ir attaisnojams arī personas apliecību jomā. Hartas 8. panta 2. punktā ir noteikts, ka personas dati var tikt apstrādāti tikai ar attiecīgās personas piekrišanu vai ar citu likumīgu pamatojumu, kas paredzēts tiesību aktos.
- 18 Iesniedzējtiesa ir pārliecināta, ka – līdzīgi tam, kā Eiropas Savienības Tiesa ir nospriedusi attiecībā uz pasēm, – šajā lietā nav saņemta personas apliecības pieteicēja piekrišana viņa pirkstu nospiedumu noņemšanai. Taču Regulas (ES) 2019/1157 3. panta 5. punktā ir paredzēts, ka tā ir obligāta jebkuras personas apliecības gadījumā.
- 19 Saskaņā ar *PAuswG* 1. panta 1. punkta pirmo teikumu ikvienam Vācijas valstspiederīgajam, kurš sasniedzis 16 gadu vecumu un kuram ir pienākums reģistrēties vai kurš galvenokārt uzturas Vācijā, bet uz viņu neattiecas pienākums reģistrēties, ir jābūt derīgai personas apliecībai. Lai izsniegtu šo dokumentu, obligāti ir paredzēts noņemt pirkstu nospiedumus. Tā kā pastāv pienākums saņemt personas apliecību, nevar uzskatīt, ka personas, kuras lūdz izsniegt viņām personas apliecību, ir devušas piekrišanu šādi datu apstrādei (skat. EST spriedumu, 2013. gada 17. oktobris, *Schwarz*, C-291/12, EU:C:2013:670, 31. punkts).
- 20 Turklāt saskaņā ar Hartas 52. panta 1. punktu ir jāpastāv *legitīmam* likumīgam pamatojumam.

- 21 Likumiski reglamentēta pirkstu nospiedumu saglabāšana personas apliecībā gan ir paredzēta Regulas (ES) 2019/1157 3. panta 5. punktā. Tas vismaz daļēji atbilst arī Savienības atzītajiem vispārējo interešu mērķiem, kuri ir formulēti tās 1., 2., 4., 18. un 46. apsvērumā.
- 22 Eiropas Savienībā personas apliecību var izmantot, šķērsojot iekšējās robežas. Turklāt arī valstis, kas nav ES sastāvā, atļauj ieceļošanu ar personas apliecību, piemēram, jo īpaši, Šveice, Islande, Norvēģija, Albānija un Melnkalne. Vismaz šajos apstākļos personas apliecība tiek izmantota arī kā ceļošanas dokuments, tādējādi šī norma kalpo arī mērķim novērst nelegālo ieceļošanu no šīm valstīm. To varētu uzskatīt par Savienības atzītu vispārējo interešu mērķi (EST, spriedums, 2013. gada 17. oktobris, *Schwarz*, C-291/12, EU:C:2013:670, 38. punkts). Tomēr personas apliecības galvenais izmantošanas nolūks nav primāri būt par ceļošanas dokumentu Šengenas zonā, kāds ir pase. Šajā ziņā Regulas (ES) 2019/1157 apsvērumos atšķirībā no Regulas 2252/2004 apsvērumiem pamatoti nav norādīts uz Šengenas zonu kā brīvības telpu.
- 23 Regulā (ES) 2019/1157 nav arī reglamentēta saglabāto biometrisko datu izmantošana šādā izpratnē, proti, Regulas (ES) 2019/1157 11. panta 6. punktā ir noteikts, ka saglabātie biometriskie dati tiek izmantoti vienīgi tādēļ, lai pārbaudītu dokumenta autentiskumu vai tā turētāja identitāti. Tātad Regula (ES) 2019/1157 nesniedz atbildi uz jautājumu, kādā veidā ir iespējams sekmēt pārvietošanās brīvību. Šajā ziņā mērķis novērst nelegālu ieceļošanu nevar būt līdzvērtīgs brīvas pārvietošanās sekmēšanai.
- 24 Pat ja šajā regulējumā būtu izvirzīts vispārējo interešu mērķis, pastāv šaubas, vai Regulas (ES) 2019/1157 3. panta 5. punkts ir samērīgs. Tas tā būtu vienīgi tajā gadījumā, ja šie Hartā nostiprināto tiesību ierobežojumi ir samērīgi ar Regulas (ES) 2019/1157 mērķi un tātad ar mērķi novērst personu nelegālu ieceļošanu Savienības teritorijā un nodrošināt apliecības turētāja ticamu identifikāciju. Šajā ziņā ar šo regulu ieviestajiem pasākumiem ir jābūt piemērotiem šo mērķu īstenošanai, un tie nedrīkst pārsniegt to, kas ir vajadzīgs to sasniegšanai (EST, spriedums, 2013. gada 17. oktobris, *Schwarz*, C-291/12, EU:C:2013:670, 38. un 40. punkts).
- 25 Šādos apstākļos iesniedzējtiesa uzskata, ka ir jāņem vērā tas, ka personas apliecība nedz faktiskā, nedz juridiskā ziņā nevar tikt pielīdzināta pasei un ka pastāv ievērojamas atšķirības šo dokumentu izmantošanas ziņā. Un tomēr – Regulas (ES) 2019/1157 3. panta 5. punktā saistībā ar pirkstu nospiedumiem abi dokumenti ir atzīti par līdzvērtīgiem.
- 26 Kā jau iepriekš izklāstīts, personas apliecību gan var izmantot arī kā ceļošanas dokumentu. Tomēr personas apliecības no pasēm atšķiras gan juridiskā, gan arī praktiskā ziņā. Pat ja brīvas pārvietošanās kontekstā personas apliecības tiek izmantotas arī kā ceļošanas dokumenti, tomēr vismaz starp ES dalībvalstīm regulāras kontroles nenotiek. Turklāt vairākums Savienības pilsoņu valsts izsniegtās identifikācijas kartes primāro funkciju visticamāk nesaista ar

- pārvietošanās brīvību. Faktiski personas apliecību var izmantot arī citādos veidos. Piemēram, personas apliecības ikdienā citastarp tiek izmantotas saziņā ar valsts pārvaldes iestādēm vai ar trešām personām privāttiesību jomās, piemēram, ar bankām vai lidsabiedrībām. Savienības pilsoņi, kuri vēlas izmantot savas brīvās pārvietošanās tiesības, to var darīt jau ar savu pasi (šajā ziņā skat. arī Eiropas datu aizsardzības uzraudzītāja 2018. gada 10. augusta atzinumu par plāniem pirkstu nospiedumu saglabāt personas apliecībās).
- 27 Turklāt Vācijā pastāv pienākums turēt personas apliecību (*PAuswG* 1. panta 1. punkta pirmais teikums). Pretēji tam, kā tas ir gadījumā ar pasi, pilsonis nevar pats izlemt, vai viņš iesniegs pieteikumu personas apliecības saņemšanai. Arī Eiropas datu aizsardzības uzraudzītājs uzskata, ka pirkstu nospiedumu noņemšanai un to saglabāšanai būtu tālejoša ietekme uz līdz pat 370 miljoniem ES pilsoņu, jo 85 % ES pilsoņu obligātā kārtā būtu jānoņem pirkstu nospiedumi. No šīs plašās izmantojuma jomas, kā arī īpaši sensitīvajiem datiem, kas tiek apstrādāti (sejas attēli apvienojumā ar pirkstu nospiedumiem), izriet, ka ir nepieciešama padziļināta izpēte, kas balstīta uz stingru nepieciešamības pārbaudi. Iesniedzējtiesa piekrīt Eiropas datu aizsardzības uzraudzītāja apsvērumam, ka, ņemot vērā atšķirības starp personas apliecībām un pasēm, tādu drošības elementu ieviešanu, kuri, iespējams, ir uzskatāmi par samērīgiem pasu gadījumā, nedrīkst automātiski attiecināt uz personas apliecībām, un turklāt ir nepieciešams to apsvērt un padziļināti izvērtēt. Aplūkojamajā gadījumā tas nav noticis.
- 28 Tiesa uzskata, ka iepriekš aprakstītās plašās izmantošanas iespējas apvienojumā ar to Savienības pilsoņu lielo skaitu, kuri ir datu subjekti, izraisa daudz intensīvāku iejaukšanos, nekā tā ir pasu gadījumā, kurai savukārt ir nepieciešams spēcīgāks attaisnojums.
- 29 Interpretējot Hartas 7. un 8. pantu, ir jāņem vērā arī VDAR vērtējumi, kas konstatējami tās 1. un 2. apsvērumā.
- 30 Saskaņā ar VDAR 9. panta 1. punktu daktiloskopijas dati ir īpašs personas datu veids, proti, biometriskie dati. Tie VDAR 4. panta 14. punktā ir definēti kā personas dati pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, kas ļauj veikt vai apstiprina minētās fiziskās personas unikālu identifikāciju, piemēram, sejas attēli vai daktiloskopijas dati. Saskaņā ar VDAR 9. panta 1. punktu šādu biometrisku datu apstrāde principā ir aizliegta, un tā ir pieļaujama vienīgi šauri interpretējamos izņēmuma gadījumos.
- 31 Tā kā personas apliecībā ir jāiekļauj pirkstu nospiedumi, lai sekmēt aizsardzību pret viltošanu, Eiropas datu aizsardzības uzraudzītāja atzinumā par plāniem pirkstu nospiedumus saglabāt personas apliecībās ir norādīts uz to, ka laikposmā no 2013. līdz 2017. gadam ir konstatēti tikai 38 870 identifikācijas karšu viltojumi, un viltotu identifikācijas karšu izmantošana jau vairākus gadus pēc kārtas samazinās.

- 32 Nav pietiekoši skaidrs jau tas, vai pirkstu nospiedumu noņemšana patiešām veicina aizsardzību pret viltojumiem. Uz personas apliecības mikroshēmas saglabāto biometrisko datu atbilstība apliecības turētāja pirkstu nospiedumiem apliecina tikai to, ka dokuments pieder tā turētājam. Kamēr nav konstatēts pašas personas apliecības autentiskums, no šīs atbilstības pašas par sevi vēl neizriet identitātes apliecinājums. Ir gan atzīts, ka biometrisko datu izmantošana samazina iespējas sekmīgi viltot dokumentu, un tāvad pirkstu nospiedumu saglabāšana vismaz daļēji var sekmēt mērķa sasniegšanu.
- 33 Tomēr ir ļoti apšaubāms, vai šī iespēja var attaisnot šādu ievērojamu iejaukšanos, it īpaši tādēļ, ka saskaņā ar Vācijas tiesību aktiem personas apliecība arī ar bojātu mikroshēmu joprojām ir derīga, kas ir pretrunā Regulai (ES) 2019/1157. Šajā ziņā *Bundesamt für Sicherheit in der Informationstechnik* [Federālais Informācijas tehnoloģiju drošības birojs] norāda, ka “apliecība ar nelietojamu mikroshēmu vēl joprojām ir derīga, pat ja tajā integrētā mikroshēma ir acīmredzami bojāta. Kā identitāti apliecinošs dokuments tas ir drošs, pateicoties fiziskajiem drošības elementiem”. Tomēr, ja drošību var panākt, izmantojot tikai fiziskos drošības elementus (it īpaši mikroiespiedumus, UV uzdrukas utt.), acīmredzami rodas jautājums par pirkstu nospiedumu noņemšanas nepieciešamību.
- 34 Arī Eiropas datu aizsardzības uzraudzītājs uzsver, ka drošības elementi, kas saistīti ar dokumenta drukāšanu, piemēram, hologrammu vai ūdenszīmju izmantošana, ir iemesls ievērojami zemākai iejaukšanās pakāpei. Šīs metodes neietverot personas datu apstrādi, tomēr ar tām esot iespējams arī novērst identitātes dokumentu viltošanu un pārbaudīt dokumenta autentiskumu.
- 35 Šajā kontekstā ir jāievēro viens no svarīgākajiem Eiropas datu aizsardzības tiesību principiem – datu minimizēšanas jeb datu apjoma samazināšanas princips. Saskaņā ar to personas datu iegūšanai un izmantošanai ir jābūt samērīgai un nepieciešamai, un tai ir jāietver tikai tas, kas nepieciešams to apstrādei.
- 36 Ja būtu nepieciešams noņemt pirkstu nospiedumus, rastos arī jautājums, kādēļ ir nepieciešama pilnāpjoma pirkstu nospieduma kopija. Tādā veidā gan tiek veicināta to dažādo sistēmu sadarbība, kas var atpazīt pirkstu nospiedumus. Šīs sistēmas var iedalīt trīs apakškategoriās. Pirmkārt, pastāv sistēmas, kas saglabā un salīdzina pilnāpjoma pirkstu nospiedumu kopijas. Citas sistēmas izmanto nospiedumu elementus (tā dēvētos *minutiae*). Šie nospiedumu elementi apraksta daļu no raksturlielumiem, kurus var iegūt no pirkstu nospiedumu kopijām. Trešajā kategorijā ietilpst sistēmas, kas darbojas ar atsevišķiem paraugiem, kurus ekstrahē no pirkstu nospiedumu kopijām. Ja būtu saglabāts tikai viens nospieduma elements, dalībvalsts, kura strādā ar sistēmu, kurā izmantoti pilnāpjoma pirkstu nospiedumi, nevarētu to izmantot. Pilnāpjoma pirkstu nospiedumu saglabāšana veicina sadarbību, tomēr tā palielina saglabāto personas datu apjomu un līdz ar to arī identitātes zādžības risku gadījumā, ja notiek datu noplūde.
- 37 Personas apliecībās izmantotās RFID mikroshēmas dažkārt ir iespējams nolasīt arī ar neautorizētu skenēšanas ierīču palīdzību. Iemesls ir tas, ka tās tiek aktivizētas ar

radiosignālu palīdzību, bet pēc tam dati tiek nosūtīti šifrētā veidā. Tātad procesa drošība galu galā ir atkarīga no datu pārnese un kodēšanas tehnoloģijas kvalitātes. Šajā kontekstā tieši pilnāpoma pirkstu nospiedumu izmantošana visvairāk palielina risku.

- 38 Ņemot vērā visu iepriekš izklāstīto, ir jāievēro arī tas, ka saistībā ar pirkstu nospiedumiem runa ir par biometriskajiem datiem. Likumdevējs līdz ar VDAR 9. panta pieņemšanu ir apliecinājis, ka uz tiem attiecas īpaša aizsardzība.
- 39 Pat Regulā (ES) 2019/1157 ir paredzēts, ka pirkstu nospiedums kā “drošības elements” neattiecas uz bērniem, kas jaunāki par 12 gadiem, un bērni, kas jaunāki par 6gadiem, ir pilnīgi atbrīvoti no prasības noņemt pirkstu nospiedumus (Regulas (ES) 2019/1157 3. panta 7. punkts). Tomēr daudz svarīgāk ir tas, ka personas, kurām fiziski nav iespējams noņemt pirkstu nospiedumus, ir atbrīvotas no prasības noņemt pirkstu nospiedumus. Tas, kādam citam nolūkam tad kalpotu šis drošības elements, Regulā (ES) 2019/1157 nav reglamentēts; šis jautājums gluži vienkārši ir palicis atvērts.
- 40 Turklāt Eiropas datu aizsardzības uzraudzītājs savā atzinumā uzsver, ka VDAR 35. panta 10. punkts ir piemērojams attiecībā uz pirkstu nospiedumu iegūšanu un apstrādi. Saskaņā ar VDAR 35. panta 1. punktu pirms apstrādes, kura varētu radīt augstu risku fizisku personu tiesībām un brīvībām, ir jāveic novērtējums par ietekmi uz datu aizsardzību. Veicot šo novērtējumu par ietekmi uz datu aizsardzību, īpašs uzsvars ir jāliek uz risku izvērtēšanu saistībā ar datu subjektu tiesībām un brīvībām, kā arī uz pasākumiem, kas veicami šo risku novēršanai, tostarp garantijām un drošības pasākumiem.
- 41 Ņemot vērā, ka tiesiskais pamats ir Savienības tiesību akti, kuras piemērojamas attiecībā uz pārzini, un šie tiesību akti reglamentē konkrēto apstrādes darbību, vispārējais novērtējums par ietekmi uz datu aizsardzību ir jāveic kopā ar minētā tiesiskā pamata pieņemšanu (VDAR 35. panta 10. punkts). Tādējādi šāds novērtējums par ietekmi uz datu aizsardzību būtu bijis jāveic kopā ar Regulas (ES) 2019/1157 pieņemšanu. Kā liecina šīs regulas apsvērumi, šāds novērtējums netika sagatavots.
- 42 Līdzīgi tam, kā Eiropas datu aizsardzības uzraudzītājs norādījis savā atzinumā, iesniedzējtiesa uzskata, ka novērtējums par ietekmi uz datu aizsardzību nepieļautu, ka personas apliecībā būtu obligāti jāiekļauj gan sejas attēls, gan arī (divu) pirkstu nospiedumi. Jau likumdošanas procesā Eiropas datu aizsardzības uzraudzītājs rekomendēja šajā kontekstā no jauna izvērtēt biometrisko datu (sejas attēls apvienojumā ar pirkstu nospiedumiem) apstrādes nepieciešamību un samērīgumu.
- 43 Likumdevējs 40. apsvērumā šo problēmu loku saistībā ar VDAR iezīmē tikai ļoti vispārīgi. Tas ir iekļāvis tikai vispārīgas frāzes, piemēram, ka Savienības pilsoņi būtu jāinformē par datu nesēju un ka būtu nepieciešams tuvāk precizēt, kādas garantijas ir spēkā attiecībā uz apstrādātajiem personu datiem, kā arī it īpaši uz

sensitīviem datiem, tādiem kā biometriskie identifikatori. Datu nesējam vajadzētu būt īpaši drošam un efektīvi aizsargāt tajā glabātos personas datus pret nesankcionētu piekļuvi. Nav konkretizēts, kas ir jāsaprot ar terminu “īpaši drošs”, un kādām būtu jābūt garantijām un drošības pasākumiem. Turklāt nav veikts risku novērtējums mikroshēmas datu noplūdes gadījumā un nav izvērtēta iejaukšanās Hartas 7. un 8. pantā nostiprinātajās tiesībās.

- 44 Tādēļ rodas jautājums, vai, ņemot vērā, ka likumdevējs nav sagatavojis obligāto novērtējumu par ietekmi uz datu aizsardzību, tiesību norma var palikt spēkā, vai tomēr, ja jau likumdevējam obligāti ir jāveic novērtējums par ietekmi uz datu aizsardzību, bet tas to nav darījis, tiesību norma visdrīzāk zaudē spēku. Pretējā gadījumā likumdevējs tiktu atalgots par sava pienākuma neizpildi.