IETEIKUMI

KOMISIJAS IETEIKUMS

(2012. gada 6. februāris)

par datu aizsardzības pamatnostādnēm agrās brīdināšanas un reaģēšanas sistēmai (ABRS)

(izziņots ar dokumenta numuru C(2012) 568)

(Dokuments attiecas uz EEZ)

(2012/73/ES)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 292. pantu,

apspriedusies ar Eiropas Datu aizsardzības uzraudzītāju,

tā kā:

(1) Ar Eiropas Parlamenta un Padomes 1998. gada 24. septembra Lēmumu Nr. 2119/98/EK par epidemioloģiskās uzraudzības un infekcijas slimību kontroles tīkla izveidošanu Kopienā [1] tika izveidots epidemioloģiskās uzraudzības un infekcijas slimību kontroles tīkls Kopienā un agrās brīdināšanas un reaģēšanas sistēma (turpmāk "ABRS") šo slimību profilaksei un kontrolei.

(2) Komisija ar 1999. gada 22. decembra Lēmumu 2000/57/EK par agrās brīdināšanas un reaģēšanas sistēmu infekcijas slimību profilaksei un kontrolei saskaņā ar Eiropas Parlamenta un Padomes Lēmumu Nr. 2119/98/EK [2] pieņēma ABRS īstenošanas noteikumus, kuru mērķis ir, izmantojot attiecīgus līdzekļus, veidot strukturētu un pastāvīgu saziņu starp Komisiju un kompetentām valsts veselības aprūpes iestādēm, kas Eiropas Ekonomikas zona dalībvalstīs ir atbildīgas par tādu pasākumu noteikšanu, kuri varētu būt vajadzīgi, lai aizsargātu sabiedrības veselību, novērstu un apturētu infekcijas slimību izplatību [3].

(3) Personas datu aizsardzības tiesības noteiktas Eiropas Savienības Pamattiesību hartā, jo īpaši tās 8. pantā.

(4) Turklāt informācijas elektroniskai apmaiņai starp dalībvalstīm un starp dalībvalstīm un Komisiju jāatbilst noteikumiem par personas datu aizsardzību, kuri paredzēti Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvā 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti [4] un Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regulā (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti [5].

(5) Ar Komisijas 2009. gada 10. jūlija Lēmumu 2009/547/EK par agrās brīdināšanas un reaģēšanas sistēmu infekcijas slimību profilaksei un kontrolei saskaņā ar Eiropas Parlamenta un Padomes Lēmumu Nr. 2119/98/EK [6] ieviesti īpaši aizsardzības pasākumi personas datu apmaiņai starp dalībvalstīm kontaktu izsekošanas procedūru laikā inficētu personu un potenciāli apdraudētu personu identifikācijai, notiekot atgadījumiem saistībā ar infekcijas slimībām, kuras, iespējams, varētu izplatīties ES.

(6) Eiropas Datu aizsardzības uzraudzītājs (turpmāk "EDAU") 2010. gada 26. aprīlī izdeva iepriekšējas pārbaudes atzinumu [7], kurā aicināja skaidrot dažādu ABRS dalībnieku pienākumus un pienācīgi risināt iespējamos pamattiesību

[1] OV L 268, 3.10.1998., 1. lpp.
[2] OV L 21, 26.1.2000., 32. lpp.
[3] ABRS uzdevums ir, izmantojot dalībvalstu kompetentās valsts veselības aprūpes iestādes, ziņot par konkrētiem sabiedrības veselības apdraudējumiem ("atgadījumiem"), kā noteikts Lēmuma 2000/57/EK I pielikumā.
[4] OV L 281, 23.11.1995., 31. lpp.
[5] OV L 8, 12.1.2001., 1. lpp.
[6] OV L 181, 14.7.2009., 57. lpp.
[7] Eiropas Datu aizsardzības uzraudzītāja 2010. gada 26. aprīļa iepriekšējas pārbaudes atzinums par agrās brīdināšanas un reaģēšanas sistēmu, par kuru Eiropas Komisija paziņoja 2009. gada 18. februārī (lieta C 2009-0137). Atzinums publicēts EDAU tīmekļa vietnē šādā adresē: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2010/10-04-26_EWRS_EN.pdf.

apdraudējumus, kas rodas, apstrādājot kontaktu izsekošanas datus plašākā mērogā, lielu pandēmijas draudu gadījumā nākotnē.

(7) Ņemot vērā minētajā atzinumā izklāstītos EDAU ieteikumus, Komisija ir izstrādājusi datu aizsardzības pamatnostādnes agrās brīdināšanas un reaģēšanas sistēmai, lai tādējādi palīdzētu skaidrot sistēmas dažādo dalībnieku nozīmi, uzdevumus un pienākumus, kā arī garantētu efektīvu atbilstību iepriekš minētajiem datu aizsardzības noteikumiem un nodrošinātu datu subjektiem saprotamu informāciju un viegli pieejamus mehānismus savu tiesību izmantošanai,

IR PIEŅĒMUSI ŠO IETEIKUMU.

1. Dalībvalstīm būtu jāpievērš ABRS lietotāju uzmanība šā ieteikuma pielikumā iekļautajām pamatnostādnēm.

2. ABRS valsts kompetentās iestādes būtu jāmudina vērsties pie savām valsts datu aizsardzības iestādēm, lai saņemtu norādījumus un palīdzību par labāko veidu, kā īstenot šīs pamatnostādnes saskaņā ar valsts tiesību aktiem.

3. Dalībvalstis tiek aicinātas nodrošināt atgriezenisko saikni ar Eiropas Komisiju attiecībā uz pielikumā paredzēto pamatnostādņu īstenošanu ne vēlāk kā divus gadus pēc šā ieteikuma pieņemšanas. Par šo atgriezenisko saikni tiks informēts arī EDAU, un to ņems vērā Komisija, lai vērtētu datu aizsardzības līmeni ABRS, kā arī jebkuru nākamo pasākumu saturu un savlaicīgumu, tostarp iespējamo juridiska instrumenta pieņemšanu.

4. Šis ieteikums ir adresēts dalībvalstīm.

Briselē, 2012. gada 6. februārī

Komisijas vārdā –
Komisijas loceklis
John DALLI

PIELIKUMS

DATU AIZSARDZĪBAS PAMATNOSTĀDNES AGRĀS BRĪDINĀŠANAS UN REAĢĒŠANAS SISTĒMAI (ABRS)

1. IEVADS

ABRS ir tīmekļa lietojumprogramma, kuru izstrādājusi Eiropas Komisija sadarbībā ar dalībvalstīm un kuras mērķis ir veidot strukturētu un pastāvīgu saziņu starp Komisiju un kompetentām valsts veselības aprūpes iestādēm, kuras EEZ dalībvalstīs ir atbildīgas par pasākumu noteikšanu sabiedrības veselības aizsardzībai. ES aģentūra Eiropas Slimību profilakses un kontroles centrs (turpmāk "*ECDC*") kopš 2005. gada arī ir saistīta ar ABRS ([1]).

Sadarbībai starp valsts veselības aprūpes iestādēm ir liela nozīme, lai palielinātu dalībvalstu spēju novērst iespējamo infekcijas slimību izplatību ES, kā arī gatavību koordinēti un savlaicīgi reaģēt uz atgadījumiem, kurus izraisa infekcijas slimības, kas ir vai potenciāli var kļūt par sabiedrības veselības apdraudējumu.

Iepriekšējie *SARS*, pandēmiskās gripas A(H1N1) un citu infekcijas slimību uzliesmojumi ir skaidri parādījuši, kā iepriekš nezināmas slimības var ātri izplatīties, izraisot augstu mirstību un saslimstību. Iespēja ātri ceļot, kā arī globālā tirdzniecība veicina infekcijas slimību pārnēsāšanu pāri robežām. Agrīnai atklāšanai un efektīvai saziņai un koordinācijai Eiropas un starptautiskā līmenī ir liela nozīme, lai kontrolētu šādus riskus un novērstu nopietnu kaitējumu.

ABRS ir centralizēts mehānisms, kurš dod iespēju savlaicīgi un droši brīdināt dalībvalstis, apmainīties ar informāciju un koordinēt reakciju uz atgadījumiem, kuri rada potenciālu veselības apdraudējumu ES.

2. PAMATNOSTĀDŅU DARBĪBAS JOMA UN MĒRĶI

ABRS pārvaldība un izmantošana atsevišķos gadījumos var ietvert personas datu apmaiņu, ja to paredz attiecīgi juridiski instrumenti (skatīt 4. iedaļu par personas datu apmaiņas juridisko pamatojumu agrās brīdināšanas un reaģēšanas sistēmā).

Personas datu apmaiņai starp kompetentām veselības aprūpes iestādēm dalībvalstīs jāatbilst noteikumiem par personas datu aizsardzību, kuri paredzēti valsts tiesību aktos, ar ko transponē Direktīvu 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti.

Tomēr, tā kā ABRS lietotāji nav datu aizsardzības eksperti un ne vienmēr var būt pietiekami informēti par tiesību aktos noteiktām datu aizsardzības prasībām, ABRS lietotājiem ir ieteicams nodrošināt pamatnostādnes, kurās lietotājiem saprotamā veidā tiek skaidrota ABRS darbība no datu aizsardzības perspektīvas. Pamatnostādņu mērķis ir arī uzlabot informētību un veicināt labu praksi, kā arī saskaņotu un vienotu pieeju datu aizsardzības atbilstībai ABRS lietotāju vidū dalībvalstīs.

Tomēr jāpiemin, ka šajās pamatnostādnēs nav paredzēts sniegt vispārēju pārskatu par visiem datu aizsardzības jautājumiem saistībā ar ABRS. Turpmākus norādījumus un palīdzību var saņemt no datu aizsardzības iestādēm (turpmāk "*DPA*") dalībvalstīs. Īpaši ABRS lietotāji tiek aicināti lūgt konsultācijas attiecīgajām datu aizsardzības iestādēm par to, kā vislabāk īstenot šīs pamatnostādnes saskaņā ar valsts tiesību aktiem, lai nodrošinātu pilnīgu atbilstību valstī noteiktajām datu aizsardzības prasībām. Datu aizsardzības iestāžu saraksts un kontaktinformācija ir pieejama šādā adresē:

http://ec.europa.eu/justice/policies/privacy/nationalcomm/index_en.htm

Visbeidzot jāuzsver, ka šīs pamatnostādnes nav autentiska ES Likuma par datu aizsardzību interpretācija, jo Savienības institucionālajā sistēmā uzdevums interpretēt ES tiesību aktus ir piešķirts tikai Tiesai.

3. PIEMĒROJAMIE TIESĪBU AKTI UN UZRAUDZĪBA

Piemērojamie tiesību akti ir atkarīgi no tā, kas ir ABRS lietotājs. Personas datu apstrādi, ko Komisija un *ECDC* veic saistībā ar sistēmas pārvaldību un darbību (nākamajās iedaļās minētajā apjomā), regulē saskaņā ar Regulu (EK) Nr. 45/2001.

([1]) *ECDC* arī atbalsta Komisiju un palīdz tai uzturēt ABRS lietojumprogrammu. Šo uzdevumu *ECDC* saņēma saskaņā ar Eiropas Parlamenta un Padomes 2004. gada 21. aprīļa Regulu (EK) Nr. 851/2004, ar ko izveido Eiropas Slimību profilakses un kontroles centru un jo īpaši tās 8. pantu (OV L 142, 30.4.2004., 1. lpp.).

Attiecībā uz personas datu apstrādi, ko veic ABRS valsts kompetentās iestādes, piemērojamie tiesību akti ir attiecīgie valsts tiesību akti datu aizsardzības jomā, ar ko transponē Direktīvu 95/46/EK. Jāpiemin, ka šī direktīva paredz dalībvalstīm zināmu rīcības brīvību attiecībā uz šo noteikumu transponēšanu valsts tiesību aktos. Direktīvā dalībvalstīm ir paredzēta iespēja konkrētos gadījumos ieviest izņēmumus vai atkāpes attiecībā uz vairākiem noteikumiem. Vienlaikus ar valsts datu aizsardzības tiesību aktiem, kuru subjekts ir ABRS lietotājs, var paredzēt stingrākas vai konkrētai valstij piemērotas datu aizsardzības prasības, kuras nav noteiktas citu dalībvalstu tiesību aktos.

Ņemot vērā šīs īpatnības, ABRS lietotāji tiek aicināti apspriest šīs pamatnostādnes ar attiecīgajām datu aizsardzības iestādēm, lai nodrošinātu, ka visas valstī piemērojamo tiesību aktu prasības tiek izpildītas. Piemēram, tas, cik detalizēta informācija jāsniedz datu subjektiem datu vākšanas laikā, dažādās dalībvalstīs var ievērojami atšķirties, kā arī var būt pieņemti dažādi noteikumi attiecībā uz konkrētu personas datu (piemēram, veselības datu) kategoriju apstrādi.

Viena no galvenajām īpatnībām ES datu aizsardzības tiesiskajā regulējumā, kurš ietver Regulu (EK) Nr. 45/2001 un Direktīvu 95/46/EK, ir uzraudzība, ko veic valsts, neatkarīgas datu aizsardzības iestādes. Personas datu apstrādi, ko veic ES iestādes un struktūras, uzrauga Eiropas Datu aizsardzības uzraudzītājs (turpmāk "EDAU") ([1]), savukārt apstrādi, ko veic fiziskas vai juridiskas personas, valsts pārvaldes iestādes, aģentūras vai citas struktūras dalībvalstīs, uzrauga to attiecīgās datu aizsardzības iestādes. Uzraudzības iestādes visās dalībvalstīs ir pilnvarotas izskatīt iedzīvotāju iesniegtās sūdzības par viņu tiesību un brīvību aizsardzību attiecībā uz personas datu apstrādi. Lai saņemtu sīkāku informāciju par to, kā izskatīt datu subjektu prasības vai sūdzības, ABRS lietotāji tiek aicināti skatīt 9. iedaļu par piekļuvi personas datiem un citām datu subjektu tiesībām.

4. PERSONAS DATU APMAIŅAS JURIDISKAIS PAMATOJUMS AGRĀS BRĪDINĀŠANAS UN REAĢĒŠANAS SISTĒMĀ (ABRS)

Lēmumā Nr. 2119/98/EK tika paredzēts izveidot tīklu ES līmenī (turpmāk "tīkls"), lai ar Komisijas palīdzību veicinātu sadarbību un koordināciju starp dalībvalstīm nolūkā uzlabot infekcijas slimību profilaksi un kontroli ES ([2]). Šajā saistībā ABRS tika izveidota kā viens no tīkla pīlāriem, kas dod iespēju nodrošināt informācijas apmaiņu, konsultācijas un koordināciju Eiropas līmenī situācijās, kad notiek infekcijas slimību izraisīti atgadījumi, kuri rada iespējamus draudus sabiedrības veselībai Eiropas Savienībā.

Jāpiemin, ka ne visa informācijas apmaiņa, kura notiek ABRS, ir saistīta ar personas datiem. Faktiski šajā sistēmā nenotiek apmaiņa ar identificētu vai identificējamu fizisku personu veselības datiem vai citiem peronas datiem.

Kas ir "personas dati"?

Direktīvas 95/46/EK un Regulas (EK) Nr. 45/2001 nozīmē personas dati ir jebkāda informācija, kas attiecas uz identificētu vai identificējamu fizisku personu ("datu subjektu"); identificējama persona ir tāda persona, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikācijas numuru vai vienu vai vairākiem šai personai raksturīgiem fiziskās, fizioloģiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem ([3]).

Kompetentās veselības aprūpes iestādes EEZ dalībvalstīs, izmantojot ABRS, tīklam cita starpā lielākoties paziņo informāciju par infekcijas slimību parādīšanās vai atjaunošanās gadījumiem, kā arī informāciju par piemērotajiem kontroles pasākumiem vai informāciju par neparastiem epidēmiskiem simptomiem vai nezināmas izcelsmes jaunām infekcijas slimībām ([4]), kuru izplatības risku ES var novērst, dalībvalstīm veicot savlaicīgas un saskaņotas darbības ([5]). Pamatojoties uz informāciju, kura pieejama tīklā, dalībvalstis saziņā ar Komisiju savā starpā apspriedīsies, lai koordinētu rīcību attiecībā uz šo slimību profilaksi un kontroli, tostarp attiecībā uz pasākumiem, kurus tās ir pieņēmušas vai plāno pieņemt valsts līmenī ([6]).

Tomēr dažos gadījumos informācijas apmaiņa sistēmā faktiski skar atsevišķas personas un minēto informāciju var uzskatīt par personas datiem.

Pirmkārt, sistēmas pārvaldībā un darbībā ir paredzēta ABRS pilnvarotu lietotāju ierobežota personas datu apjoma apstrāde. Lietotāju kontaktinformācijas (vārds, uzvārds, organizācija, e-pasta adrese, tālruņa numurs u. c.) apstrādei ir liela nozīme, lai izveidotu un vadītu sistēmu. Dalībvalstis Komisijas pārraudzībā vāc šos personas datus un veic to turpmāku apstrādi tikai tādēļ, lai efektīvi sadarbotos saistībā ar ABRS pārvaldību un esošo tīklu.

([1]) http://www.edps.europa.eu/EDPSWEB/edps/EDPS.
([2]) Tīklā ietvertas tikai tās infekcijas slimību kategorijas, kuras uzskaitītas Lēmuma Nr. 2119/98/EK pielikumā.
([3]) Direktīvas 95/46/EK 2. panta a) apakšpunkts un Regulas (EK) Nr. 45/2001 2. panta a) apakšpunkts.
([4]) Lēmuma Nr. 2119/98/EK 4. pants.
([5]) Lēmuma 2000/57/EK I pielikums par "atgadījumiem", par ko jāziņo agrās brīdināšanas un reaģēšanas sistēmā.
([6]) Lēmuma Nr. 2119/98/EK 6. pants.

Vēl svarīgāk – notiekot atgadījumam saistībā ar infekcijas slimībām, kuras, iespējams, varētu izplatīties ES, skartajām dalībvalstīm, savstarpēji sadarbojoties, var būt jāīsteno konkrēti kontroles pasākumi, tā sauktie "kontaktu izsekošanas" pasākumi, lai noteiktu inficētās personas un iespējami apdraudētās personas, kā arī novērstu nopietnu infekcijas slimību pārnēsāšanu. Šāda sadarbība var ietvert ar apstiprinātiem vai iespējamiem cilvēku saslimšanas gadījumiem saistītu personas datu apmaiņu agrās brīdināšanas un reaģēšanas sistēmā, tostarp konfidenciālu veselības datu apmaiņu starp dalībvalstīm, kuras tieši iesaistītas kontaktu izsekošanas pasākumos ([1]).

Kas ir "personas datu apstrāde"?

Direktīvas 95/46/EK un Regulas (EK) Nr. 45/2001 nozīmē "personas datu apstrāde ir jebkura ar personas datiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, datu vākšana, reģistrēšana, organizēšana, uzglabāšana, piemērošana vai pārveidošana, atgūšana, apskatīšana, izmantošana, atklāšana, izmantojot nosūtīšanu, izplatīšana vai to atklāšana citādā veidā, saskaņošana, savienošana, piekļuves noslēgšana, dzēšana vai iznīcināšana" ([2]).

Iepriekš minētajos gadījumos personas datu apstrāde agrās brīdināšanas un reaģēšanas sistēmā jāattaisno ar konkrētu juridisku pamatojumu. Šajā saistībā Direktīvas 95/46/EK 7. pantā un Regulas (EK) Nr. 45/2001 5. panta atbilstošajos noteikumos ir paredzēti kritēriji likumīgas datu apstrādes nodrošināšanai.

Attiecībā uz ABRS lietotāju kontaktinformāciju šo datu apstrādes pamatā ir:

— Regulas (EK) Nr. 45/2001 5. panta b) apakšpunkts: "apstrāde ir vajadzīga, lai ievērotu juridiskus pienākumus, kas jāpilda par apstrādi atbildīgajai personai [([3])]". Apstrāde ir vajadzīga ABRS pārvaldībai un darbībai, ko veic Komisija ar *ECDC* atbalstu,

— Regulas (EK) Nr. 45/2001 5. panta d) apakšpunkts: "datu subjekti ir nepārprotami devuši savu piekrišanu". Lietotāju kontaktinformācija tiek iegūta no pašiem datu subjektiem pēc tam, kad tie ir izteikuši skaidru piekrišanu savu personas datu apstrādei agrās brīdināšanas un reaģēšanas sistēmā (skatīt 8. iedaļu par informācijas sniegšanu datu subjektiem).

Direktīvas 95/46/EK 7. panta c), d) un e) apakšpunktā paredzētie kritēriji ir visatbilstošākie personu kontaktu izsekošanas datu apmaiņai agrās brīdināšanas un reaģēšanas sistēmā (piemēram, inficēto personu kontaktinformācija, informācija par izmantoto satiksmes līdzekli un citi ar personas ceļojuma maršrutu un apmešanās vietām saistīti dati, informācija par apmeklētajām personām un personām, kuras iespējami pakļautas inficēšanai) ([4]):

— Direktīvas 95/46/EK 7. panta c) apakšpunkts: "apstrāde vajadzīga, lai izpildītu uz personas datu apstrādātāju attiecināmas juridiskas saistības". Lēmumā Nr. 2119/98/EK ir paredzēts izveidot agrās brīdināšanas un reaģēšanas sistēmu infekcijas slimību profilaksei un kontrolei ES. Ar šo lēmumu dalībvalstīm paredz pienākumu, izmantojot ABRS, iesniegt datus par konkrētiem atgadījumiem, kurus izraisījušas infekcijas slimības, kas apdraud vai iespējami var apdraudēt sabiedrības veselību ([5]). Pienākums iesniegt datus ietver arī pasākumus, ko veic attiecīgo dalībvalstu kompetentās iestādes, lai novērstu un apturētu šo slimību izplatību, tostarp kontaktu izsekošanas pasākumus, kurus īsteno, lai izsekotu inficētās personas vai personas, kurām iespējami draud inficēšanās ([6]),

— Direktīvas 95/46/EK 7. panta d) apakšpunkts: "apstrāde vajadzīga, lai aizsargātu datu subjekta būtiskas intereses". Principā apmaiņa ar inficēto personu un personu, kuras nenovēršami ir pakļautas inficēšanās riskam, personas datiem starp attiecīgajām dalībvalstīm ir vajadzīga, lai nodrošinātu šīm personām atbilstošu aprūpi vai ārstēšanu, kā arī ļautu izsekot un identificēt tās ar mērķi izolēt un noteikt karantīnu, lai aizsargātu attiecīgo personu un līdz ar to arī visu ES iedzīvotāju veselību,

— Direktīvas 95/46/EK 7. panta e) apakšpunkts: "apstrāde vajadzīga sabiedrības interesēs realizējama uzdevuma izpildei vai personas datu apstrādātājam vai trešajai personai, kurai dati tiek atklāti, piešķirto oficiālo pilnvaru realizācijai". ABRS ir instruments, kurš izstrādāts, lai palīdzētu dalībvalstīm koordinēt pasākumus nopietnu infekcijas slimību profilaksei un kontrolei ES. Tāpēc šī sistēma ir izveidota, lai sekmētu sabiedrības interešu īstenošanu dalībvalstīs nolūkā aizsargāt sabiedrības veselību.

([1]) Personas datu apstrādes agrās brīdināšanas un reaģēšanas sistēmā likumīgo nolūku skaidrošana, lai iekļautu "kontaktu izsekošanas" datus, notika līdz ar Komisijas Lēmumā 2000/57/EK ieviestajiem grozījumiem, kurus veica ar Lēmumu 2009/547/EK.
([2]) Direktīvas 95/46/EK 2. panta b) apakšpunkts un Regulas (EK) Nr. 45/2001 2. panta b) apakšpunkts.
([3]) Termina "par apstrādi atbildīgā persona" jeb "personas datu apstrādātājs" definīciju skatīt 5. iedaļā.
([4]) To personas datu indikatīvs saraksts, kuru apmaiņu var veikt kontaktu izsekošanas vajadzībām, pievienots kā pielikums Lēmumam 2009/547/EK.
([5]) Lēmuma 2000/57/EK 1. pants un I pielikums par to "atgadījumu" definīciju, par kuriem jāziņo agrās brīdināšanas un reaģēšanas sistēmā.
([6]) Lēmuma 2000/57/EK 2.a pants, kas ieviests ar Lēmumu 2009/547/EK.

Ar sabiedrības interesēm var attaisnot arī gadījumus, kad dalībvalstis agrās brīdināšanas un reaģēšanas sistēmā apstrādā konfidenciālus veselības datus (piemēram, informācija par atgadījumu, kas rada veselības apdraudējumu, dati par inficēto personu un to personu veselības stāvokli, kas potenciāli pakļautas inficēšanās draudiem). Lai gan saskaņā ar Direktīvas 95/46/EK 8. panta 1. punktu veselības datu apstrāde principā ir aizliegta, uz šīs konkrētās datu kategorijas apstrādi agrās brīdināšanas un reaģēšanas sistēmā attiecas izņēmums, kas paredzēts saskaņā ar minētās direktīvas 8. panta 3. punktu, ciktāl apstrādi "pieprasa profilaktiskās medicīnas, medicīniskas diagnozes, aprūpes vai ārstēšanas vai veselības aprūpes pakalpojumu pārvaldības nodrošināšanas nolūkiem un ja šos datus apstrādā veselības aizsardzības darba profesionālis saskaņā ar attiecīgās valsts tiesībām vai valsts kompetento iestāžu ieviestiem noteikumiem par dienesta noslēpuma pienākumu vai cita persona, uz kuru arī attiecas tāds pat pienākums ievērot slepenību".

Papildu izņēmumus attiecībā uz aizliegumu apstrādāt personas veselības datus var paredzēt būtisku sabiedrības interešu gadījumos un, veicot atbilstīgus drošības pasākumus, saskaņā ar dalībvalstu tiesību aktiem vai valsts datu aizsardzības iestāžu lēmumu dalībvalstīs ([1]).

5. KAS IR KAS AGRĀS BRĪDINĀŠANAS UN REAĢĒŠANAS SISTĒMĀ? KOPĪGAS PĀRBAUDES TIESĪBU PIEŠĶIRŠANA

ABRS ir iecerēta kā vairāku lietotāju sistēma, kuri sazinās, izmantojot attiecīgus tehniskus līdzekļus, tostarp dažādus strukturētus saziņas kanālus, noteiktas kontaktpersonas no kompetentām valsts veselības aprūpes iestādēm EEZ dalībvalstīs (turpmāk "valsts ABRS kontaktpunkti"), Komisijas, *ECDC* un nelielā apmērā arī no PTO.

Katrs no minētajiem ABRS dalībniekiem ir atsevišķs sistēmas lietotājs, lai gan piekļuve informācijas apmaiņai sistēmā ir modulēta, izveidojot dažādus lietotāju profilus un "selektīvus" saziņas kanālus, kuros paredzēti atbilstoši aizsardzības pasākumi, lai nodrošinātu atbilstību piemērojamiem datu aizsardzības noteikumiem.

Sistēma ietver divus galvenos saziņas kanālus. Pirmais kanāls, tā sauktais "vispārīgais ziņojumu apmaiņas" kanāls, ļauj kompetentai veselības aprūpes iestādei attiecīgajā dalībvalstī paziņot visiem valsts ABRS kontaktpunktiem, Komisijai, *ECDC* un PTO informāciju par atgadījumiem, kurus izraisījušas infekcijas slimības, kas, iespējams, varētu izplatīties ES, un kuri ir ietverti Lēmumā Nr. 2119/98/EK paredzētajos ziņošanas pienākumos ([2]).

Kopumā, izmantojot vispārīgo ziņojumu apmaiņas kanālu, netiek veikta identificētu vai identificējamu fizisku personu ar veselību saistītas informācijas vai citu personas datu paziņošana. Sistēmā ir ieviesti īpaši aizsardzības pasākumi, lai novērstu nelikumīgu datu apstrādi šajā kanālā (skatīt 7. iedaļu).

Tomēr situācijās, kad notiek tādu infekcijas slimību izraisīti atgadījumi, kas, iespējams, varētu izplatīties ES, skartajām dalībvalstīm, savstarpēji sadarbojoties, var būt jāīsteno noteikti kontaktu izsekošanas pasākumi, kuru mērķis ir izsekot inficētās personas un citas personas, kas pakļautas inficēšanās draudiem, lai novērstu šo nopietno slimību izplatību.

Lai nodrošinātu atbilstību datu aizsardzības noteikumiem, ir ieviesti atbilstoši aizsardzības pasākumi, kuri ļauj veikt apmaiņu ar personu kontaktu izsekošanas un veselības datiem tikai tajās dalībvalstīs, kas tieši iesaistītas attiecīgajā kontaktu izsekošanas procedūrā, un liegt citām tīkla dalībvalstīm, Komisijai un *ECDC* piekļuvi šiem datiem ([3]).

Tāpēc agrās brīdināšanas un reaģēšanas sistēmā ir izveidots tā sauktais "selektīvais ziņojumu apmaiņas" kanāls, lai nodrošinātu īpašu saziņas kanālu starp attiecīgajām dalībvalstīm, kas iesaistītas konkrētajā kontaktu izsekošanas pasākumā.

Veicot personas datu apmaiņu selektīvajā ziņojumu apmaiņas kanālā, kompetentās iestādes kļūst par "personas datu apstrādātāju" attiecībā uz šo personas datu apstrādi un tādējādi uzņemas atbildību par šo apstrādes darbību likumību un par to, lai tiktu nodrošināta atbilstība datu aizsardzības saistībām, kas noteiktas piemērojamos valsts tiesību aktos, ar kuriem transponē Direktīvu 95/46/EK.

([1]) Kā paredzēts Direktīvas 95/46/EK 8. panta 4. punktā.
([2]) Sal. jo īpaši tā 4., 5. un 6. pantu.
([3]) Lēmuma 2000/57/EK 2.a pants, kas ieviests ar Lēmumu 2009/547/EK.

Kas ir "personas datu apstrādātājs"?

Direktīvas 95/46/EK nozīmē "personas datu apstrādātājs ir fiziska vai juridiska persona, valsts iestāde, aģentūra vai jebkura cita institūcija, kura viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus" ([1]).

Principā lietotājiem Komisijā un *ECDC* nav piekļuves personas datiem, kuru apmaiņu veic selektīvajā ziņojumu apmaiņas kanālā ([2]). Tomēr tehnisku iemeslu dēļ par centrālo datu uzglabāšanu ABRS atbild tikai Komisija, kas darbojas kā sistēmas administratore un koordinatore. Pildot šos pienākumus, Komisija ir atbildīga arī par ABRS pilnvaroto lietotāju personas datu reģistrāciju, uzglabāšanu un turpmāku apstrādi, kas nepieciešama, lai nodrošinātu sistēmas darbību.

Tāpēc ABRS ir uzskatāms kopīgas pārbaudes tiesību piemērs, kur atbildība par datu aizsardzības nodrošināšanu tiek sadalīta dažādos līmeņos starp Komisiju un dalībvalstīm. Turklāt Komisija un dalībvalstis, kas kopš 2005. gada pilda savus pienākumus kā personas datu līdzapstrādātājas, ABRS informātikas lietojumprogrammu ikdienas darbības nodrošināšanu ir nolēmušas deleģēt *ECDC*, kurš veic šo uzdevumu Komisijas vārdā. Pēc minētās deleģēšanas aģentūra kā "apstrādātāja" uzņēmās atbildību nodrošināt sistēmā veikto apstrādes darbību konfidencialitāti un drošību saskaņā ar saistībām, kuras paredzētas Regulas (EK) Nr. 45/2001 21. un 22. pantā.

Kas ir "apstrādātājs" un kādas ir tā saistības?

Regulas (EK) Nr. 45/2001 nozīmē "apstrādātājs ir fiziska vai juridiska persona, valsts iestāde, aģentūra vai cita struktūra, kas apstrādā personas datus par apstrādi atbildīgās personas uzdevumā" ([3]).

Regulā paredzēts: ja apstrādes darbības veic par apstrādi atbildīgās personas uzdevumā, tā izvēlas apstrādātāju, kurš sniedz pietiekamas garantijas attiecībā uz tehniskajiem un organizatoriskajiem pasākumiem, kas vajadzīgi datu drošības nolūkā. Par to, lai tiktu ievērota atbilstība šiem pasākumiem, atbild tikai par apstrādi atbildīgā persona. Tomēr regulas 21. un 22. pantā noteiktie pienākumi attiecībā uz apstrādes konfidencialitāti un drošību ir saistoši arī apstrādātājam ([4]).

6. PIEMĒROJAMIE DATU AIZSARDZĪBAS PRINCIPI

Personas datu apstrādei agrās brīdināšanas un reaģēšanas sistēmā jāatbilst datu aizsardzības principiem, kas noteikti Regulā (EK) Nr. 45/2001 un Direktīvā 95/46/EK.

Pildot savus pienākumus kā personas datu apstrādātājas, Komisija un dalībvalstu kompetentās iestādes ir atbildīgas par to, ka tiek nodrošināta atbilstība šiem principiem katru reizi, kad tiek apstrādāti personas dati agrās brīdināšanas un reaģēšanas sistēmā. Turpmāk ir uzskaitīti datu aizsardzības pamatprincipi. Tie neskar citas piemērojamās datu aizsardzības prasības, kas noteiktas attiecīgajos juridiskajos instrumentos, par kuriem norādījumi ir doti saskaņā ar šo pamatnostādņu dažādām iedaļām. ABRS lietotāji tiek aicināti rūpīgi izlasīt 8. iedaļu par informācijas sniegšanu datu subjektiem un 9. iedaļu par piekļuvi un citām datu subjektu tiesībām.

6.1. *Apstrādes likumības un mērķa ierobežošanas principi*

Personas datu apstrādātājiem būtu jānodrošina, ka personas dati tiek apstrādāti godprātīgi un likumīgi. Šis princips, pirmkārt, paredz, ka personas datu vākšana un turpmāka apstrāde jāveic saskaņā ar tiesību aktos noteiktu tiesisko pamatojumu ([5]). Otrkārt, personas dati jāvāc tikai konkrētam, precīzi formulētam un likumīgam nolūkam un tos nedrīkst turpmāk apstrādāt veidos, kuri neatbilst minētajam nolūkam ([6]).

([1]) Definīcija ietverta Direktīvas 95/46/EK 2. panta d) apakšpunktā.

([2]) Ārkārtas apstākļos Komisija var tikt iekļauta personas datu apmaiņā, izmantojot ABRS selektīvo kanālu, ja ir absolūti nepieciešams koordinēt vai dot iespēju savlaicīgi un efektīvi īstenot valsts veselības aprūpes pasākumus, kuri noteikti saskaņā ar Lēmumu Nr. 2119/98/EK un tā īstenošanas noteikumiem. Šajos gadījumos Komisija nodrošinās, ka apstrāde ir likumīga un ka tā tiek veikta atbilstīgi Regulas (EK) Nr. 45/2001 noteikumiem.

([3]) Definīcija ietverta Regulas (EK) Nr. 45/2001 2. panta e) apakšpunktā.

([4]) Šie principi ir paredzēti Regulas (EK) Nr. 45/2001 23. panta 1. punktā par personas datu apstrādi par apstrādi atbildīgo personu uzdevumā.

([5]) Apstrādes rezultātu likumības princips paredzēts Direktīvas 95/46/EK 6. panta 1. punkta a) apakšpunkta, 7. panta un 8. panta kopīgajos noteikumos. Sal. arī Regulas (EK) Nr. 45/2001 atbilstošos noteikumus.

([6]) Mērķa ierobežojuma princips tiek formulēts Direktīvas 95/46/EK 6. panta 1. punkta b) apakšpunktā un Regulas (EK) Nr. 45/2001 4. panta 1. punkta b) apakšpunkta atbilstošajā noteikumā.

6.2. *Datu kvalitātes principi*

Personas datu apstrādātājiem jānodrošina, ka personas dati ir adekvāti, atbilstīgi un ne pārlieku apjomīgi attiecībā pret nolūkiem, kādiem tos vāc. Turklāt datiem jābūt precīziem un atjauninātiem ([1]).

6.3. *Datu glabāšanas principi*

Personas datu apstrādātājiem jānodrošina, ka dati tiek glabāti formā, kas ļauj identificēt datu subjektus ne ilgāk, kā vajadzīgs nolūkiem, kādos dati ir savākti vai kādos tos pēc tam apstrādā ([2]).

6.4. *Konfidencialitātes un datu drošības principi*

Personas datu apstrādātājiem jānodrošina, ka jebkura persona, darbojoties saskaņā ar personas datu apstrādātāja vai apstrādātāja pilnvarām, ieskaitot pašu apstrādātāju, kam ir piekļuve personu datiem, nedrīkst apstrādāt šos datus citādi, kā pēc personas datu apstrādātāja norādījumiem ([3]). Turklāt personas datu apstrādātājiem jāīsteno tehniski un organizatoriski pasākumi, lai aizsargātu personas datus pret nejaušu, neatļautu vai nelikumīgu iznīcināšanu vai pazaudēšanu, pārveidošanu, atklāšanu vai piekļuvi un pret visām citām nelikumīgām apstrādes formām ([4]).

Lai, izmantojot sistēmas, pareizi un efektīvi tiktu piemēroti iepriekš minētie principi, ABRS lietotāji tiek aicināti veikt turpmāk minētās darbības.

Lai pārliecinātos, ka apstrādes darbībai ir juridisks pamatojums, ka dati tiek vākti precīzi formulētos un likumīgos nolūkos un ka tie turpmāk netiek apstrādāti veidos, kuri neatbilst minētajam nolūkam, katru reizi, vācot vai citādi apstrādājot personas datus agrās brīdināšanas un reaģēšanas sistēmā, ABRS lietotājiem:

— izvērtējot katru gadījumu atsevišķi, vajadzētu novērtēt, vai koordinētu kontaktu izsekošanas pasākumu īstenošana un turpmāka ABRS selektīvā kanāla aktivizēšana, lai apmainītos ar attiecīgajiem kontaktu izsekošanas un citiem personas datiem, ir attaisnota, pamatojot to ar slimības būtību un zinātniski apstiprinātām kontaktu izsekošanas priekšrocībām turpmākā slimības izplatības profilaksē vai samazināšanā, ņemot vērā dalībvalstu veselības aprūpes iestāžu un esošo zinātnisko aģentūru, proti, *ECDC* un PTO, sniegto riska novērtējumu,

— nevajadzētu izmantot vispārīgo ziņojumu apmaiņas kanālu, lai apmainītos ar kontaktu izsekošanas un citiem personas datiem. Tiem būtu jānodrošina, ka šādi dati netiek ietverti nosūtāmo vispārīgo ziņojumu tekstos, to pielikumos vai jebkuros citos dokumentos. Vispārīgu ziņojumu apmaiņas kanāla izmantošana kontaktu izsekošanas nolūkā jāuzskata par nelikumīgu un nesamērīgu, jo tā rezultātā personas dati tiek atklāti saņēmējiem (tostarp Komisijai un *ECDC*), uz kuriem minētā kontaktu izsekošanas procedūra neattiecas un kuriem nav vajadzības piekļūt šiem datiem,

— izmantojot selektīvo funkciju, vajadzētu pieņemt pieeju "vajadzība zināt" un atlasīt tikai tādas dalībvalstu kompetentās iestādes, kas saņem selektīvus ziņojumus, kuri ietver personas datus, un sadarbojas minētajā kontaktu izsekošanas procedūrā.

ABRS lietotājiem jābūt īpaši piesardzīgiem, kad tie, izmantojot selektīvo ziņojumu apmaiņas kanālu, apmainās ar konfidenciāliem datiem par identificēto vai identificējamo personu veselības stāvokli, piemēram, inficētām personām vai personām, kas iespējami pakļautas inficēšanai, kuru kontaktinformācija vai citi personas dati tiek atklāti, izmantojot ABRS tādā veidā, ka attiecīgo personu var tieši vai netieši identificēt. Šajā gadījumā visus iepriekš minētos ieteikumus jāturpina piemērot; turklāt ABRS lietotājiem jāielāgo, ka konfidenciālu datu apmaiņa saskaņā ar Direktīvu 95/46/EK ir atļauta tikai nedaudzos gadījumos. Jo īpaši turpmāk minētajos gadījumos ([5]):

— persona, kuras dati tiek vākti, ir devusi savu precīzi formulētu piekrišanu to apstrādei (Direktīvas 95/46/EK 8. panta 2. punkta a) apakšpunkts). Tomēr, ja rodas vajadzība savlaicīgi iejaukties sanitārās ārkārtas situācijās, prasība par datu subjektu nodrošināšanu ar visu informāciju par iespēju sniegt apzinātu piekrišanu var kļūt neiespējama (skatīt 8. iedaļu par informācijas sniegšanu datu subjektiem). Turklāt informācijas vākšanas laikā ne vienmēr ir zināms, ka dati tiks atklāti agrās brīdināšanas un reaģēšanas sistēmā,

([1]) Direktīvas 95/46/EK 6. panta 1. punkta c) un d) apakšpunkts un Regulas (EK) Nr. 45/2001 4. panta 1. punkta c) un d) apakšpunkts.
([2]) Direktīvas 95/46/EK 6. panta 1. punkta e) apakšpunkts un Regulas (EK) Nr. 45/2001 4. panta 1. punkta e) apakšpunkts.
([3]) Konfidencialitātes princips ir paredzēts Direktīvas 95/46/EK 16. pantā un Regulas (EK) Nr. 45/2001 21. panta atbilstošajā noteikumā.
([4]) Datu drošības princips ir formulēts Direktīvas 95/46/EK 17. pantā un Regulas (EK) Nr. 45/2001 22. panta atbilstošajā noteikumā.
([5]) Visu izņēmumu sarakstu attiecībā uz aizliegumu apstrādāt konkrētas datu kategorijas, tostarp veselības datus, skatīt Direktīvas 95/46/EK 8. panta 2., 3., 4., 5. punktā.

— bez datu subjektu piekrišanas veselības datu apstrādi var uzskatīt par likumīgu, ja "datu apstrādi pieprasa profilaktiskās medicīnas, medicīniskas diagnozes, aprūpes vai ārstēšanas vai veselības aprūpes pakalpojumu pārvaldības nodrošināšanas nolūkiem", ja veselības datus apstrādā veselības aizsardzības darba profesionālis, uz kuru attiecas pienākums glabāt dienesta noslēpumu, vai cita persona, uz kuru attiecas tāds pats pienākums (Direktīvas 95/46/EK 8. panta 3. punkts). Citiem vārdiem sakot, katru reizi sūtot citas dalībvalsts saņēmējam selektīvu ziņojumu, kurš ietver konfidenciālus veselības datus, ABRS lietotājiem jāizvērtē, vai šādu datu atklāšana ir absolūti nepieciešama, lai dotu iespēju kompetentām iestādēm attiecīgajās dalībvalstīs īstenot konkrētus pasākumus, kuri vajadzīgi vienam no iepriekš minētajiem nolūkiem. ABRS lietotājiem tiek atgādināts, ka papildu pamatojumu veselības datu apstrādei var nodrošināt attiecīgie valsts tiesību akti, ar ko transponē Direktīvu 95/46/EK, vai valsts datu aizsardzības iestādes lēmums ([1]).

Lai nodrošinātu to personas datu kvalitāti, kuru apmaiņu ABRS lietotāji veic sistēmā, un jo īpaši pirms selektīvā ziņojuma nosūtīšanas, jāizvērtē, vai:

— personas dati, kuru apmaiņu lietotāji vēlas veikt, ir absolūti nepieciešami, lai nodrošinātu kontaktu izsekošanas procedūras efektīvu īstenošanu. Citiem vārdiem runājot, kompetentai iestādei, kura sūta ziņojumu, jānodrošina iestādei citā attiecīgajā dalībvalstī tikai tie personas dati, kas ir nepieciešami, lai nepārprotami identificētu inficētās personas vai personas, kuras pakļautas inficēšanai. To personas datu indikatīvais saraksts, kuri var tikt apmainīti kontaktu izsekošanas vajadzībām, kas pievienots Lēmumam 2009/547/EK, nav uzskatāms par visaptverošu un beznosacījuma pilnvaru piešķirumu šo kategoriju datu apstrādei. Vienlaikus attiecībā uz to personas datu apstrādi, kuri nav uzskaitīti minētajā pielikumā, jāievēro stingra piesardzība, jo šo datu atklāšana, iespējams, ir pārmērīga un nepamatota. Tā vietā, izvērtējot katru gadījumu atsevišķi, jānovērtē, vai konkrētu personas datu iekļaušana ir absolūti nepieciešama, lai īstenotu šo kontaktu izsekošanas procedūru.

Turpmāka personas datu apstrāde un uzglabāšana ārpus ABRS:

Ir ļoti svarīgi pieminēt, ka valsts datu aizsardzības tiesību aktus, ar ko transponē Direktīvu 95/46/EK, piemēro arī to personas datu uzglabāšanai un turpmākai apstrādei *ārpus* ABRS, kuri iegūti, izmantojot sistēmu. Tas var notikt, piemēram, ja personas datus, kuri sistēmā tiek glabāti centralizēti, pēc tam glabā lietotāju vietējos personālajos datoros vai datubāzēs, kuras izveidotas valsts līmenī, vai, ja kompetenta iestāde, kura atbildīga par šo datu apstrādi ABRS, nosūta tos citām iestādēm vai trešām personām. Šajos gadījumos ABRS lietotājiem tiek atgādināts, ka:

— uzglabāšana un turpmākā apstrāde ārpus ABRS nedrīkst būt pretrunā ar sākotnējo nolūku, kuram dati tika vākti un apmainīti agrās brīdināšanas un reaģēšanas sistēmā,

— šai turpmākajai apstrādei jābūt juridiskam pamatojumam attiecīgajos valsts datu aizsardzības tiesību aktos, kā arī tai jābūt vajadzīgai, adekvātai, atbilstīgai un ne pārlieku apjomīgai attiecībā pret sākotnējiem vākšanas nolūkiem agrās brīdināšanas un reaģēšanas sistēmā,

— dati ir jāatjaunina un jādzēš, tikko tie vairs nav vajadzīgi nolūkiem, kuriem tie tika turpmāk apstrādāti,

— ja dati tiek iegūti no ABRS un atklāti trešām personām, personas datu apstrādātājam par šo apstākli jāinformē datu subjekti, lai garantētu godprātīgu apstrādi, izņemot gadījumus, kad tas izrādītos neiespējami vai radītu nesamērīgas pūles, vai ja datu atklāšana ir konkrēti noteikta tiesību aktos (skatīt Direktīvas 95/46/EK 11. panta 2. punktu). Ņemot vērā, ka atklāšana var būt pieprasīta tikai vienas iesaistītās dalībvalsts tiesību aktos un tāpēc šī informācija var nebūt plaši zināma citur, jāveic pasākumi, lai nodrošinātu informāciju pat tajos gadījumos, kad datu atklāšana ir konkrēti noteikta tiesību aktos.

7. DATU AIZSARDZĪBAI DRAUDZĪGA VIDE

Lai palielinātu atbilstību 6. iedaļā izklāstītajiem datu aizsardzības principiem un veicinātu ABRS lietotāju piekļuvi datu aizsardzības aspektiem katru reizi, kad tie izmanto sistēmu, dažas funkcijas jau ir iekļautas agrās brīdināšanas un reaģēšanas sistēmā. Piemēram:

— ABRS ziņojumu pārskata lapā labi redzamā vietā parādās brīdinājums, informējot lietotājus, ka vispārīgais ziņojumu apmaiņas kanāls nav paredzēts kontaktu izsekošanas un citu personas datu izvietošanai, jo šī kanāla izmantošanas rezultātā šie dati var tikt nevajadzīgi atklāti saņēmējiem, kuriem nav nepieciešams tiem piekļūt,

— piekļuve informācijai, ar kuru apmainās sistēmā, ir modulēta, izveidojot dažādus lietotāju profilus un selektīvus saziņas kanālus, kuros paredzēti atbilstoši aizsardzības pasākumi, lai nodrošinātu atbilstību datu aizsardzības noteikumiem,

([1]) Direktīvas 95/46/EK 8. panta 4. punkts.

— ABRS selektīvais ziņojumu apmaiņas kanāls nodrošina īpašu saziņas kanālu personas datu apmaiņai tikai starp attiecīgajām dalībvalstīm. Sistēmā ir iekļauta noklusējuma izvēle, kura automātiski izslēdz Komisiju un *ECDC* no to selektīvo ziņojumu iespējamo saņēmēju saraksta, kuri ietver personas datus ([1]),

— 12 mēnešus pēc selektīvo ziņojumu nosūtīšanas sistēma automātiski dzēš visus šos ziņojumus, kuri ietver personas datus (plašāku informāciju skatīt 11. iedaļā par datu glabāšanu),

— sistēmā ir iekļauta funkcija, kas dod iespēju lietotājiem jebkurā laikā tieši mainīt vai dzēst tos selektīvos ziņojumus, kuri ietver personas datus un ir neprecīzi, nav atjaunināti, nav vairs vajadzīgi vai citādi neatbilst datu aizsardzības prasībām. Sistēma automātiski paziņos citiem ABRS lietotājiem, kuri iesaistīti šajā konkrētajā selektīvajā datu apmaiņā, ka ziņojums ir izdzēsts vai tā saturs mainīts, lai nodrošinātu atbilstību datu aizsardzības noteikumiem,

— selektīvajā ziņojumu apmaiņas kanālā ir pieejams īpašs mehānisms, kurš dod iespēju šajā informācijas apmaiņā iesaistītajām valsts iestādēm sazināties un sadarboties saistībā ar piekļuvi datu subjektu pieprasījumiem, to labošanu, bloķēšanu vai dzēšanu.

Turklāt vidējā termiņā ir paredzēts, ka tiks integrēts ABRS lietojumprogrammā pieejamais mācību modulis, lai ABRS lietotājiem nodrošinātu plašus skaidrojumus par sistēmas darbību no datu aizsardzības perspektīvas. Izmantojot praktiskus piemērus, tiks atspoguļotas dažādas funkcijas un darbības, kuru mērķis ir palielināt atbilstību datu aizsardzības noteikumiem.

Komisijas nodoms ir strādāt ar dalībvalstīm, lai nodrošinātu, ka ar integrēta privātuma koncepciju tiktu sniegta informācija par šiem un turpmākiem ABRS pasākumiem no paša sākuma ([2]) un ka, pieņemot lēmumus par to, kādas informācijas apmaiņu, ar ko un saskaņā ar kādiem nosacījumiem var veikt agrās brīdināšanas un reaģēšanas sistēmā, pienācīgi tiks ņemts vērā vajadzības, proporcionalitātes, mērķa ierobežošanas un datu iespējami minimālā apjoma vākšanas princips.

8. INFORMĀCIJAS SNIEGŠANA DATU SUBJEKTIEM

Viena no galvenajām prasībām saskaņā ar ES datu aizsardzības tiesisko regulējumu ir personas datu apstrādātāja pienākums sniegt skaidru informāciju datu subjektiem par apstrādes darbībām, kuras tas plāno veikt ar personas datiem.

Saskaņā ar savu lomu ABRS koordinēšanas procesā un lai pildītu iepriekš minētās prasības ([3]), Komisija savā ABRS veltītajā tīmekļa vietnē ir padarījusi pieejamu skaidru un vispārīgu paziņojumu par personas datu aizsardzību, ņemot vērā apstrādes darbības, kuras veiktas saskaņā ar minēto Komisijas pienākumu, un darbības, ko veic kompetentās iestādes, jo īpaši kontaktu izsekošanas darbību kontekstā.

Tomēr pienākums sniegt informāciju datu subjektiem ir saistošs arī valsts kompetentajām iestādēm dalībvalstīs, pildot savus personas datu apstrādātāja pienākumus attiecīgo apstrādes darbību jomā agrās brīdināšanas un reaģēšanas sistēmā.

Kāda "informācija" valsts ABRS kompetentajām iestādēm jāsniedz datu subjektiem?

Gadījumos, kad dati tiek vākti tieši no datu subjekta, Direktīvas 95/46/EK 10. pantā norādīts, ka personas datu apstrādātājam vai tā pārstāvim jāsniedz datu subjektam, no kura ievāc datus, vismaz šādu informāciju, izņemot gadījumus, kad datu subjektam tā jau ir:

a) par personas datu apstrādātāja un viņa pārstāvja, ja tāds ir, identitāti;

([1]) Lai gan ABRS lietotājiem ir iespēja izmantot šo kanālu selektīvai informācijas apmaiņai attiecībā uz tehniskiem jautājumiem, kuri neietver personas datu nosūtīšanu. Ja noklusētās izvēles vietā izraugās alternatīvo izvēli, iestāde, kura nosūta ziņojumu, var atlasīt Komisiju un *ECDC* kā saņēmējus. Šī funkcija ir iekļauta sistēmā, lai ņemtu vērā Komisijas institucionālo nozīmi riska un atgadījumu pārvaldības jautājumu koordinācijā un *ECDC* nozīmi riska novērtēšanā.

([2]) Saskaņā ar integrēta privātuma principu informācijas un komunikācijas tehnoloģijas (IKT) jāizstrādā un jāpilnveido, ņemot vērā privātuma un datu aizsardzības prasības no tehnoloģijas izveides sākuma un visos attīstības posmos.

([3]) Komisijai ir saistošs informēšanas pienākums, kura pamatā ir Regulas (EK) Nr. 45/2001 11. un 12. pants.

b) apstrādes nolūki, kuriem dati ir paredzēti;

c) jebkāda papildu informācija, piemēram:

— datu saņēmēji vai datu saņēmēju kategorijas,

— vai atbildes uz jautājumiem ir obligātas vai brīvprātīgas, kā arī atbildes nesniegšanas iespējamās sekas,

— tiesības piekļūt datiem un tiesības labot savus datus,

ciktāl šāda papildu informācija vajadzīga, ņemot vērā konkrētos apstākļus, kādos dati ievākti, lai nodrošinātu godprātīgu apstrādi attiecībā uz datu subjektu.

Direktīvas 95/46/EK 11. pantā uzskaitīta obligātā informācija, kura jāsniedz personas datu apstrādātājam, ja dati nav saņemti no paša datu subjekta. Šī informācija jāsniedz laikā, kad tiek veikta personas datu uzskaite vai, ja tiek paredzēta to atklāšana trešām personām, ne vēlāk kā laikā, kad dati tiek atklāti pirmo reizi ([1]).

Iepriekš minēto noteikumu ieviešanas rezultātā laikā, kad no atsevišķām personām tiek vākti personas dati (vai vēlākais laikā, kad dati pirmo reizi tiek atklāti agrās brīdināšanas un reaģēšanas sistēmā), to pasākumu pieņemšanas nolūkā, kas vajadzīgi, lai aizsargātu sabiedrības veselību saistībā ar atgadījumiem, par kuriem jāpaziņo saskaņā ar Lēmumu Nr. 2119/98/EK un tā īstenošanas noteikumiem, valsts kompetentajām iestādēm tieši datu subjektiem jāsniedz juridisks paziņojums, kurš ietver Direktīvas 95/46/EK 10. un 11. pantā uzskatīto informāciju. Paziņojumā jāietver arī īsa atsauce uz ABRS un saite uz attiecīgajiem dokumentiem un paziņojumiem par personas datu aizsardzību kompetentu iestāžu valsts tīmekļa vietnēs, kā arī Komisijas tīmekļa vietnē, kas veltīta ABRS.

Sīkāka informācija, kas jāsniedz juridiskajā paziņojumā, dažādās dalībvalstīs var ievērojami atšķirties. Konkrēti valsts tiesību akti paredz plašākas saistības personas datu apstrādātajiem, ietverot tādas papildu informācijas sniegšanu kā informācija par datu subjektu tiesībām saņemt kompensāciju, par datu uzglabāšanas un glabāšanas periodiem, par datu drošības pasākumiem u. c.

Ja rodas vajadzība savlaicīgi iejaukties sanitārās ārkārtas situācijās, prasība par datu subjektu nodrošināšanu ar informāciju par to personas datu apstrādes nolūkiem, ja dati netiek iegūti no paša datu subjekta, var kļūt neiespējama. Šajā saistībā Direktīvas 95/46/EK 11. panta 2. punktā norādīts, ka datu subjektu tiesības iesniegt informāciju var ierobežot, ja "šādas informācijas sniegšana izrādās neiespējama vai radītu nesamērīgas pūles vai ja reģistrēšanu vai atklāšanu konkrēti nosaka attiecīgās valsts tiesības. Šajos gadījumos dalībvalstis nodrošina atbilstošas garantijas."

Vispārīgi jāpiemin, ka īpašus aizliegumus vai ierobežojumus attiecībā uz datu subjektu tiesībām iesniegt informāciju var piemērot saskaņā ar valsts datu aizsardzības tiesību aktiem, ar ko transponē Direktīvu 95/46/EK ([2]). Jebkuriem šādiem valstī noteiktiem aizliegumiem vai ierobežojumiem jābūt nepārprotami minētiem paziņojumos par konfidencialitāti, ko sniedz datu subjektiem, vai paziņojumos par personas datu aizsardzību, kuri publicēti kompetento iestāžu valsts tīmekļa vietnēs.

Dalībvalstu kompetentajām iestādēm jālemj, kādā formā un kā nodot šo informāciju datu subjektiem. Tā kā lielākā daļa kompetento iestāžu veiks apstrādes darbības, kuras atšķiras no informācijas apmaiņas agrās brīdināšanas un reaģēšanas sistēmā, tās personu informēšanai var izvēlēties tādu pašu informācijas nodošanas veidu kā attiecībā uz citām apstrādes darbībām saskaņā ar valsts tiesību aktiem. Turklāt ieteicams, ka kompetentās iestādes atjaunina vai papildina privātās dzīves aizsardzības politiku vai paziņojumus par privātās dzīves aizsardzību – ja tie ir ietverti valsts tīmekļa vietnēs – ar īpašu atsauci uz personas datu apmaiņu agrās brīdināšanas un reaģēšanas sistēmā.

([1]) Minētā informācija ir izklāstīta 10. pantā, kurā tā noteikta ar papildu attiecīgo datu kategorijām. Šī informācija netiek prasīta gadījumā, ja dati tiek vākti tieši no datu subjekta, kurš ir informēts par attiecīgo datu kategorijām, kas tiek vāktas.

([2]) Direktīvas 95/46/EK 13. panta 1. punktā par atbrīvojumiem un ierobežojumiem noteikts: "Dalībvalstis var pieņemt tiesību aktus, lai ierobežotu 6. panta 1. punktā, 10. pantā, 11. panta 1. punktā, 12. pantā un 21. pantā paredzēto pienākumu un tiesību jomu, ja šāds ierobežojums ir nepieciešams aizsargpasākums: a) valsts drošībai; b) aizsardzībai; c) sabiedrības drošībai; d) kriminālsodāmu noziedzīgu nodarījumu vai reglamentētu profesiju ētikas pārkāpumu profilaksei, izziņai, atklāšanai un kriminālvajāšanai; e) dalībvalsts vai Eiropas Savienības svarīgās ekonomiskās vai finansiālās interesēs, ieskaitot monetāros, budžeta un nodokļu jautājumus; f) ar oficiālo pilnvaru realizāciju c), d) un e) apakšpunktā minētajos gadījumos pat laiku pa laikam saistītajai uzraudzībai, pārbaudei un reglamentējošām funkcijām; g) datu subjekta aizsardzībai vai citu personu tiesību un brīvību aizsardzībai."

Attiecībā uz visiem iepriekš minētajiem iemesliem ir ļoti svarīgi, ka kompetentās iestādes dalībvalstīs apspriežas ar attiecīgajām valsts datu aizsardzības iestādēm, izstrādājot standarta juridiskos paziņojumus un paziņojumus par personas datu aizsardzību saskaņā ar Direktīvas 95/46/EK 10. un 11. pantu.

9. PIEKĻUVE PERSONAS DATIEM UN CITAS DATU SUBJEKTU TIESĪBAS

Datu aizsardzības prasību (aplūkotas iepriekš 8. iedaļā) par informācijas sniegšanu datu subjektiem mērķis ir nodrošināt personas datu apstrādes darbību pārredzamību. Pārredzamība ir arī to datu subjektu piekļuves tiesību noteikumu pamatmērķis, kuri paredzēti ES datu aizsardzības juridiskos instrumentos ([1]).

Kas ir datu subjekta "tiesības piekļūt datiem"?

Personas datu apstrādātājiem jāgarantē katra datu subjekta tiesības bez pārmērīgas vilcināšanās vai izdevumiem iegūt apstiprinājumu, ka tiek vai netiek apstrādāti ar viņu saistīti personas dati, kā arī informāciju par šīs apstrādes nolūku un saņēmējiem, kuriem šie dati var tikt atklāti.

Personas datu apstrādātājiem arī jāgarantē datu subjektu tiesības labot, dzēst vai bloķēt datus, kuru apstrāde neatbilst piemērojamiem datu aizsardzības tiesību aktiem, piemēram, ja dati ir nepilnīgi vai nepareizi.

Visbeidzot, personas datu apstrādātājiem jāpaziņo trešām personām, kurām dati ir tikuši atklāti, par jebkuriem labojumiem, dzēšanu vai bloķēšanu, kas veikta pēc datu subjekta likumīgas prasības, izņemot gadījumus, kad tas nav iespējams vai rada nesamērīgas pūles.

Tā kā Komisija un dalībvalstis pilda personas datu apstrādātāja pienākumus, tās ir atbildīgas par to, lai tiktu nodrošinātas tiesības piekļūt personas datiem, kā arī labot, bloķēt un dzēst personas datus, kuri apstrādāti agrās brīdināšanas un reaģēšanas sistēmā saskaņā ar iepriekš minētiem noteikumiem.

Komisijas pienākums ir nodrošināt piekļuvi valstu ABRS kontaktpunktu personas datiem un izpildīt ar tiem saistītās labošanas, bloķēšanas un dzēšanas prasības. Valsts kontaktpunkti tiek aicināti atsaukties uz konkrētu klauzulu vispārējā paziņojumā par personas datu aizsardzību Komisijas ABRS veltītajā tīmekļa vietnē ([2]), lai saņemtu sīkāku informāciju par to, kā īstenot savas datu subjekta tiesības.

ABRS lietotāji tiek arī informēti, ka sistēmā jau ir iekļauta funkcija, kura dod iespēju tieši mainīt savus personas datus. Tomēr tos datu laukus, kuros tiek identificēts minētais ABRS lietotāja konts (lietotāja apstiprināta e-pasta adrese, konta veids u. c.), paši lietotāji nevar mainīt, lai novērstu nepilnvarotu lietotāju piekļuves risku sistēmai. Tāpēc jebkuri pieprasījumi mainīt šajos datu laukos iekļauto informāciju jāadresē personas datu apstrādātājam Komisijā, kā norādīts vispārējā paziņojumā par personas datu aizsardzību Komisijas ABRS veltītajā tīmekļa vietnē.

Tās attiecīgās kompetentās iestādes pienākums, kura veic šo selektīvās informācijas apmaiņu, ir izskatīt datu subjektu pieprasījumus par kontaktu izsekošanas, veselības un citiem personas datiem, kuru apmaiņa starp dalībvalstīm notikusi agrās brīdināšanas un reaģēšanas sistēmā. Šo pienākumu regulē to valsts datu aizsardzības tiesību aktu attiecīgie noteikumi, ar ko transponē Direktīvu 95/46/EK.

Tomēr jāpiemin, ka īpašus aizliegumus vai ierobežojumus attiecībā uz datu subjektu tiesībām piekļūt datiem, tos labot, dzēst vai bloķēt var piemērot saskaņā ar valsts datu aizsardzības tiesību aktiem, ar ko transponē Direktīvu 95/46/EK ([3]). Jebkuriem šādiem aizliegumiem vai ierobežojumiem jābūt nepārprotami minētiem paziņojumos par konfidencialitāti, ko sniedz datu subjektiem, vai paziņojumos par personas datu aizsardzību, kuri publicēti kompetento iestāžu valsts tīmekļa vietnēs. Tāpēc ABRS kontaktpunkti tiek aicināti vērsties pie savām valstu datu aizsardzības iestādēm, lai saņemtu papildu informāciju par šo jautājumu.

Tā kā ABRS ir sarežģīta sistēma un tai ir daudz lietotāju, kuri iesaistīti kopīgās apstrādes procedūrās, ir jānodrošina skaidra un vienkārša pieeja datu subjektu piekļuves tiesībām, jo datu subjekti nepārzina sistēmas darbību un tiem jārada apstākļi efektīvai tiesību īstenošanai.

([1]) Direktīvas 95/46/EK 12. pants un Regulas (EK) Nr. 45/2001 13.–18. pants.
([2]) Paziņojums par personas datu aizsardzību ir pieejams arī visiem ABRS lietotājiem no drošas iedaļas ABRS lietojumprogrammā.
([3]) Minētās Direktīvas 95/46/EK 13. panta 1. punkts.

Vēlamā pieeja būtu tāda, ka datu subjekts, kas uzskata, ka viņa personas datus apstrādā agrās brīdināšanas un reaģēšanas sistēmā, kā arī vēlas piekļūt tiem, dzēst vai labot tos, var vērsties pie jebkuras valsts kompetentās iestādes, ar kuru viņš apspriedās un/vai kura vāca viņa datus saistībā ar konkrētu atgadījumu, kurš apdraud sabiedrības veselību (piemēram, gan tās valsts iestāde, kuras pilsonis ir datu subjekts, gan tās valsts iestāde, kurā persona uzturas atgadījuma laikā), kā arī jebkurā citā iestādē, kas iesaistīta šajā informācijas apmaiņā saistībā ar kontaktu izsekošanas pasākumu īstenošanu.

Neviena kompetentā iestāde, kura iesaistīta attiecīgajā informācijas apmaiņā, nedrīkst atteikt piekļuvi informācijai, tās labošanu vai dzēšanu, pamatojoties uz to, ka tā nav ievadījusi datus agrās brīdināšanas un reaģēšanas sistēmā, vai uz to, ka datu subjektam jāvēršas citā kompetentā iestādē. Ja datu subjekta pieprasījumu saņem kompetenta iestāde, kura nav nosūtījusi sākotnējo informāciju selektīvajā apmaiņas kanālā, tad saņēmējai iestādei, izmantojot īpašo 7. iedaļā minēto mehānismu, jānosūta pieprasījums kompetentajai iestādei, kura ir nosūtījusi sākotnējo ziņojumu un kura pieņems lēmumu par pieprasījumu.

Vajadzības gadījumā pirms lēmuma pieņemšanas kompetentā iestāde, kura nosūtījusi informāciju sistēmā, var vērsties pie citas kompetentās iestādes, kas iesaistīta informācijas apmaiņā vai citādi saistīta ar datu subjekta pieprasījumu, izmantojot īpašo 7. iedaļā minēto mehānismu.

Datu subjekti būtu jāinformē arī par to, ka gadījumā, ja viņi nav apmierināti ar saņemto atbildi, viņi var vērsties pie citas informācijas apmaiņā iesaistītās kompetentās iestādes. Jebkurā gadījumā datu subjektiem ir tiesības iesniegt sūdzību kādai no šo kompetento iestāžu valsts datu aizsardzības iestādēm, kura tiem ir vislabāk piemērota. Vajadzības gadījumā valsts datu aizsardzības iestādēm ir jāsadarbojas savā starpā, lai izskatītu minēto sūdzību (Direktīvas 95/46/EK 28. pants).

Visbeidzot pēc konkrētiem EDAU atzinumā paustiem ieteikumiem Komisija agrās brīdināšanas un reaģēšanas sistēmā ir ieviesusi jaunu funkciju, lai dotu iespēju datu aizsardzības atbilstības nolūkā veikt to selektīvo ziņojumu labošanu un dzēšanu, kuri ietver nepareizus, neatjaunotus personas datus, kā arī datus, kuri vairs nav vajadzīgi vai citādi neatbilst datu aizsardzības prasībām.

10. DATU DROŠĪBA

Sistēmai var piekļūt tikai pilnvaroti lietotāji no Komisijas un *ECDC*, kā arī oficiāli apstiprināti ABRS valstu kontaktpunkti. Piekļuvi aizsargā, izmantojot drošu un personalizētu lietotāju kontu un paroli.

Personas datu apstrādes procedūras agrās brīdināšanas un reaģēšanas sistēmā nosaka saskaņā ar Regulas (EK) Nr. 45/2001 21. un 22. pantā norādītajām prasībām.

11. DATU GLABĀŠANA

Saskaņā ar datu aizsardzības prasībām Regulas (EK) Nr. 45/2001 4. panta 1. punkta e) apakšpunktā un Direktīvas 95/46/EK 6. panta 1. punkta e) apakšpunktā 12 mēnešus pēc selektīvo ziņojumu nosūtīšanas sistēma automātiski dzēsīs visus ziņojumus, kuri ietver personas datus.

Tomēr, ņemot vērā to, ka par savām apstrādes darbībām selektīvajā ziņošanas kanālā atbildīgi ir tikai ABRS lietotāji, šis sistēmā integrētais aizsardzības pasākums neatbrīvo lietotājus no pienākuma pirms noklusējumā paredzētā viena gada termiņa beigām izņemt no sistēmas tādus personas datus, kuri turpmāk vairs nav vajadzīgi.

Tāpēc Komisija agrās brīdināšanas un reaģēšanas sistēmā ir ieviesusi jaunu funkciju, lai dotu iespēju lietotājiem jebkurā laikā tieši dzēst tos selektīvos ziņojumus, kuri ietver personas datus, kas vairs nav vajadzīgi.

Visbeidzot jāatceras, ka valsts kompetentās iestādes ir atbildīgas par to savu datu aizsardzības noteikumu ievērošanu personas datu glabāšanas jomā, kuri noteikti attiecīgajos tiesību aktos, ar ko transponē Direktīvu 95/46/EK. Automātiska sistēmā glabāto personas datu dzēšana pēc viena gada neliedz ABRS lietotājiem noteikt atšķirīgu (piemēram, ilgāku) minētās informācijas uzglabāšanas termiņu ārpus ABRS, ja to veic saskaņā ar saistībām, kuras paredzētas valsts attiecīgajos datu aizsardzības tiesību aktos, un ja valsts tiesību aktos paredzētie termiņi atbilst Direktīvas 95/46/EK 6. panta 1. punkta e) apakšpunktā noteiktajām prasībām.

12. SADARBĪBA AR VALSTS DATU AIZSARDZĪBAS IESTĀDĒM

Kompetentās iestādes tiek mudinātas vērsties attiecīgajās valsts datu aizsardzības iestādēs, īpaši, ja tās saskaras ar problēmām, kas saistītas ar datu aizsardzību, bet nav ietvertas šajās pamatnostādnēs.

Tāpat kompetentām iestādēm jābūt informētām, ka saskaņā ar to valsts tiesību aktu noteikumiem, ar ko transponē Direktīvu 95/46/EK, tām jāpaziņo attiecīgajām datu aizsardzības iestādēm par savām datu apstrādes darbībām agrās brīdināšanas un reaģēšanas sistēmā. Dažās dalībvalstīs var būt vajadzīga pat iepriekšēja atļauja no valsts datu aizsardzības iestādes.