KOMISIJAS LĒMUMS (ES) 2021/2243

(2021. gada 15. decembris),

kurā izklāstīti iekšējie noteikumi par datu subjektu informēšanu un dažu viņu tiesību ierobežošanu persondatu apstrādē Komisijas sakaru un informācijas sistēmu drošības vajadzībām

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 249. panta 1. punktu,

tā kā:

(1) Komisijai tās uzdevumu izpildes gaitā ir pienākums ievērot fizisko personu tiesības attiecībā uz personas datu apstrādi, kas paredzētas Savienības Pamattiesību hartas 8. panta 1. punktā un Līguma par Eiropas Savienības darbību 16. panta 1. punktā. Tai ir arī jāievēro tiesības, kas paredzētas Eiropas Parlamenta un Padomes Regulā (ES) 2018/1725 ([1]). Vienlaikus Komisijai ir jārisina IT drošības incidenti saskaņā ar Lēmuma (ES, Euratom) 2017/46 ([2]) 15. panta noteikumiem.

(2) Lai nodrošinātu IT drošību, proti, lai saglabātu sakaru un informācijas sistēmu un tajās apstrādāto datu kopumu konfidencialitāti, integritāti un pieejamību attiecībā uz cilvēkiem, aktīviem un informāciju, Komisija, jo īpaši ar Informātikas ģenerāldirektorāta starpniecību, ir veikusi pasākumus, kā paredzēts Lēmumā (ES, Euratom) 2017/46 un Lēmumā C(2017) 8841 final ([3]). Minēto pasākumu vidū ir IT drošības risku un īstenoto IT drošības pasākumu uzraudzība, prasība sistēmu īpašniekiem veikt īpašus IT drošības pasākumus, lai mazinātu Komisijas sakaru un informācijas sistēmu IT drošības riskus, un IT drošības incidentu pārvaldība.

(3) Informātikas ģenerāldirektorāts nodrošina Komisijai IT drošības operācijas un pakalpojumus, un tam ir jāapstrādā vairākas persondatu kategorijas nolūkā:

— paziņot brīdinājumus par IT drošības notikumiem un incidentiem,

— reaģēt uz IT drošības notikumiem un incidentiem un ierobežot tos,

— veicināt rīkus un darbības, izmantojot drošības revīzijas, drošības novērtējumus un ievainojamības pārvaldību,

— palielināt Komisijas darbinieku informētību kiberdrošības jomā,

— uzraudzīt, atklāt un novērst IT drošības notikumus un incidentus,

— pārskatīt privileģēto lietotāju kontus.

(4) IT drošības incidenti, kas varētu apdraudēt Komisijas informācijas un sakaru sistēmu drošību, var notikt jebkurā Komisijas veiktā apstrādes darbībā. Tie var ietvert jebkuru Komisijas apstrādāto persondatu kategoriju.

([1]) Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp.).

([2]) Komisijas Lēmums (ES, Euratom) 2017/46 (2017. gada 10. janvāris) par komunikācijas un informācijas sistēmu drošību Eiropas Komisijā (OV L 6, 11.1.2017., 40. lpp.).

([3]) Komisijas Lēmums (C(2017) 8841) (2017. gada 13. decembris), ar ko paredz īstenošanas noteikumus 3., 5., 7., 8., 9., 10., 11., 12., 14. un 15. pantam Komisijas Lēmumā 2017/46 par sakaru un informācijas sistēmu drošību Komisijā.

(5) Noteiktos apstākļos var izrādīties nepieciešams saskaņot datu subjektu tiesības atbilstoši Regulai (ES) 2018/1725 ar Komisijas vajadzību efektīvi veikt savus uzdevumus, proti, nodrošināt personu, aktīvu un informācijas IT drošību Komisijā atbilstoši Lēmumam (ES, Euratom) 2017/46, kā arī ar citu datu subjektu pamattiesību un brīvību pilnīgu ievērošanu. Šajā nolūkā Regulas (ES) 2018/1725 25. panta 1. punktā Komisija ir pilnvarota ierobežot minētās regulas 14.–17., 19., 20. un 35. panta piemērošanu, kā arī tās 4. panta 1. punkta a) apakšpunktā nostiprināto pārredzamības principu, ciktāl tā normas atbilst minētās regulas 14.–17., 19. un 20. pantā paredzētajām tiesībām un pienākumiem.

(6) Šis lēmums būtu jāpiemēro visām apstrādes darbībām, ko Komisija veic kā datu pārzinis, pildot savus uzdevumus nodrošināt personu, aktīvu un informācijas IT drošību Komisijā saskaņā ar Lēmumu (ES, Euratom) 2017/46. Tādēļ tam būtu jāattiecas uz persondatu kategoriju datu subjektiem, uz kuriem attiecas visas minētās apstrādes darbības, t. i., personām, kas mijiedarbojas ar kādu no Komisijas informācijas un sakaru sistēmām.

(7) Persondati tiek glabāti drošā elektroniskā vidē, un tādējādi tiek novērsta iespējamība, ka personas ārpus Komisijas varētu tiem nelikumīgi piekļūt. Dažādām apstrādes darbībām atkarībā no iesaistīto persondatu veida piemēro atšķirīgus datu glabāšanas termiņus. Datņu glabāšanu Komisijā reglamentē Komisijas saglabājamo dokumentu vienotais saraksts (SEC(2019) 900), kas ir regulatīvs dokuments glabāšanas grafika veidā, kurā noteikti dažādu veidu Komisijas datņu glabāšanas periodi, lai ierobežotu datu glabāšanu līdz nepieciešamajam līmenim.

(8) Komisijai varētu būt jāierobežo datu subjektu tiesību piemērošana, lai aizsargātu savu iekšējo drošību saskaņā ar Regulas (ES) 2018/1725 25. panta 1. punkta d) apakšpunktu (t. i., lai saglabātu savu sakaru un informācijas sistēmu un tajās apstrādāto datu kopumu, savu aktīvu un informācijas konfidencialitāti, integritāti un pieejamību). Jo īpaši, Komisijai tas varētu būt jādara, kad tā:

— izdod signālus un brīdinājumus par IT drošības notikumiem un incidentiem,

— reaģē uz IT drošības notikumiem un incidentiem un tos ierobežo; veicina rīkus un darbības, izmantojot drošības revīzijas, drošības novērtējumus un ievainojamības pārvaldību,

— palielina Komisijas darbinieku informētību kiberdrošības jomā,

— uzrauga, atklāj un novērš IT drošības notikumus un incidentus,

— pārskata privileģēto lietotāju kontus.

(9) Lai risinātu IT drošības incidentus, kā minēts Lēmuma (ES, Euratom) 2017/46 15. pantā, Informātikas ģenerāldirektorāts var apmainīties ar informāciju ar Cilvēkresursu un drošības ģenerāldirektorāta Grupu reaģēšanai uz kibernoziegumiem.

(10) Lai izpildītu Regulas (ES) 2018/1725 14., 15. un 16. panta prasības, Komisijai būtu jāinformē visas personas par darbībām, kas ietver viņu persondatu apstrādi un ietekmē viņu tiesības. Tas būtu jādara pārredzami un saskaņoti, Komisijas tīmekļa vietnē publicējot paziņojumu par datu aizsardzību. Attiecīgā gadījumā tai būtu jāpiemēro papildu aizsardzības pasākumi, lai attiecīgā formātā atsevišķi informētu datu subjektus.

(11) Atbilstība Regulas (ES) 2018/1725 14., 15. un 16. pantam varētu atklāt, ka pastāv IT drošības pasākumi, vājās vietas vai incidenti, kas veikti saskaņā ar Lēmuma (ES, Euratom) 2017/46 15. pantu. Atklājot minētos IT drošības pasākumus, ievainojamību un incidentus, palielinās risks, ka attiecīgais IT drošības pasākums pēc tam tiks apiets, attiecīgā ievainojamība tiks ļaunprātīgi izmantota un ka varētu tikt apdraudēta notiekošā IT drošības incidenta analīze, jo lietotājs vai ļaunprātīgs dalībnieks var nejauši vai tīši manipulēt ar artefaktiem. Tas var nopietni apdraudēt Komisijas spēju nodrošināt IT drošību un, jo īpaši, efektīvi risināt IT drošības incidentus nākotnē.

(12) Saskaņā ar Regulas (ES) 2018/1725 25. panta 1. punkta h) apakšpunktu Komisija ir arī pilnvarota ierobežot datu subjektu tiesību piemērošanu, lai aizsargātu citu personu tiesības un brīvības saistībā ar IT drošības incidentiem, kas var apdraudēt IT drošības operācijas.

(13) Komisijai var nākties ierobežot informācijas sniegšanu datu subjektiem un datu subjektu citu tiesību piemērošanu saistībā ar persondatiem, kas saņemti no trešām valstīm vai starptautiskām organizācijām, lai īstenotu savu pienākumu sadarboties ar šīm valstīm vai organizācijām. Tā ir daļa no Komisijas pienākuma aizsargāt svarīgu ES vispārējo sabiedrības interešu mērķi, kā minēts Regulas (ES) 2018/1725 25. panta 1. punkta c) apakšpunktā. Tomēr dažos gadījumos datu subjekta pamattiesību intereses prevalē pār starptautiskās sadarbības interesēm.

(14) Tāpēc Komisija ir noteikusi Regulas (ES) 2018/1725 25. panta 1. punkta c), d) un h) apakšpunktā uzskaitītos iemeslus par pamatojumu ierobežojumiem, kurus var būt nepieciešams piemērot datu apstrādes darbībām, ko veic Informātikas ģenerāldirektorāts, saistībā ar IT drošības operāciju un pakalpojumu sniegšanu Komisijai.

(15) Visiem ierobežojumiem, ko piemēro, pamatojoties uz šo lēmumu, jābūt nepieciešamiem un samērīgiem, ņemot vērā riskus datu subjektu tiesībām un brīvībām.

(16) Komisijai visi ierobežojumi būtu jāizskata pārredzamā veidā un jāreģistrē visi ierobežojumu piemērošanas gadījumi attiecīgajā ierakstu sistēmā.

(17) Saskaņā ar Regulas (ES) 2018/1725 25. panta 8. punktu datu pārziņi var atlikt, izlaist vai atteikt informācijas sniegšanu datu subjektam par ierobežojuma piemērošanas iemesliem, ja šādas informācijas sniegšanas rezultātā ierobežojums vairs nebūtu iedarbīgs. Jo īpaši, tas attiecas uz pienākumu ierobežojumiem, kas paredzēti Regulas (ES) 2018/1725 16. un 35. pantā. Komisijai būtu regulāri jāpārskata noteiktie ierobežojumi, lai nodrošinātu, ka datu subjekta tiesības tikt informētam saskaņā ar Regulas (ES) 2018/1725 16. un 35. pantu ir ierobežotas tikai tik ilgi, kamēr šādi ierobežojumi ir nepieciešami, lai Komisija varētu nodrošināt tās IT drošību, jo īpaši – IT drošības incidentu risināšanu.

(18) Ja Komisija ierobežo tādu datu subjektu tiesību piemērošanu, kas nav minēti Regulas (ES) 2018/1725 16. un 35. pantā, datu pārzinim katrā gadījumā atsevišķi būtu jāizvērtē, vai ierobežojuma paziņošana apdraudētu tā mērķi.

(19) Lai pārliecinātos, ka tiek nodrošināta atbilstība šim lēmumam, Komisijas datu aizsardzības speciālistam būtu neatkarīgi jāpārskata ierobežojumu piemērošana.

(20) Lai Komisija varētu nekavējoties ierobežot konkrētu tiesību un pienākumu piemērošanu saskaņā ar Regulas (ES) 2018/1725 25. pantu, šim lēmumam būtu jāstājas spēkā divdesmitajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

(21) Eiropas Datu aizsardzības uzraudzītājs sniedza atzinumu 2021. gada 16. septembrī,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Priekšmets un darbības joma

1. Šajā lēmumā ir izklāstīti noteikumi, kas Komisijai jāievēro, saskaņā ar Regulas (ES) 2018/1725 14., 15. un 16. pantu informējot datu subjektus par viņu persondatu apstrādi, kad tā veic savus uzdevumus atbilstoši Lēmumam (ES, Euratom) 2017/46.

Tajā arī noteikts, ar kādiem nosacījumiem Komisija, ievērojot Regulas (ES) 2018/1725 25. panta 1. punkta c), d) un h) apakšpunktu, var ierobežot minētās regulas 4., 14.–17., 19., 20. un 35. panta piemērošanu, kad tā veic savus uzdevumus atbilstoši Lēmumam (ES, Euratom) 2017/46.

2. Šis lēmums attiecas uz Komisijas vai tās vārdā veikto persondatu apstrādi tādu darbību vajadzībām vai saistībā ar tādām darbībām, kas tiek veiktas, lai nodrošinātu personu, aktīvu un informācijas IT drošību Komisijā saskaņā ar Lēmumu (ES, Euratom) 2017/46.

2. pants

Piemērojamie izņēmumi un ierobežojumi

1. Kad Komisija veic savus pienākumus saistībā ar datu subjektu tiesībām, kā noteikts Regulā (ES) 2018/1725, tā apsver, vai būtu piemērojams kāds no minētajā regulā paredzētajiem izņēmumiem.

2. Ievērojot šā lēmuma 3.–7. pantu, ja Regulas (ES) 2018/1725 14.–17., 19., 20. un 35. pantā paredzēto tiesību un pienākumu īstenošana saistībā ar Komisijas apstrādātajiem persondatiem, kas apdraudētu IT drošības operāciju un pakalpojumu sniegšanas nolūku, cita starpā atklājot Komisijas izmeklēšanas līdzekļus, vājās vietas un metodes, vai negatīvi ietekmētu citu datu subjektu tiesības un brīvības un drošību, jo īpaši attiecībā uz persondatu apstrādi nolūkā:

— paziņot brīdinājumus par IT drošības notikumiem un incidentiem,

— reaģēt uz IT drošības notikumiem un incidentiem un ierobežot tos,

— veicināt rīkus un darbības, izmantojot drošības revīzijas, drošības novērtējumus un ievainojamības pārvaldību,

— palielināt Komisijas darbinieku informētību kiberdrošības jomā,

— uzraudzīt, atklāt un novērst IT drošības notikumus un incidentus,

— pārskatīt privileģēto lietotāju kontus,

Komisija var ierobežot:

a) Regulas (ES) 2018/1725 14.–17., 19., 20. un 35. panta piemērošanu;

b) Regulas (ES) 2018/1725 4. panta 1. punkta a) apakšpunktā noteiktā pārredzamības principa piemērošanu, ciktāl tā normas atbilst Regulas (ES) 2018/1725 14.–17., 19. un 20. pantā paredzētajām tiesībām un pienākumiem.

Komisija to var darīt saskaņā ar Regulas (ES) 2018/1725 25. panta 1. punkta c), d) un h) apakšpunktu.

3. Ievērojot 3.–7. pantu, Komisija var ierobežot šā panta 2. punktā minētās tiesības un pienākumus:

a) ja minēto tiesību un pienākumu īstenošanu attiecībā uz persondatiem, kas iegūti no citas Eiropas Savienības iestādes, struktūras, aģentūras vai biroja, minētā cita Eiropas Savienības iestāde, struktūra, aģentūra vai birojs varētu ierobežot uz Regulas (ES) 2018/1725 25. pantā minēto tiesību aktu pamata vai saskaņā ar minētās regulas IX nodaļu, vai saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/794 ([4]) vai Padomes Regulu (ES) 2017/1939 ([5]);

b) ja minēto tiesību un pienākumu īstenošanu attiecībā uz persondatiem, kas iegūti no dalībvalsts kompetentās iestādes, minētās dalībvalsts kompetentās iestādes varētu ierobežot uz Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 ([6]) 23. pantā minēto likumdošanas pasākumu pamata vai saskaņā ar valsts noteikumiem, ar kuriem transponēts Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/680 ([7]) 13. panta 3. punkts, 15. panta 3. punkts vai 16. panta 3. punkts;

([4]) Eiropas Parlamenta un Padomes Regula (ES) 2016/794 (2016. gada 11. maijs) par Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (Eiropolu) un ar kuru aizstāj un atceļ Padomes Lēmumus 2009/371/TI, 2009/934/TI, 2009/935/TI, 2009/936/TI un 2009/968/TI (OV L 135, 24.5.2016., 53. lpp.).

([5]) Padomes Regula (ES) 2017/1939 (2017. gada 12. oktobris), ar ko īsteno ciešāku sadarbību Eiropas Prokuratūras (*EPPO*) izveidei (OV L 283, 31.10.2017., 1. lpp.).

([6]) Eiropas Parlamenta un Padomes Regula (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) (OV L 119, 4.5.2016., 1. lpp.).

([7]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV L 119, 4.5.2016., 89. lpp.).

c) ja minēto tiesību un pienākumu īstenošana apdraudētu Komisijas sadarbību ar trešām valstīm vai starptautiskām organizācijām kopīgu kiberdrošības draudu jomā.

Pirms ierobežojumu piemērošanas apstākļos, kas minēti šā punkta pirmās daļas a) un b) punktā, Komisija apspriežas ar attiecīgajām ES iestādēm, struktūrām, aģentūrām, birojiem vai dalībvalstu iestādēm par ierobežojumu noteikšanas iespējamo pamatojumu un par attiecīgo ierobežojumu nepieciešamību un samērīgumu, ja vien tas neapdraud Komisijas darbību un ja vien Komisijai nav skaidrs, ka ierobežojuma piemērošana ir paredzēta kādā no minētajos apakšpunktos minētajiem aktiem vai ka apspriešanās kaitētu Komisijas Lēmumā (ES, Euratom) 2017/46 paredzēto darbību mērķim.

Pirmās daļas c) punktu nepiemēro, ja datu subjekta intereses vai pamattiesības un brīvības prevalē pār Komisijas interesēm sadarboties ar trešām valstīm vai starptautiskām organizācijām.

4. 1., 2. un 3. punkts neskar citu Komisijas lēmumu piemērošanu, kuros noteikti iekšējie noteikumi attiecībā uz informācijas sniegšanu datu subjektiem un konkrētu tiesību piemērošanas ierobežojumi saskaņā ar Regulas (ES) 2018/1725 25. pantu.

5. Visi 2. punktā minētie tiesību un pienākumu ierobežojumi ir nepieciešami un samērīgi ar datu subjektu tiesību un brīvību riskiem.

6. Pirms ierobežojumu piemērošanas katrā gadījumā atsevišķi veic nepieciešamības un samērīguma pārbaudi, un ierobežojumi drīkst būt tikai tādi, kas ir absolūti nepieciešami paredzētā mērķa sasniegšanai.

3. pants

Informācijas sniegšana datu subjektiem

1. Komisija savā tīmekļa vietnē publicē datu aizsardzības paziņojumu, kurā visus datu subjektus informē par tās darbībām, kas ietver viņu persondatu apstrādi, tostarp attiecīgo persondatu kategoriju aprakstu, nolūkā pildīt uzdevumus atbilstoši Lēmumam (ES, Euratom) 2017/46. Ja to ir iespējams izdarīt, neapdraudot IT drošību, Komisija nodrošina, ka datu subjekti atbilstošā formātā tiek atsevišķi informēti.

2. Ja Komisija pilnībā vai daļēji ierobežo informācijas sniegšanu datu subjektiem, kuru persondatus tā apstrādā, lai īstenotu savus uzdevumus atbilstoši Lēmumam (ES, Euratom) 2017/46, tā sagatavo ierakstu par ierobežojuma iemesliem un tos reģistrē saskaņā ar minētā lēmuma 6. pantu.

4. pants

Datu subjekta piekļuves tiesības, tiesības uz datu dzēšanu un tiesības ierobežot datu apstrādi

1. Ja Komisija pilnībā vai daļēji ierobežo datu subjektu piekļuves tiesības persondatiem, tiesības uz datu dzēšanu vai tiesības ierobežot datu apstrādi, kuras minētas Regulas (ES) 2018/1725 attiecīgi 17., 19. un 20. pantā, tā savā atbildē uz piekļuves, datu dzēšanas vai apstrādes ierobežošanas pieprasījumu attiecīgo datu subjektu informē par:

a) piemēroto ierobežojumu un šādas rīcības galvenajiem iemesliem;

b) to, kā iesniegt sūdzību Eiropas Datu aizsardzības uzraudzītājam (EDAU) vai celt prasību Eiropas Savienības Tiesā.

2. Komisija var atlikt, neveikt vai atteikt informācijas sniegšanu par 1. punktā minētā ierobežojuma iemesliem, ja tādējādi ierobežojums vairs nebūtu iedarbīgs.

3. Komisija sagatavo ierakstu un reģistrē šā ierobežojuma iemeslus saskaņā ar 6. pantu.

4. Ja piekļuves tiesības tiek ierobežotas pilnā vai daļējā apmērā, datu subjekti savas piekļuves tiesības var izmantot ar Eiropas Datu aizsardzības uzraudzītāja starpniecību saskaņā ar Regulas (ES) 2018/1725 25. panta 6., 7. un 8. punktu.

5. pants

Datu subjekta informēšana par persondatu aizsardzības pārkāpumu

Ja Komisija ierobežo datu subjekta informēšanu par persondatu aizsardzības pārkāpumu atbilstoši Regulas (ES) 2018/1725 35. pantam, tā sagatavo ierakstu par ierobežojuma iemesliem un reģistrē tos saskaņā ar šā lēmuma 6. pantu. Komisija ierakstu dara zināmu EDAU, kad tiek paziņots par persondatu aizsardzības pārkāpumu.

6. pants

Ierobežojumu ieraksta veikšana un reģistrēšana

1. Komisija veic ierakstu par saskaņā ar šo lēmumu piemēroto ierobežojumu iemesliem, tai skaitā atsauci uz ierobežojumam piemēroto juridisko pamatu un novērtējumu par ierobežojuma nepieciešamību un samērīgumu, ņemot vērā attiecīgos elementus, kas noteikti Regulas (ES) 2018/1725 25. panta 2. punktā.

2. Ierakstā norāda, kā datu subjekta tiesību īstenošana varētu apdraudēt IT drošības operāciju un pakalpojumu sniegšanas nodrošināšanas mērķi Komisijai atbilstoši Lēmumam (ES, Euratom) 2017/46 vai saskaņā ar šā lēmuma 2. panta 2. vai 3. punktu piemēroto ierobežojumu, vai varētu negatīvi ietekmēt citu datu subjektu tiesības un brīvības.

3. Komisija reģistrē minētos ierakstus un visus dokumentus, kas satur pamatā esošos faktiskos un juridiskos elementus. Tos pēc pieprasījuma dara pieejamus Eiropas Datu aizsardzības uzraudzītājam.

7. pants

Ierobežojumu ilgums

1. Ierobežojumus, kas minēti 3., 4. un 5. pantā, piemēro tik ilgi, kamēr ir spēkā tos pamatojošie iemesli.

2. Ja 3., 4. un 5. pantā minēto ierobežojumu iemesli vairs nav spēkā, Komisija:

a) atceļ ierobežojumu;

b) informē datu subjektu par ierobežojuma galvenajiem iemesliem;

c) informē datu subjektu par to, kā jebkurā laikā iesniegt sūdzību Eiropas Datu aizsardzības uzraudzītājam vai celt prasību Eiropas Savienības Tiesā.

8. pants

Aizsardzības pasākumi un glabāšanas periodi

1. Komisija pārskata 3.. 4. un 5. pantā minētā ierobežojuma piemērošanu sešus mēnešus pēc tā pieņemšanas un konkrētās IT drošības operācijas noslēgumā. Pēc tam Komisija ik gadu pārskata un pārliecinās, vai ierobežojumu joprojām nepieciešams uzturēt spēkā.

Pārskatīšana ietver novērtējumu par ierobežojuma nepieciešamību un samērīgumu, ņemot vērā attiecīgos elementus, kas noteikti Regulas (ES) 2018/1725 25. panta 2. punktā.

2. Komisija ir pieņēmusi tehniskus un organizatoriskus pasākumus, lai izvairītos no nejaušas vai nelikumīgas nosūtīto, glabāto vai citādi apstrādāto persondatu iznīcināšanas, nozaudēšanas, pārveidošanas, neatļautas izpaušanas vai piekļuves tiem, piemēram, piekļuves tiesību pārvaldība, dublējumkopēšanas politika un citi pasākumi saskaņā ar Lēmumu (ES, Euratom) 2017/46.

3. Komisija reģistrē piemērojamos glabāšanas periodus atbilstoši Komisijas saglabājamo dokumentu vienotajam sarakstam un dara pieejamus datu subjektiem attiecīgos glabāšanas periodus attiecībā uz šīm apstrādes darbībām savā datu aizsardzības paziņojumā.

9. pants

Komisijas datu aizsardzības speciālista veikta pārskatīšana

1. Komisija bez liekas kavēšanās informē datu aizsardzības speciālistu par ikvienu datu subjektu tiesību ierobežošanas gadījumu saskaņā ar šo lēmumu. Datu aizsardzības speciālistam pēc pieprasījuma nodrošina piekļuvi protokolam un dokumentiem, kuros ir fiksēti attiecīgie faktu un juridiskie elementi.

2. Datu aizsardzības speciālists var pieprasīt ierobežojumu pārskatīšanu, un viņu informē par pieprasītās pārskatīšanas iznākumu.

3. Komisija dokumentē datu aizsardzības speciālista iesaisti ikvienā datu subjektu tiesību ierobežošanas gadījumā saskaņā ar šo lēmumu.

10. pants

Stāšanās spēkā

Šis lēmums stājas spēkā divdesmitajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Briselē, 2021. gada 15. decembrī

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN