Mnenje št. 15/2020 o osnutku sklepa pristojnih nadzornih organov Nemčije glede odobritve zahtev za akreditacijo certifikacijskega organa v skladu s členom 43.3 (Splošna uredba o varstvu podatkov)

Sprejeto 25. maja 2020

Sprejeto

Kazalo

Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 63, člena 64(1c) in (3)–(8) ter člena 43(3) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba o varstvu podatkov),

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu EGP, kakor sta bila spremenjena s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018, [1]

ob upoštevanju členov 10 in 22 svojega poslovnika z dne 25. maja 2018,

ob upoštevanju naslednjega:

(1) Glavna vloga Evropskega odbora za varstvo podatkov je zagotavljati dosledno uporabo Uredbe (EU) 2016/679 (v nadaljevanju: Splošna uredba o varstvu podatkov) v celotnem Evropskem gospodarskem prostoru. V skladu s členom 64(1) Splošne uredbe o varstvu podatkov odbor izda mnenje, kadar namerava nadzorni organ odobriti zahteve za akreditacijo teles za certificiranje v skladu s členom 43. Cilj tega mnenja je zato zagotoviti usklajen pristop glede zahtev, ki jih bo nadzorni organ za varstvo podatkov ali nacionalni akreditacijski organ uporabljal pri akreditaciji telesa za certificiranje. Splošna uredba o varstvu podatkov sicer neposredno ne uvaja enotnega sklopa zahtev za akreditacijo, spodbuja pa doslednost. Odbor si v svojih mnenjih ta cilj prizadeva doseči, prvič, s spodbujanjem nadzornih organov, naj pripravijo osnutek svojih zahtev za akreditacijo ob upoštevanju strukture iz Priloge 1 k smernicam odbora št. 4/2018 o akreditaciji teles za certificiranje, in, drugič, z analiziranjem takih zahtev na podlagi predloge odbora, ki omogoča primerjalno analizo zahtev (v skladu z ISO 17065 in smernicami odbora o akreditaciji teles za certificiranje).

(2) V skladu s členom 43 Splošne uredbe o varstvu podatkov pristojni nadzorni organi sprejmejo zahteve za akreditacijo. Vendar uporabijo mehanizem za skladnost, da omogočijo vzpostavitev zaupanja v mehanizem certificiranja, zlasti z določitvijo visoke ravni zahtev.

(3) Čeprav se za zahteve za akreditacijo uporablja mehanizem za skladnost, to ne pomeni, da bi morale biti zahteve enake. Pristojni nadzorni organi imajo polje proste presoje glede nacionalnih ali regionalnih okoliščin, pri čemer morajo upoštevati svojo lokalno zakonodajo. Cilj mnenja Evropskega odbora za varstvo podatkov ni doseči enoten sklop zahtev EU, temveč preprečiti pomembna neskladja, ki bi lahko vplivala na primer na zaupanje v neodvisnost ali strokovno znanje akreditiranih teles za certificiranje.

(4) „Smernice št. 4/2018 o akreditaciji teles za certificiranje na podlagi člena 43 Splošne uredbe o varstvu podatkov (2016/679)“ (v nadaljevanju: smernice) in „Smernice št. 1/2018 o certificiranju in opredelitvi meril za certificiranje v skladu s členoma 42 in 43 Uredbe 2016/679“ se bodo uporabljale kot rdeča nit v okviru mehanizma za skladnost.

(5) Če država članica določi, da mora telesa za certificiranje akreditirati nadzorni organ, mora ta opredeliti zahteve za akreditacijo, ki med drugim vključujejo zahteve iz člena 43(2) Splošne uredbe o varstvu podatkov. V primerjavi z obveznostmi za akreditacijo teles za certificiranje pri nacionalnih

[1] Sklicevanje na „Unijo“ v tem mnenju je treba razumeti kot sklicevanje na „EGP“.

akreditacijskih organih člen 43 Splošne uredbe o varstvu podatkov daje manj navodil o zahtevah za akreditacijo, kadar nadzorni organ sam izvaja akreditacijo. Kot prispevek k usklajenemu pristopu k akreditaciji bi morala biti merila zanjo, ki jih uporablja nadzorni organ, urejena s standardom ISO/IEC 17065 in bi jih bilo treba dopolniti z dodatnimi zahtevami, ki jih določi nadzorni organ v skladu s členom 43(1)(b) Splošne uredbe o varstvu podatkov. Evropski odbor za varstvo podatkov poudarja, da določbe v členu 43(2)(a) do (e) odražajo in določajo zahteve iz standarda ISO 17065, kar bo pripomoglo k dosledni uporabi.[2]

(6) V skladu s členom 64(1)(c), (3) in (8) Splošne uredbe o varstvu podatkov v povezavi s členom 10(2) svojega poslovnika Evropski odbor za varstvo podatkov sprejme mnenje v osmih tednih od prvega delovnega dne po sprejetju sklepa predsednika in pristojnega nadzornega organa, da je dokumentacija popolna. Predsednik lahko odloči, da se to obdobje lahko glede na kompleksnost vsebine podaljša za šest tednov –

SPREJEL MNENJE:

1 POVZETEK DEJSTEV

1. Nemški zvezni in deželni nadzorni organi (v nadaljnjem besedilu: nemški nadzorni organi) so Evropskemu odboru za varstvo podatkov predložili osnutek zahtev za akreditacijo v skladu s členom 43(1)(b). Dokumentacija je bila 13. februarja 2020 ocenjena kot popolna. Nemški nacionalni akreditacijski organ (DAkkS) bo telesa za certificiranje akreditiral na podlagi meril za certificiranje iz Splošne uredbe o varstvu podatkov. To pomeni, da bo nacionalni akreditacijski organ za akreditacijo teles za certificiranje uporabil standard ISO 17065 in dodatne zahteve, ki so jih določili nemški nadzorni organi, in sicer po tem, ko bo nadzorni organ te zahteve odobril na podlagi mnenja odbora o osnutku zahtev.

2. V skladu s členom 10(2) poslovnika odbora je predsednica zaradi kompleksnosti obravnavane zadeve sprejela odločitev o podaljšanju prvotnega osemtedenskega obdobja za sprejetje za dodatnih šest tednov.

2 OCENA

2.1 Splošna obrazložitev Evropskega odbora za varstvo podatkov glede predloženega osnutka sklepa

3. Namen tega mnenja je oceniti zahteve za akreditacijo, ki jih je določil nadzorni organ, bodisi glede standarda ISO 17065 bodisi celotnega sklopa zahtev, da se nacionalnemu akreditacijskemu organu ali nadzornemu organu, kot določa člen 43(1) Splošne uredbe o varstvu podatkov, omogoči akreditacija telesa za certificiranje, odgovornega za izdajo in podaljšanje certifikata v skladu s členom 42 Splošne uredbe o varstvu podatkov. To ne posega v naloge in pristojnosti pristojnega nadzornega organa. V

[2] Smernice 4/2018 o akreditaciji certifikacijskih organov na podlagi člena 43 Splošne uredbe o varstvu podatkov, točka 39. Na voljo na spletnem naslovu: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_sl

tem primeru odbor ugotavlja, da so se nemški nadzorni organi odločili, da se za izdajo akreditacije pridružijo akreditaciji svojega nacionalnega akreditacijskega organa, saj je ta v skladu s smernicami pripravil dodatne zahteve, ki jih mora nacionalni akreditacijski organ uporabiti pri izdaji akreditacije.

4. Namen te ocene dodatnih zahtev nemških nadzornih organov za akreditacijo je proučiti spremembe (dopolnitve ali črtanja) smernic in zlasti njihove Priloge 1. Poleg tega je mnenje Evropskega odbora za varstvo podatkov osredotočeno tudi na vse vidike, ki lahko vplivajo na dosleden pristop v zvezi z akreditacijo teles za certificiranje.

5. Opozoriti je treba, da je cilj smernic o akreditaciji teles za certificiranje pomagati nadzornim organom pri opredelitvi njihovih zahtev za akreditacijo. Priloga k smernicam ne pomeni zahtev za akreditacijo kot takih. Nadzorni organi morajo zato zahteve za akreditacijo teles za certificiranje opredeliti tako, da omogočijo njihovo praktično in dosledno uporabo, kot se zahteva v skladu z njihovimi okoliščinami.

6. Odbor priznava dejstvo, da bi bilo treba nacionalnim akreditacijskim organom in pristojnim nadzornim organom glede na njihovo strokovno znanje zagotoviti manevrski prostor pri opredelitvi nekaterih posebnih določb v okviru veljavnih zahtev za akreditacijo. Vendar pa je treba po mnenju odbora poudariti, da je treba v primeru določitve dodatnih zahtev te opredeliti na način, ki omogoča njihovo praktično in dosledno uporabo ter pregled, če je to potrebno.

7. Odbor ugotavlja, da standarde ISO, zlasti standard ISO 17065, ščitijo pravice intelektualne lastnine, zato se v tem mnenju ne bo skliceval na besedilo zadevnega dokumenta. Zato se je odbor odločil, da po potrebi vključi napotila na posamezne oddelke standarda ISO, ne da bi pri tem navajal dejansko besedilo standarda.

8. Nazadnje je odbor izvedel svojo oceno v skladu z zgradbo, predvideno v Prilogi 1 k smernicam (v nadaljevanju: Priloga). Če posamezen oddelek osnutka zahtev nemških nadzornih organov za akreditacijo v tem mnenju ni omenjen, se šteje, da odbor nima nobenih pripomb, in ne zahteva, da nemški nadzorni organi sprejmejo nadaljnje ukrepe.

9. V tem mnenju niso zajeti elementi, ki so jih posredovali nemški nadzorni organi in ne spadajo na področje uporabe člena 43(2) Splošne uredbe o varstvu podatkov, kot so na primer sklicevanja na nacionalno zakonodajo. Ne glede na to pa odbor poudarja, da mora biti nacionalna zakonodaja v skladu s Splošno uredbo o varstvu podatkov, kadar se to zahteva.

2.2 Glavne točke za oceno (člen 43(2) Splošne uredbe o varstvu podatkov in Priloga 1 k smernicam Evropskega odbora za varstvo podatkov), da zahteve za akreditacijo dosledno ocenjujejo naslednje:

1) obravnavo vseh ključnih področij, kot je poudarjeno v prilogi k smernicam, in upoštevanje vseh odstopanj od priloge;

2) neodvisnost telesa za certificiranje;

3) navzkrižja interesov telesa za certificiranje;

4) strokovno znanje telesa za certificiranje;

5) ustrezne zaščitne ukrepe za zagotovitev, da telo za certificiranje ustrezno uporabi merila za certificiranje iz Splošne uredbe o varstvu podatkov;

6) postopke za izdajo, redni pregled in preklic certificiranja v skladu s Splošno uredbo o varstvu podatkov in

7) pregledno obravnavo pritožb zaradi kršitev, povezanih s certificiranjem.

10. Ob upoštevanju, da:

a. člen 43(2) Splošne uredbe o varstvu podatkov določa seznam področij akreditacij, ki jih mora telo za certificiranje obravnavati, če želi pridobiti akreditacijo;

b. člen 43(3) Splošne uredbe o varstvu podatkov določa, da zahteve za akreditacijo teles za certificiranje odobri pristojni nadzorni organ;

c. člen 57(1)(p) in (q) Splošne uredbe o varstvu podatkov določa, da mora pristojni nadzorni organ pripraviti osnutek zahtev in objaviti zahteve za akreditacijo za telesa za certificiranje ter da se lahko odloči, da sam izvede postopek akreditacije telesa za certificiranje;

d. člen 64(1)(c) Splošne uredbe o varstvu podatkov določa, da odbor izda mnenje, kadar nadzorni organ namerava odobriti zahteve za akreditacijo za telesa za certificiranje v skladu s členom 43(3);

e. če postopek akreditacije izvaja nacionalni akreditacijski organ v skladu s standardom ISO/IEC 17065/2012, je treba uporabiti tudi dodatne zahteve, ki jih določi pristojni nadzorni organ;

f. so v Prilogi 1 k smernicam o akreditaciji teles za certificiranje predlagane zahteve, katerih osnutek pripravi nadzorni organ za varstvo podatkov in ki se uporabljajo pri akreditaciji telesa za certificiranje pri nacionalnem akreditacijskem organu,

odbor podaja naslednje mnenje:

2.2.1 UVOD

11. Odbor priznava dejstvo, da pogoji sodelovanja, ki urejajo odnos med nacionalnim akreditacijskim organom in njegovim nadzornim organom za varstvo podatkov, sami po sebi niso zahteva za akreditacijo teles za certificiranje. Vendar odbor zaradi popolnosti in preglednosti meni, da je treba take pogoje sodelovanja, če obstajajo, javno objaviti v obliki, ki je po mnenju nadzornega organa primerna.

2.2.2 IZRAZI IN OPREDELITVE POJMOV

12. Odbor ugotavlja, da poglavje 3 („Opredelitve“) osnutka zahtev nemških nadzornih organov za akreditacijo opredeljuje, katere vrste certifikacijskih shem so dovoljene, pri čemer določa, da morajo izpolnjevati zahteve standarda DIN EN/IEC 17065. Glede tega je treba poudariti, da je v poglavjih 5.1 in 5.2 Smernic Evropskega odbora za varstvo podatkov že navedeno, kaj se lahko v celoti certificira na podlagi Splošne uredbe o varstvu podatkov. Zato odbor priznava, da namen nemških nadzornih organov ni omejiti, kar je navedeno v smernicah, in da je treba trditve, vsebovane v poglavju 3 osnutka zahtev nemških nadzornih organov za akreditacijo, šteti za veljavne v okviru teh zahtev za akreditacijo.

2.2.3 SPLOŠNE OPOMBE

13. Odbor ugotavlja, da se oddelek „s splošnimi pripombami“ osnutka zahtev nemških nadzornih organov za akreditacijo sklicuje na „odobritev“ meril Evropskega odbora za varstvo podatkov za certificiranje „v skladu s čl. 63 in 64(1)(c) Splošne uredbe o varstvu podatkov“. Odbor ugotavlja, da mu Splošna uredba o varstvu podatkov ne daje pristojnosti za „odobritev“ meril za certificiranje. Vendar lahko v skladu z zgoraj navedenimi členi merila za certificiranje potrdi. Zato priporoča, naj nemški nadzorni organi izbrišejo sklicevanje na „odobritev Evropskega odbora za varstvo podatkov“, da bodo osnutek uskladili z besedilom Splošne uredbe o varstvu podatkov.

2.2.4 SPLOŠNE ZAHTEVE ZA AKREDITACIJO (poglavje 4 osnutka zahtev za akreditacijo)

14. Glede zahteve o pravni odgovornosti (oddelek 4.1 osnutka zahtev nemških nadzornih organov za akreditacijo) Evropski odbor za varstvo podatkov ugotavlja, da nemški nadzorni organi v dokazilih pojasnjujejo, da se od telesa za certificiranje pričakuje, da bo moral postopke posodobiti, in zato nadaljnje zahteve glede tega niso potrebne. Vendar odbor meni, da pričakovanje teles za certificiranje k takim postopkom ne zavezuje. Kot je določeno v oddelku 4.1.1 priloge k smernicam, morajo telesa za certificiranje posodobiti postopke, ki dokazujejo skladnost s pravnimi odgovornostmi, določenimi v pogojih akreditacije. Poleg tega mora biti telo za certificiranje sposobno dokazati skladnost svojih postopkov in ukrepov s Splošno uredbo o varstvu podatkov, zlasti za nadzor in upravljanje organizacije osebnih podatkov stranke v okviru certifikacijskega procesa. Zato Evropski odbor za varstvo podatkov nemškim nadzornim organom priporoča, naj spremenijo osnutek zahtev, da jih uskladijo s smernicami.

15. Pri pododdelku 4.1.2.2 osnutka zahtev nemških nadzornih organov za akreditacijo („sporazum o certificiranju“) odbor ugotavlja, da osnutek zahtev nemških nadzornih organov za akreditacijo ne vključuje obveznosti, ki bi pristojnemu nadzornemu organu omogočale popolno preglednost postopka certificiranja, vključno s pogodbeno zaupnimi zadevami. Poleg tega ni sklicevanja na obveznost vložnika, da telesu za certificiranje zagotovi dostop do svojih dejavnosti obdelave. Zato odbor nemškim nadzornim organom priporoča, naj v svoj osnutek vključijo zgoraj navedene obveznosti.

16. Evropski odbor za varstvo podatkov ugotavlja, da izrecno sklicevanje na naloge in pooblastila pristojnega nadzornega organa (tretja alineja oddelka 4.1.2 priloge) ni vključeno v pododdelek 4.1.2.2 osnutka zahtev nemških nadzornih organov za akreditacijo. Obor meni, da bi se moralo to sklicevanje dodati v osnutek zahtev, in zato nemškim nadzornim organom priporoča, naj osnutek ustrezno spremenijo.

17. Poleg tega osnutek zahtev nemških nadzornih organov glede sporazuma o certificiranju ne vključuje obveznosti telesa za certificiranje, da razkrije vse informacije, potrebne za dodelitev certifikata, v skladu s členoma 42(8) in 43(5) Splošne uredbe o varstvu podatkov (7. alineja oddelka 4.1.2 priloge). Čeprav je ta obveznost vključena v oddelek vodenje poslovnih procesov osnutka zahtev nemških nadzornih organov za akreditacijo, Evropski odbor za varstvo podatkov meni, da bi morala biti del sporazuma o certificiranju, da bi okrepila njegovo zavezujočnost. Odbor torej nemškim nadzornim organom priporoča, naj vključijo zgoraj navedene obveznosti kot del elementov sporazuma o certificiranju.

18. V skladu s prilogo mora vložnik obvestiti telo za certificiranje o znatnih spremembah svojega dejanskega ali pravnega položaja ter spremembah svojih proizvodov, procesov in storitev, ki jih zadeva certificiranje (10. alineja oddelka 4.1.2 priloge). Alineja 6 pododdelka 4.1.2.2 osnutka zahtev nemških nadzornih organov za akreditacijo sicer vključuje obveznost, da se telo za certificiranje obvesti o

znatnih spremembah dejanskih ali pravnih okoliščin, vendar izrecno ne navaja proizvodov, procesov in storitev. Evropski odbor za varstvo podatkov nemškim nadzornim organom priporoča, naj tako sklicevanje vključijo v skladu s prilogo.

19. Glede pododdelka 4.2.7 osnutka zahtev nemških nadzornih organov za akreditacijo („upravljanje nepristranskosti“) Evropski odbor za varstvo podatkov priporoča, naj se okrepijo merila, ki veljajo za telesa za certificiranje, ki spadajo v ločen pravni subjekt ali jih ta nadzoruje, ter se upošteva, da lahko vsaka oblika gospodarskega odnosa med telesom za certificiranje in pravnim subjektom, odvisno od njegovih lastnosti, vpliva na nepristranskost certifikacijske dejavnosti.

20. Glede oddelka 4.6 osnutka zahtev nemških nadzornih organov za akreditacijo („javno dostopne informacije“) Evropski odbor za varstvo podatkov ugotavlja, da ni nobenega sklicevanja na objavo vseh različic odobrenih meril in vseh postopkov za certificiranje. Zato odbor nemške nadzorne organe spodbuja k spremembi osnutka zahtev za akreditacijo, da bi bilo jasno, da objava vključuje vse različice odobrenih meril in postopkov za certificiranje. Poleg tega odbor ugotavlja, da je v drugem odstavku oddelka 4.6 navedeno, da morajo biti „certifikacijske sheme, ki jih uporablja telo za certificiranje, merila, odobrena v skladu s čl. 42(5) Splošne uredbe o varstvu podatkov, ki navajajo odobreno trajanje uporabe, *javno objavljene*“. Da bi se odbor izognil nejasnosti, nemške nadzorne organe spodbuja, naj črtajo besedo „javno“ ter med „telo za certificiranje“ in „merila, odobrena“ dodajo veznik „in“.

2.2.5 ZAHTEVE GLEDE VIROV (oddelek 6 osnutka zahtev za akreditacijo)

21. Glede zahtev o strokovnem znanju in zlasti pododdelka 6.1.2.1 osnutka zahtev nemških nadzornih organov za akreditacijo („pristojnost za človeške vire“) Evropski odbor za varstvo podatkov ugotavlja, da zahtevano znanje na naštetih področjih ne določa, da mora biti znanje relevantno in ustrezno. Da bi zagotovili skladnost z ravnjo znanja, ki se zahteva v prilogi, odbor nemškim nadzornim organom priporoča, naj uskladijo besedilo s smernicami ter zahtevajo, da je znanje relevantno in ustrezno.

22. Poleg tega Evropski odbor za varstvo podatkov ugotavlja, da zahteve za osebje s tehničnim znanjem, odgovorno za sprejemanje odločitev, vključujejo vsaj sedem let strokovnih izkušenj ali pet let strokovnih izkušenj na področju tehničnega varstva podatkov, odvisno od njihove stopnje izobrazbe, osebje, odgovorno za vrednotenje, pa bi moralo imeti štiri leta strokovnih izkušenj ali dve leti strokovnih izkušenj na področju tehničnega varstva podatkov ter izkušnje na področju postopkov testiranja, odvisno od njihove stopnje izobrazbe. Podobno mora osebje s pravnim znanjem, odgovorno za sprejemanje odločitev, imeti vsaj pet let strokovnih izkušenj na področju prava varstva podatkov, osebje, odgovorno za vrednotenje, pa mora imeti vsaj dve leti izkušenj na področju prava varstva podatkov in revizijskih postopkov. Odbor ugotavlja, da se zahtevano najmanjše število let strokovnih izkušenj med osebjem, odgovornim za odločanje, in osebjem, odgovornim za vrednotenje, močno razlikuje. Glede tega meni, da bi bilo treba zahteve glede pristojnosti za ocenjevalce in nosilce odločanja prilagoditi glede na upoštevanje različnih nalog, ki jih opravljajo, ter ne glede na število let izkušenj. Nadalje meni, da bi morali ocenjevalci imeti specialistično strokovno znanje in strokovne izkušnje s področja tehničnih postopkov (na primer revizije in certificiranja), nosilci odločanja pa bi morali imeti splošnejše in celovitejše strokovno znanje ter strokovne izkušnje s področja prava varstva podatkov. Ob upoštevanju zgoraj navedenega odbor nemškim nadzornim organom svetuje, naj bolj poudarijo različno vsebinsko znanje in/ali izkušnje za ocenjevalce in nosilce odločanja ter zmanjšajo razlike v zahtevanih letih izkušenj zanje.

23. Poleg tega Evropski odbor za varstvo podatkov meni, da bi bilo treba poznavanje sistemov upravljanja, primernih za področje certificiranja, razširiti na standard ISO/IEC 27701:2019 – Varnostne tehnike – razširitev na standarda ISO/IEC 27001 in ISO/IEC 27002 za upravljanje informacij o zasebnosti – Zahteve in smernice ter nemške nadzorne organe spodbuja, naj vključijo tako sklicevanje.

24. Nazadnje, glede zahtev o izobrazbi tehničnega osebja Evropski odbor za varstvo podatkov meni, da je seznam predmetov že prilagojen tehničnemu znanju, ki se zahteva v prilogi. Zato odbor nemške nadzorne organe spodbuja, naj izbrišejo sklicevanje na „naravoslovne vede“ s seznama predmetov glede univerzitetne izobrazbe tehničnega osebja.

2.2.6 ZAHTEVE GLEDE POSTOPKOV (oddelek 7 osnutka zahtev za akreditacijo)

25. Evropski odbor za varstvo podatkov ugotavlja, da je v poglavju 7 osnutka zahtev nemških nadzornih organov za akreditacijo več sklicevanj na izraz „njegova merila“ (na primer v oddelkih 7.4, 7.6, 7.11 in 7.13). Da bi se izognili nejasnosti, odbor nemške nadzorne organe spodbuja, naj pojasnijo pomen tega izraza, na primer z dodano razlago v prilogi 1 (Glosar).

26. Glede oddelka 7.1 osnutka zahtev nemških nadzornih organov za akreditacijo („splošne informacije“) Evropski odbor za varstvo podatkov ugotavlja, da ni nobenega izrecnega sklicevanja na obveznost telesa za certificiranje, da mora izpolniti dodatne zahteve. Čeprav bi bilo o taki obveznosti mogoče sklepati iz besedila osnutka zahtev, odbor meni, da bi bilo treba vključiti izrecno sklicevanje na zgoraj navedeno obveznost. Zato nemškim nadzornim organom priporoča, naj osnutek ustrezno spremenijo.

27. Evropski odbor za varstvo podatkov ugotavlja, da osnutek dodatnih zahtev nemških nadzornih organov ne vsebuje nobenega sklicevanja na delovanje odobrenega evropskega pečata za varstvo podatkov v skladu z oddelkom 7.1.2 priloge. Odbor meni, da je treba to sklicevanje vključiti, zlasti glede na to, da se lahko akreditacija telesa za certificiranje, ki odobri evropski pečat za varstvo podatkov, izvede v vsaki državi članici, v kateri je telo za certificiranje ustanovljeno.[3] Zato nemškim nadzornim organom priporoča, naj vključijo zgoraj navedena sklicevanja. Na primer, v osnutku zahtev bi bilo lahko navedeno naslednje: *„Pristojni nadzorni organ bo obveščen, preden telo za certificiranje začne upravljati odobren evropski pečat za varstvo podatkov v novi državi članici iz podružnice.“*

28. Evropski odbor za varstvo podatkov ugotavlja, da je v oddelku 7.2 („vloga“) osnutka zahtev nemških nadzornih organov za akreditacijo predviden primer, v katerem se obdelovalci uporabijo za izvajanje dejanj obdelave osebnih podatkov v skladu s prilogo k smernicam. Vendar odbor opozarja, da mora vloga, kadar se uporabijo obdelovalci, vsebovati ustrezne kontaktne podatke upravljavcev/obdelovalcev, kot je navedeno v prilogi. Zato nemškim nadzornim organom priporoča, naj uskladijo besedilo smernic z vključitvijo sklicevanja na kontaktne podatke upravljavcev/obdelovalcev. Poleg tega nemške nadzorne organe spodbuja, naj premislijo, ali bi v tem primeru omenili tudi sklicevanje na skupne upravljavce in njihove posebne dogovore.

29. Evropski odbor za varstvo podatkov ugotavlja, da je v oddelku 7.2 osnutka zahtev nemških nadzornih organov za akreditacijo določeno, da „sta upravljavec in obdelovalec podatkov upravičena, da zaprosita za certifikacijo“. Možnost za obdelovalce, da zaprosijo za certifikacijo, bo odvisna od posebne certifikacijske sheme. Da bi se izognili zmedi, odbor torej nemške nadzorne organe spodbuja, naj

[3] V tem smislu glej smernice 1/2018, odstavek 44.

izbrišejo zgornje sklicevanje ali pojasnijo, da je možnost za obdelovalce, da bodo certificirani, odvisna od področja uporabe certifikacijske sheme.

30. Glede oddelka 7.3 osnutka zahtev nemških nadzornih organov („vloge za vrednotenje“) Evropski odbor za varstvo podatkov ugotavlja, da je v osnutku zahtev nemških nadzornih organov za akreditacijo navedeno, da „so načrtovane metode vrednotenja pogodbeno določene […]“. Da bi bilo jasno, da je to zahteva, odbor nemške nadzorne organe spodbuja, naj prvi odstavek preoblikujejo tako, da bo jasno, da metode vrednotenja bodo vključene v sporazum o certificiranju, skratka zahtevo preoblikuje v „načrtovane metode vrednotenja morajo biti pogodbeno določene […]“. Poleg tega nemške nadzorne organe spodbuja, naj nadomestijo sklicevanje na oddelek 7.3.1.b ISO 17065 z oddelkom 7.3 ISO 17065, da bi besedilo uskladili s prilogo. Odbor ugotavlja tudi, da se četrti odstavek nanaša na ustrezne tehnične in pravne pristojnosti. Zaradi jasnosti odbor nemške nadzorne organe spodbuja, naj dodajo „na področju varstva podatkov“.

31. Evropski odbor za varstvo podatkov ugotavlja, da oddelek 7.4 osnutka zahtev nemških nadzornih organov za akreditacijo („metode vrednotenja“) ne vključuje obveznosti telesa za certificiranje, da opiše zadostne metode vrednotenja za ocenjevanje skladnosti dejanj obdelave z merili za certificiranje. Odbor nemškim nadzornim organom priporoča, naj spremenijo osnutek zahtev in vključijo to sklicevanje. Dodali bi lahko na primer: *„Telo za certificiranje zagotovi, da se v mehanizmih, ki se uporabljajo za dodelitev certifikata, opišejo zadostne metode vrednotenja za ocenjevanje skladnosti dejanj obdelave z merili za certificiranje.*“ Glede prvega območja, ki ga je treba zajeti z metodami vrednotenja, odbor meni, naj se potrebnost in sorazmernost ocenita tudi glede na zadevne posameznike, na katere se nanašajo osebni podatki. Končno odbor ugotavlja, da ni sklicevanja na dokumentacijo o metodah in ugotovitvah. Zato nemškim nadzornim organom priporoča, naj spremenijo osnutek in izrecno vključijo taka sklicevanja.

32. Glede obstoječih certifikatov (oddelek 7.4 osnutka zahtev nemških nadzornih organov za akreditacijo) Evropski odbor za varstvo podatkov meni, da 4. alineja na strani 13 vodi v zmedo, ker ni jasno, kakšna je povezava med obdobji veljavnosti sedanjega in prejšnjega certificiranja ter kako se ujemata drug z drugim. Poleg tega se ne zdi izvedljivo, da bi se spraševali o veljavnosti predhodnega certifikata, ki ga je izdal drugi akreditirani certifikacijski organ. Skratka, odnosi med različnimi navedenimi elementi v odstavku bi lahko bili jasnejši. Odbor nemškim nadzornim organom priporoča, naj osnutek spremenijo zlasti s pojasnilom, da pogoj za trajanje veljavnosti certifikata po Splošni uredbi o varstvu podatkov ne sme biti veljavnost drugih vrst certifikatov.

33. Glede oddelka 7.5 („vrednotenje“) osnutka zahtev nemških nadzornih organov za akreditacijo Evropski odbor za varstvo podatkov nemške nadzorne organe spodbuja, naj spremenijo naslov oddelka v „pregled“.

34. Glede sprememb, ki vplivajo na certificiranje (oddelek 7.10 osnutka zahtev nemških nadzornih organov), Evropski odbor za varstvo podatkov ugotavlja, da je v osnutku zahtev nemških nadzornih organov za akreditacijo navedeno, da „je stranka pravočasno obveščena o spremembah pravnega okvira, ki vplivajo nanjo“. Ob upoštevanju potrebe po ohranitvi nepristranskosti telesa za certificiranje odbor nemške nadzorne organe spodbuja, naj poved preoblikujejo tako, da bo jasno, da so stranki pravočasno zagotovljene informacije o spremembah, ki bi lahko vplivale nanjo. Za zagotovitev jasnega razumevanja, kaj pomenijo „sklepi Evropskega odbora za varstvo podatkov“, odbor nemške nadzorne organe poziva, naj sklicevanje pojasnijo. Besedilo bi se lahko na primer glasilo: „dokumenti, ki jih sprejme Evropski odbor za varstvo podatkov“.

35. Evropski odbor za varstvo podatkov ugotavlja, da oddelek 7.11 osnutka zahtev nemških nadzornih organov („prekinitev, restrikcija, začasen odvzem ali preklic certifikata“) ne določa obveznosti telesa za certificiranje glede sprejetja odločitev in odredb nemških nadzornih organov o preklicu ali zavrnitvi izdaje certifikata vložniku, če zahteve glede certificiranja niso ali niso več izpolnjene. Zato odbor nemškim nadzornim organom priporoča, naj vključijo tako obveznost. Poleg tega nemške nadzorne organe spodbuja, naj besedo „restrikcija“ zamenjajo z besedo „omejitev“ iz naslova oddelka v skladu s prilogo k smernicam.

2.2.7 NADALJNJE DODATNE ZAHTEVE

36. Glede pododdelka 8.11.3 zahtev nemških nadzornih organov za akreditacijo („obravnavanje pritožb“) Evropski odbor za varstvo podatkov nemške nadzorne organe spodbuja, naj povečajo jasnost tako, da sklicevanje na „upravičene pritožbe“ nadomestijo z „utemeljene pritožbe“.

3 SKLEPI/PRIPOROČILA

37. Osnutek zahtev nemških zveznih in deželnih nadzornih organov za akreditacijo lahko vodi v nedosledno uporabo akreditacije teles za certificiranje, zato je treba uvesti naslednje spremembe:

38. Glede „splošnih pripomb“ Evropski odbor za varstvo podatkov nemškim nadzornim organom priporoča, naj:

    1) izbrišejo sklicevanje na „odobritev Evropskega odbora za varstvo podatkov“ in tako osnutek uskladijo z besedilom Splošne uredbe o varstvu podatkov.

39. Glede „splošnih zahtev za akreditacijo“ Evropski odbor za varstvo podatkov nemškim nadzornim organom priporoča, naj:

    1) spremenijo zahteve, ki se nanašajo na pravno odgovornost (pododdelek 4.1), da jih uskladijo s smernicami;

    2) spremenijo pododdelek 4.1.2.2 tako, da bo v sporazum o certificiranju vključena obveznost, da se nemškim nadzornim organom omogoči popolna preglednost glede postopka certificiranja in da se telesu za certificiranje zagotovi dostop do vložnikovih dejavnosti obdelave;

    3) vključijo v oddelek 4.1.2.2 izrecno sklicevanje na naloge in pooblastila pristojnega nadzornega organa v skladu s prilogo;

    4) vključijo med elemente sporazuma o certificiranju obveznost, da se telesu za certificiranje omogoči razkritje vseh informacij, potrebnih za dodelitev certifikata, v skladu s členoma 42(8) in 43(5) Splošne uredbe o varstvu podatkov;

    5) vključijo izrecno sklicevanje na „proizvode, procese in storitve, na katere se nanaša certificiranje“, v alinejo 6 pododdelka 4.1.2.2;

    6) v pododdelku 4.2.7 okrepijo merila, ki veljajo za telesa za certificiranje, ki spadajo v ločen pravni subjekt ali jih ta nadzoruje, ter upoštevajo, da lahko vsaka oblika

gospodarskega odnosa med telesom za certificiranje in pravnim subjektom, odvisno od njegovih lastnosti, vpliva na nepristranskost certifikacijske dejavnosti.

40. V zvezi z „zahtevami glede virov“ Evropski odbor za varstvo podatkov nemškim nadzornim organom priporoča, naj:

    1) uskladijo besedilo pododdelka 6.1.2.1 s smernicami tako, da zahtevajo, da je znanje relevantno in ustrezno.

41. V zvezi z „zahtevami glede postopkov“ Evropski odbor za varstvo podatkov nemškim nadzornim organom priporoča, naj:

    1) spremenijo oddelek 7.1 tako, da bo vseboval izrecno sklicevanje na obveznost telesa za certificiranje, da izpolni dodatne zahteve;

    2) vključijo sklicevanje na delovanje odobrenega evropskega pečata za varstvo podatkov;

    3) uskladijo besedilo oddelka 7.2 smernic z vključitvijo sklicevanja na kontaktne podatke upravljavcev/obdelovalcev;

    4) vključijo v oddelek 7.4 obveznost telesa za certificiranje, da opiše zadostne metode vrednotenja za ocenjevanje skladnosti dejanj obdelave z merili za certificiranje;

    5) pojasnijo v oddelku 7.4, da pogoj za trajanje veljavnosti certifikata po Splošni uredbi o varstvu podatkov ne sme biti veljavnost drugih vrst certifikatov;

    6) vključijo v oddelek 7.11 obveznost telesa za certificiranje glede sprejetja odločitev in odredb nemških nadzornih organov o preklicu ali zavrnitvi izdaje certifikata vložniku, če zahteve glede certificiranja niso ali niso več izpolnjene.

4 KONČNE PRIPOMBE

42. To mnenje se naslovi na nemške zvezne in deželne nadzorne organe ter se objavi v skladu s členom 64(5)(b) Splošne uredbe o varstvu podatkov.

43. V skladu s členom 64(7) in (8) Splošne uredbe o varstvu podatkov nemški nadzorni organi svojo odločitev o spremembi oziroma ohranitvi svojega osnutka sklepa sporočijo predsednici po elektronski poti v dveh tednih po prejemu mnenja. V istem času predložijo spremenjen osnutek sklepa; kjer ne nameravajo upoštevati mnenja Evropskega odbora za varstvo podatkov, pa zagotovijo ustrezno obrazložitev razlogov za neupoštevanje tega mnenja, bodisi v celoti ali le delno.

44. Nemški nadzorni organi v skladu s členom 70(1)(y) Splošne uredbe o varstvu podatkov svojo končno odločitev glede vprašanj, obravnavanih v okviru mehanizma za skladnost, sporočijo Evropskemu odboru za varstvo podatkov za vključitev v register odločitev.

Za Evropski odbor za varstvo podatkov

Predsednica

Sprejeto

(Andrea Jelinek)

Sprejeto