Mnenje 16/2020 o osnutku sklepa pristojnega nadzornega organa Češke republike o odobritvi zahtev za akreditacijo telesa za certificiranje 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(1)(c), (3) do (8) in 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 celotnem Evropskem gospodarskem prostoru. V skladu s členom 64(1) Splošne uredbe o varstvu podatkov Evropski odbor za varstvo podatkov izda mnenje, kadar namerava nadzorni organ odobriti zahteve za akreditacijo telesa 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. Evropski odbor za varstvo podatkov si v svojih mnenjih ta cilj prizadeva doseči, prvič, s spodbujanjem nadzornih organov, naj pripravijo osnutek svojih zahtev za akreditacijo ob upoštevanju zgradbe iz Priloge 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 s standardom 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.

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

(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 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)–(e) Splošne uredbe o varstvu podatkov 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) 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. Češki nadzorni organ je Evropskemu odboru za varstvo podatkov predložil osnutek zahtev za akreditacijo v skladu s členom 43(1)(b). Dokumentacija je bila 17. februarja 2020 ocenjena kot popolna. Češki nacionalni akreditacijski organ 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 jih je določil češki nadzorni organ, in sicer po tem, ko bo češki nadzorni organ te zahteve odobril na podlagi mnenja Evropskega odbora za varstvo podatkov o osnutku zahtev.

2. V skladu s členom 10(2) poslovnika Evropskega odbora za varstvo podatkov 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

[2] Smernice 4/2018 o akreditaciji teles za certificiranje 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

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 tem primeru Evropski odbor za varstvo podatkov ugotavlja, da se je češki nadzorni organ odločil, da se za izdajo akreditacije obrne na nacionalni akreditacijski organ, saj je v skladu s smernicami pripravil dodatne zahteve, ki jih mora nacionalni akreditacijski organ uporabiti pri izdaji akreditacije.

4. Namen te ocene dodatnih zahtev češkega nadzornega organa za akreditacijo je proučiti spremembe (dopolnitve ali črtanja) smernic in zlasti njihove Priloge 1. Poleg tega je mnenje Evropskega odbora za varstvo podatkov osredinjeno 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 organ mora zato zahteve za akreditacijo teles za certificiranje opredeliti tako, da omogoči njihovo praktično in dosledno uporabo, kot se zahteva v skladu z njegovimi okoliščinami.

6. Evropski odbor za varstvo podatkov priznava dejstvo, da bi bilo treba nacionalnim akreditacijskim 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 Evropskega odbora za varstvo podatkov 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. Evropski odbor za varstvo podatkov 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 odločil, da po potrebi vključi napotila na določene oddelke standarda ISO, ne da bi pri tem navajal dejansko besedilo standarda.

8. Nazadnje je Evropski odbor za varstvo podatkov izvedel svojo oceno v skladu z zgradbo, predvideno v Prilogi 1 k smernicam (v nadaljevanju: Priloga). Če posamezen oddelek osnutka zahtev češkega nadzornega organa za akreditacijo v tem mnenju ni omenjen, se šteje, da odbor nima nobenih pripomb in ne zahteva, da češki nadzorni organ sprejme nadaljnje ukrepe.

9. V tem mnenju niso zajeti elementi, ki jih je posredoval češki nadzorni organ in ne spadajo na področje uporabe člena 43(2) Splošne uredbe o varstvu podatkov, kot so na primer sklici na nacionalno zakonodajo. Ne glede na to pa Evropski odbor za varstvo podatkov 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 odbora), da zahteve za akreditacijo dosledno ocenjujejo naslednje:

a. obravnavo vseh ključnih področij, kot je poudarjeno v Prilogi k smernicam, in upoštevanje vseh odstopanj od Priloge;

b. neodvisnost telesa za certificiranje;

c. nasprotja interesov telesa za certificiranje;

d. strokovno znanje telesa za certificiranje;

e. ustrezne zaščitne ukrepe za zagotovitev, da telesa za certificiranje ustrezno uporabijo merila za certificiranje iz Splošne uredbe o varstvu podatkov;

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

g. 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 teles za certificiranje ter da se lahko odloči, da sam izvede postopek akreditacije teles 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 teles 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. Evropski odbor za varstvo podatkov priznava dejstvo, da pogoji sodelovanja, ki urejajo razmerje med nacionalnim akreditacijskim organom in njegovim nadzornim organom za varstvo podatkov, sami po sebi niso zahteva za akreditacijo teles za certificiranje. Vendar 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 SPLOŠNE OPOMBE

12. Evropski odbor za varstvo podatkov ugotavlja, da osnutek zahtev za akreditacijo ni popolnoma v skladu z zgradbo iz Priloge 1 k smernicam. Manjkata na primer oddelka „področje uporabe“ ter „izrazi in opredelitve pojmov“. Glede tega odbor zaradi jasnosti in lažje ocene zahtev meni, da bi lahko izboljšali številčenje in splošno zgradbo dokumenta. Zato Evropski odbor za varstvo podatkov zaradi lažjega ocenjevanja češki nadzorni organ spodbuja, naj v osnutku zahtev za akreditacijo upošteva zgradbo Priloge in doda manjkajoče oddelke, pri čemer je še posebno pomembna

opredelitev izrazov, ki se uporabljajo v dokumentu. Poleg tega odbor ugotavlja, da se osnutek zahtev za akreditacijo češkega nadzornega organa večkrat nanaša na ustrezen oddelek standarda ISO 17065 ali ustrezne oddelke iz Priloge brez navedbe takega sklicevanja. Evropski odbor za varstvo podatkov tako češki nadzorni organ poziva, naj jasno navede sklicevanja na oddelke standarda ISO 17065 in Priloge.

13. Evropski odbor za varstvo podatkov ugotavlja, da se osnutek zahtev za akreditacijo češkega nadzornega organa večkrat nanaša na „vrednoteni predmet“ (na primer oddelki 3.2.1.2.1.2.10; 3.2.1.2.6.3.1; 3.2.1.2.8.1.6.3; 3.2.1.2.10.4.1; 3.1.2.10.7.3.1; 3.1.2.10.7.3.2 in 3.2.1.2.10.10.2). Odbor razume, da je ta izraz sopomenka besedne zveze „cilj vrednotenja“. Vendar za zagotovitev jasnosti češki nadzorni organ poziva k dosledni uporabi besedne zveze „cilj vrednotenja“.

14. Evropski odbor za varstvo podatkov ugotavlja, da več zahtev ni opredeljenih kot obveznost telesa za certificiranje (na primer 3.2.1.2.2 in 3.2.1.2.3). Odbor češki nadzorni organ poziva, naj preoblikuje zahteve in jasno navede, da so obvezne – tj. zahteva naj se začne s „telo za certificiranje se obvezuje [...]“.

2.2.3 SPLOŠNE ZAHTEVE ZA AKREDITACIJO

15. Glede sporazuma o certificiranju (oddelek 3.2.1.2.1.2 osnutka zahtev za akreditacijo češkega nadzornega organa) Evropski odbor za varstvo podatkov ugotavlja, da se pododdelek 3.2.1.2.1.2.2 ne sklicuje na „pogodbeno zaupne zadeve“, do katerih bo imel dostop tudi nadzorni organ. Zato češkemu nadzornemu organu priporoča, naj spremeni osnutek, in sicer tako, da vključi obveznost zagotavljanja dostopa nadzornemu organu do pogodbeno zaupnih zadev.

16. Evropski odbor za varstvo podatkov glede pododdelka 3.2.1.2.1.2.8 osnutka zahtev za akreditacijo češkega nadzornega organa ugotavlja, da ni jasno, komu bodo informacije razkrite. Zato češkemu nadzornemu organu svetuje, naj pojasni, kdo bo prejemnik informacij. Poleg tega so navedene informacije „potrebne za odobritev certifikata“, kot je opredeljeno v točki 7 oddelka 4.1.2 Priloge. Odbor češkemu nadzornemu organu priporoča, naj izraz „informacije o odobritvi certifikata“ nadomesti z „informacije, potrebne za odobritev certifikata“.

17. Glede pododdelka 3.2.1.2.1.2.9 osnutka zahtev za akreditacijo češkega nadzornega organa ni jasno, katere vrste informacij bi bilo treba neposredno sporočiti Evropskemu odboru za varstvo podatkov. Člen 42(8) Splošne uredbe o varstvu podatkov določa, da mora odbor med drugim zbirati vse mehanizme certificiranja. Glede tega se predpostavlja, da bodo pristojni nadzorni organi ustrezne informacije predložili Evropskemu odboru za varstvo podatkov, ki jih bo nato objavil v javnem registru. Odbor zato češkemu nadzornemu organu priporoča, naj v skladu s členom 42(8) Splošne uredbe o varstvu podatkov pojasni pododdelek 3.2.1.2.1.2.9 osnutka zahtev.

18. Glede pododdelka 3.2.1.2.1.2.12 osnutka zahtev za akreditacijo češkega nadzornega organa je Evropski odbor za varstvo podatkov seznanjen z dejstvom, da je češki nadzorni organ ustvaril preoblikovano različico dela zahteve, ki je predvidena v Prilogi. Vendar je češki nadzorni organ [kjer je ustrezno] izpustil besedilo „bi morale biti obravnavane tudi posledice za stranko“. Evropski odbor za varstvo podatkov zato češkemu nadzornemu organu priporoča, naj doda manjkajoči del zgoraj navedene zahteve.

19. Poleg tega pododdelek 3.2.1.2.1.2.13 osnutka zahtev za akreditacijo češkega nadzornega organa določa obveznost „vključitve zaveze vložnika, da bo telo za certificiranje obvestilo o vseh spremembah, ki bi lahko vplivale na skladnost certificiranega predmeta z merili za certificiranje“.

Evropski odbor za varstvo podatkov meni, da je ta formulacija preveč splošna, in češkemu nadzornemu organu priporoča, naj osnutek zahtev spremeni tako, da se doda besedilo „vseh sprememb njegovega dejanskega ali pravnega položaja ter sprememb njegovih proizvodov, procesov in storitev, ki jih zadeva certificiranje“.

20. Glede pečatov in označb za varstvo podatkov (oddelek 3.2.1.2.1.3 osnutka zahtev za akreditacijo češkega nadzornega organa) Evropski odbor za varstvo podatkov ugotavlja, da osnutek zahtev češkega nadzornega organa določa, da mora sporazum o certificiranju vsebovati „pravila o uporabi certifikatov, pečatov in označb, če jih določi lastnik sistema certificiranja“. Enaka formulacija je v pododdelku 3.2.1.2.1.2.14. Evropski odbor za varstvo podatkov meni, da je ta obveznost že zajeta v točki 4.1.2.2. pod črko (l) standarda ISO 17065, zato mora biti vključena v vsak sistem certificiranja (glej tudi točko 4.1.3 standarda ISO 17065). Evropski odbor za varstvo podatkov zaradi jasnosti češkemu nadzornemu organu priporoča, naj zgoraj navedene oddelke črta.

21. Kar zadeva zahteve glede upravljanja nepristranskosti, sta glede na informacije, ki jih je češki nadzorni organ navedel v predlogi, oddelka 4.2.1.(b) in 4.2.2 Priloge zadostno zajeta v točki 4.2 standarda ISO 17065. Vendar Evropski odbor za varstvo podatkov meni, da je treba te zahteve izrecno vključiti v osnutek zahtev za akreditacijo, ki so jih v skladu s Prilogo pripravili nadzorni organi. Zato priporoča, naj češki nadzorni organ vključi manjkajoče zahteve glede upravljanja nepristranskosti, ki so predvidene v Prilogi.

22. Kar zadeva zahtevo glede odgovornosti in financiranja (oddelek 3.2.1.2.3.1 osnutka zahtev češkega nadzornega organa) Evropski odbor za varstvo podatkov češkemu nadzornemu organu priporoča, naj določi, da jo je treba redno zagotavljati.

2.2.4 ZAHTEVE GLEDE VIROV

23. Glede osebja telesa za certificiranje (oddelek 3.2.1.2.8.1.6 osnutka zahtev za akreditacijo češkega nadzornega organa) Evropski odbor za varstvo podatkov ugotavlja, da zahteve za osebje, odgovorno za vrednotenje (pododdelek 3.2.1.2.8.1.6.3), vključujejo *„pet let delovnih izkušenj z najmanj desetimi opravljenimi revizijami, izvedenimi v okviru dejavnosti certificiranja na istem ali podobnem področju […] ali pet let delovnih izkušenj v okviru certificiranja predmetov, ki so v interesu telesa za certificiranje)“*. Podobno zahteve za osebje, odgovorno za odločanje (pododdelek 3.2.1.2.8.1.6.4), vključujejo *„najmanj pet let delovnih izkušenj z najmanj desetimi opravljenimi revizijami, izvedenimi v okviru dejavnosti certificiranja na istem ali podobnem področju.“* Evropski odbor za varstvo podatkov meni, da bi bilo treba zahteve po strokovnem znanju za ocenjevalce in nosilce odločanja prilagoditi ob upoštevanju različnih nalog, ki jih opravljajo. Glede tega odbor meni, da bi morali imeti ocenjevalci specialistično strokovno znanje in strokovne izkušnje na področju tehničnih postopkov (na primer revizije in certificiranja), nosilci odločanja pa bi morali imeti splošnejše in celovitejše strokovno znanje ter delovne izkušnje s področja varstva podatkov. Ob upoštevanju zgoraj navedenega Evropski odbor za varstvo podatkov češkemu nadzornemu organu svetuje, naj ta pododdelek preoblikuje ob upoštevanju različnih vsebinskih zahtev glede znanja in/ali izkušenj za ocenjevalce in nosilce odločanja.

24. Poleg tega ugotavlja, da je v točki 3.2.1.2.9.1 osnutka zahtev za akreditacijo češkega nadzornega organa navedeno, da zunanje izvajanje storitev certificiranja ni dovoljeno. Kljub temu naslednja točka dovoljuje uporabo zunanjih revizorjev in strokovnjakov za vrednotenje, razen če je del dejavnosti certificiranja. Evropski odbor za varstvo podatkov meni, da bi bilo treba v osnutku zahtev

za akreditacijo natančno določiti, kdaj „pomeni dejavnosti certificiranja“, ali pojasniti, da bo telo za certificiranje ohranilo odgovornost za odločanje, tudi v primerih, ko bo uporabil zunanje strokovnjake. Zato odbor češkemu nadzornemu organu priporoča, naj ustrezno spremeni osnutek.

2.2.5 ZAHTEVE GLEDE POSTOPKA

25. Evropski odbor za varstvo podatkov ugotavlja, da se oddelek 3.2.1.2.10.1.1 osnutka dodatnih zahtev češkega nadzornega organa nanaša na „vse dodatne zahteve glede nasprotja interesov (7.1, točka 1)“. Vendar osnutek dodatnih zahtev češkega nadzornega organa ne vsebuje dodatnih zahtev glede nasprotja interesov. Zato češkemu nadzornemu organu priporoča, naj spremeni osnutek, da se izogne zmedi.

26. Glede zahtev za prijavo Evropski odbor za varstvo podatkov ugotavlja, da se zdi, da pododdelek 3.2.1.2.10.2.3 osnutka zahtev za akreditacijo češkega nadzornega organa nakazuje, da se informacije o prenesenih podatkih v vlogi navedejo le, če gre za prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo. Kljub temu poudarja, da mora vloga vedno vsebovati opis podatkov, prenesenih v druge sisteme ali organizacije, ne glede na njihovo lokacijo. Evropski odbor za varstvo podatkov zato češkemu nadzornemu organu priporoča, naj spremeni besedilo, da se izogne zmedi.

27. Evropski odbor za varstvo podatkov ugotavlja, da obveznost določitve zavezujočih metod vrednotenja v sporazumu o certificiranju (oddelek 3.2.1.2.1.2.6 osnutka zahtev za akreditacijo češkega nadzornega organa) ne vsebuje sklicevanja na cilj vrednotenja, kot je določeno v točki 1 oddelka 7.3 Priloge k smernicam. Zaradi jasnosti odbor češkemu nadzornemu organu priporoča, naj doda tako sklicevanje.

28. Poleg tega ugotavlja, da osnutek zahtev za akreditacijo češkega nadzornega organa predvideva stanje, v katerem se obdelovalci uporabljajo za obdelavo podatkov, v skladu s Prilogo k smernicam (oddelek 3.2.1.2.10.2 osnutka zahtev za akreditacijo češkega nadzornega organa). Evropski odbor za varstvo podatkov češkim nadzornim organom priporoča, naj premislijo, ali bi v tem primeru navedli tudi sklicevanje na skupne upravljavce in njihove posebne dogovore.

29. V zvezi z zahtevami glede vrednotenja (oddelek 3.2.1.2.10.4 osnutka zahtev češkega nadzornega organa) Evropski odbor za varstvo podatkov ugotavlja, da zahteve za akreditacijo češkega nadzornega organa ne določajo obveznosti telesa za certificiranje, da v svojem mehanizmu certificiranja podrobno opredeli, kako se informacije, zahtevane v točki 7.4.6 standarda ISO 17065, predložijo vložniku glede neskladnosti iz mehanizma certificiranja. Kot je določeno v Prilogi (pododdelek 7.4), se opredelita vsaj narava in časovni okvir takega obveščanja. Zato Evropski odbor za varstvo podatkov češkemu nadzornemu organu priporoča, naj vključi zgoraj navedeno obveznost.

30. Poleg tega se zdi, da pododdelek 3.2.1.2.10.4.2 osnutka zahtev češkega nadzornega organa omejuje metode vrednotenja na preskušanje, revizijo ali preglede. Evropski odbor za varstvo podatkov meni, da bi se lahko uporabljale tudi druge metode vrednotenja, zato češkemu nadzornemu organu priporoča, naj spremeni osnutek in pojasni, da naštete metode niso izčrpne.

31. Glede pododdelka 3.2.1.2.10.4.4.1.4 osnutka zahtev za akreditacijo češkega nadzornega organa Evropski odbor za varstvo podatkov meni, da bi moralo biti v zahtevah jasno navedeno, da mora telo za certificiranje preveriti izpolnjevanje meril, in češkemu nadzornemu organu priporoča, naj v skladu s tem spremeni osnutek.

32. Glede zahtev za pregled (pododdelek 3.2.1.2.10.5 osnutka zahtev za akreditacijo češkega nadzornega organa) Evropski odbor za varstvo podatkov ugotavlja, da se osnutek zahtev za akreditacijo češkega nadzornega organa ne sklicuje na obveznost določitve postopkov za dodelitev in preklic certifikatov. Češkemu nadzornemu organu zato priporoča, naj osnutek ustrezno spremeni.

33. Glede zahtev za dokumentacijo o certificiranju Evropski odbor za varstvo podatkov ugotavlja, da je v oddelku 3.1.2.10.7.2 osnutka zahtev za akreditacijo češkega nadzornega organa navedeno, da telo za certificiranje določi, da je spremljanje pogoj za veljavnost certifikata, „če sistem certificiranja zahteva spremljanje [...]“. Odbor meni, da so v primeru certificiranja v skladu s Splošno uredbo o varstvu podatkov dejavnosti spremljanja vedno obvezne, zato češkemu nadzornemu organu priporoča, naj vključi to obveznost.

34. Glede zahtev, povezanih z registrom certificiranih proizvodov (oddelek 3.2.1.2.10.8 osnutka zahtev za akreditacijo češkega nadzornega organa in oddelek 7.8 v Prilogi), in zlasti obveznosti obveščanja pristojnega nadzornega organa o razlogih za odobritev ali preklic zahtevanega certifikata Evropski odbor za varstvo podatkov ugotavlja, da se osnutek zahtev za akreditacijo češkega nadzornega organa nanaša na oddelek 3.2.1.2.10.4.5. Vendar se ta oddelek nanaša na obveznost, da se češkemu organu na zahtevo zagotovi dostop do dokumentacije o vrednotenju, zahteva iz oddelka 7.8 Priloge k smernicam pa vsebuje obveznost proaktivnega obveščanja nadzornega organa o razlogih za odobritev ali preklic certifikata. Zato češkemu nadzornemu organu priporoča, naj osnutek ustrezno spremeni.

35. Glede sprememb, ki vplivajo na certificiranje, Evropski odbor za varstvo podatkov ugotavlja, da osnutek zahtev za akreditacijo češkega nadzornega organa med postopki, o katerih se je treba dogovoriti, ne omenja postopka odobritve s strani pristojnega nadzornega organa, na katerega se sklicuje v Prilogi k smernicam (stran 19). Odbor priznava, da seznam iz oddelka 7.10 Priloge ni obvezen. Da pa bi zagotovil doslednost, češkemu nadzornemu organu priporoča, naj postopku odobritve s strani nadzornega organa doda sklic.

36. Evropski odbor za varstvo podatkov ugotavlja, da osnutek zahtev za akreditacijo češkega nadzornega organa ne določa jasno obveznosti telesa za certificiranje glede sprejetja odločitev in odredb češkega nadzornega organa o preklicu ali neizdaji certifikata vložniku, če zahteve glede certificiranja niso več izpolnjene. Zato češkemu nadzornemu organu priporoča, naj to obveznost jasno vključi v osnutek zahtev za akreditacijo. Glede prekinitve, omejitve, začasnega odvzema ali preklica certifikata ugotavlja, da se oddelka 3.2.1.2.10.10.2 in 3.2.1.2.10.10.3 osnutka zahtev nanašata na „pobudo“. Če je namen sklicevanje na „odločitve in odredbe“ nadzornega organa, kot je določeno v členu 58(2)(h) Splošne uredbe o varstvu podatkov, Evropski odbor za varstvo podatkov češkemu nadzornemu organu priporoča, naj uporabi izrazje iz Splošne uredbe o varstvu podatkov ter se sklicuje na „odločitve in odredbe“.

2.2.6 SISTEM UPRAVLJANJA

37. Evropski odbor za varstvo podatkov meni, da oddelek 3.2.1.2.11 osnutka dodatnih zahtev češkega nadzornega organa ne vsebuje obveznosti telesa za certificiranje, da mora „stalno in nenehno javno objavljati, katera certificiranja so bila opravljena in na kateri podlagi, kako dolgo so certifikati veljavni, na podlagi katerih okvirov in pod katerimi pogoji,“ kot je navedeno v oddelku 8 Priloge. Zato češkemu nadzornemu organu priporoča, naj z dodajanjem zgoraj navedenega sklicevanja osnutek zahtev ustrezno spremeni.

3 SKLEPNE UGOTOVITVE/PRIPOROČILA

38. Osnutek zahtev češkega nadzornega organa za akreditacijo lahko vodi v nedosledno uporabo akreditacije teles za certificiranje, zato je treba spremeniti naslednje:

39. Glede „splošnih zahtev za akreditacijo“ Evropski odbor za varstvo podatkov češkemu nadzornemu organu priporoča, naj:

    1) v oddelek 3.2.1.2.1.2 vključi obveznost zagotavljanja dostopa nadzornega organa do „pogodbeno zaupnih zadev“;

    2) v pododdelku 3.2.1.2.1.2.8 besedilo „informacije o odobritvi certifikata“ nadomesti z besedilom „informacije, potrebne za odobritev certifikata“;

    3) razjasni pododdelek 3.2.1.2.1.2.9 v skladu s členom 42(8) Splošne uredbe o varstvu podatkov;

    4) v pododdelku 3.2.1.2.1.2.12 doda sklic na besedilo [kadar je ustrezno] „bi bilo treba obravnavati tudi posledice za stranko“;

    5) spremeni pododdelek 3.2.1.2.1.2.13 tako, da se doda besedilo „vseh sprememb njegovega dejanskega ali pravnega položaja ter sprememb njegovih proizvodov, procesov in storitev, ki jih zadeva certificiranje“;

    6) črta oddelek 3.2.1.2.1.3 in pododdelek 3.2.1.2.1.2.14;

    7) vključi manjkajoče zahteve glede upravljanja nepristranskosti, ki so predvidene v Prilogi.

40. V zvezi z „zahtevami glede virov“ Evropski odbor za varstvo podatkov češkemu nadzornemu organu priporoča, naj:

    1) spremeni oddelek 3.2.1.2.9.1 in določi, kdaj „pomeni dejavnosti certificiranja“, ali pojasni, da bo telo za certificiranje ohranilo odgovornost odločanja, tudi v primerih, ko bo uporabil zunanje strokovnjake.

41. V zvezi z „zahtevami glede postopka“ Evropski odbor za varstvo podatkov češkemu nadzornemu organu priporoča, naj:

    1) v oddelek 3.2.1.2.10.4 vključi obveznosti telesa za certificiranje, da v svojem mehanizmu certificiranja podrobno določi, kako se informacije, zahtevane v točki 7.4.6 standarda ISO 17065, predložijo vložniku glede neskladnosti iz mehanizma certificiranja;

    2) spremeni oddelek 3.2.1.2.10.5 z vključitvijo sklicevanja na obveznost določitve postopkov za dodelitev in preklic certifikatov;

    3) spremeni oddelek 3.1.2.10.7.2, da bo izražal, da so v primeru certificiranja v skladu s Splošno uredbo o varstvu podatkov dejavnosti spremljanja vedno obvezne;

    4) spremeni oddelek 3.2.1.2.10.8, da bo izražal obveznost proaktivnega obveščanja nadzornega organa o razlogih za odobritev ali preklic certifikata;

5) vključi obveznost telesa za certificiranje glede sprejetja odločitev in odredb češkega nadzornega organa o preklicu ali neizdaji certifikata vložniku, če zahteve glede certificiranja niso več izpolnjene.

42. Glede „sistema upravljanja“ Evropski odbor za varstvo podatkov predlaga, naj češki nadzorni organ:

1) vključi obveznosti telesa za certificiranje, da mora „stalno in nenehno javno objavljati, katera certificiranja so bila opravljena in na kateri podlagi, kako dolgo so certifikati veljavni, na podlagi katerih okvirov in pod katerimi pogoji,“ kot je navedeno v oddelku 8 Priloge.

4 KONČNE PRIPOMBE

43. To mnenje je namenjeno češkemu nadzornemu organu in bo v skladu s členom 64(5)(b) Splošne uredbe o varstvu podatkov na voljo javnosti.

44. V skladu s členom 64(7) in (8) Splošne uredbe o varstvu podatkov češki nadzorni organ svojo odločitev o spremembi oziroma ohranitvi svojega osnutka seznama sporoči predsedniku po elektronski poti v dveh tednih po prejemu mnenja. V istem obdobju pošlje spremenjeni osnutek seznama; če ne namerava v celoti ali deloma upoštevati mnenja Evropskega odbora za varstvo podatkov, pa ustrezno utemelji, zakaj ga ne namerava upoštevati.

45. Češki nadzorni organ bo v skladu s členom 70(1)(y) Splošne uredbe o varstvu podatkov svojo končno odločitev sporočil Evropskemu odboru za varstvo podatkov za vključitev v register odločitev glede vprašanj, obravnavanih v okviru mehanizma za skladnost.

Za Evropski odbor za varstvo podatkov

Predsednica

(Andrea Jelinek)

Sprejeto