

FRANCIJAS REPUBLIKA

Premjerministrs

Dekrēta projekts par stratēģisku un sensitīvu datu aizsardzību mākoņdatošanas tirgū

NOR:

Mērķauditorija: valsts pārvaldes iestādes un operatori, sabiedrības interešu grupas

Priekšmets: ...

Stāšanās spēkā: dekrēts stājas spēkā nākamajā dienā pēc tā publicēšanas.

Paziņojums:

Atsauces: ar dekrētu īsteno 2024. gada 21. maija Likuma Nr. 2024-449 par digitālās telpas nodrošināšanu un reglamentēšanu 31. pantu. To var aplūkot *Légifrance* tīmekļa vietnē (<http://www.legifrance.gouv.fr>).

Premjerministrs,

saskaņā ar XX ziņojumu;

ņemot vērā Eiropas Parlamenta un Padomes 2019. gada 17. aprīļa Regulu (ES) 2019/881 par *ENISA* (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013;

ņemot vērā Eiropas Parlamenta un Padomes 2015. gada 9. septembra Direktīvu (ES) 2015/1535, ar ko nosaka informācijas sniegšanas kārtību tehnisko noteikumu un Informācijas sabiedrības pakalpojumu noteikumu jomā;

ņemot vērā Aizsardzības kodeksu, jo īpaši D. 3126-2. pantu;

ņemot vērā 2005. gada 8. decembra Rīkojumu Nr. 2005-1516 par elektronisko apmaiņu starp lietotājiem un administratīvajām iestādēm un starp administratīvajām iestādēm un jo īpaši tā 9. pantu,

ņemot vērā 2016. gada 7. oktobra Likumu Nr. 2016-1321 par Digitālo Republiku, jo īpaši tā 16. pantu;

ņemot vērā 2024. gada 21. maija Likumu Nr. 2024-449 par digitālās telpas nodrošināšanu un reglamentēšanu, jo īpaši tā 31. pantu;

ņemot vērā 2014. gada 30. aprīļa Dekrētu Nr. 2014-445 par Iekšējās drošības ģenerāldirektorāta uzdevumiem un organizāciju;

ņemot vērā grozīto 2015. gada 27. marta Dekrētu Nr. 2015-350 par drošības produktu un uzticamības pakalpojumu sniedzēju kvalifikācijas sistēmu drošības vajadzībām;
ņemot vērā paziņojumu Nr. XX, kas XXX nosūtīts Eiropas Komisijai;
apspriedies ar Valsts padomi (Administrācijas nodaļu),

izdod šādu dekrētu.

1. pants

Iepriekš minētā 2024. gada 21. maija likuma 31. panta I punktā minētais sabiedrības interešu grupu saraksts ietver:

- sabiedrības interešu grupu, kas pazīstama kā “Digitālās veselības aģentūra (ANS)”;
- sabiedrības interešu grupu, kas pazīstama kā “Nacionālā AIDS pētniecības aģentūra (ANRS)”;
- sabiedrības interešu grupu, kas pazīstama kā “Izglītības un zinātniskās apmācības un apmaiņas veicināšanas aģentūra”;
- sabiedrības interešu grupu “Drošas datu piekļuves centrs (CASD)”;
- sabiedrības interešu grupu “Resursu centrs radikalizācijas novēršanai”;
- sabiedrības interešu grupu “Nacionālā veterinārā skola”;
- sabiedrības interešu grupu “Sabiedrības interešu grupa augstas aktivitātes slēgtu radioaktīvo avotu jautājumos (GIP SOURCES HA)”;
- sabiedrības interešu grupu “Valsts sistēma sociālo mājokļu pieprasījuma reģistrēšanai (GIP SNE)”;
- sabiedrības interešu grupu “Sociālo deklarāciju modernizācija (GIP-MDS)”;
- sabiedrības interešu grupu “Zinātnes un tehnoloģiju observatorija”.

2. pants

I. - Lai piemērotu iepriekš minētā 2024. gada 21. maija likuma 31. pantu, privātajam pakalpojumu sniedzējam ir jāievieš šādi drošības un datu aizsardzības kritēriji:

- dokumentēta informācijas drošības un riska pārvaldības politika, kas aptver apakšuzņēmēju ķēdi,
- droša cilvēkresursu pārvaldības sistēma pakalpojuma sniegšanā iesaistītajam personālam,
- rīki un procedūras tādu iekārtu drošai pārvaldībai, ar kurām īsteno pakalpojumu un informācijas sistēmas,

- fiziskie, vides un loģiskie drošības pasākumi, piemēram, šifrēšanas mehānismu izmantošana, piekļuves kontrole un lietotāja identitātes pārvaldība,
- informācijas drošības incidentu pārvaldības procedūras un darbības nepārtrauktības pasākumi,
- pasākumi Francijā spēkā esošo tiesību aktu ievērošanai un datu aizsardzības pasākumi, jo īpaši līgumiskie, apstrādātiem vai uzglabātiem datiem pret jebkādu trešo valstu publisko iestāžu piekļuvi, kas nav atļauta ar Eiropas Savienības tiesību aktiem vai dalībvalsts tiesību aktiem, tostarp jo īpaši nosacījumi, kas reglamentē kapitāla un balsstiesību turēšanu pakalpojumu sniedzēja uzņēmumā un pakalpojumu sniedzēja un jebkuru apakšuzņēmēju uzņēmējdarbības veikšanu.

Satvarā, ko izstrādājusi Francijas Kiberdrošības aģentūra saskaņā ar iepriekš minētā 2015. gada 27. marta dekrēta nosacījumiem, ir noteiktas prasības attiecībā uz šiem kritērijiem. Apspriešanās, kas vajadzīga, lai izveidotu un izstrādātu šo valsts informācijas sistēmas atsauces satvaru, notiek sadarbībā ar Starpministriju digitālo direktorātu.

II. - Lai izpildītu iepriekš minētā 2024. gada 21. maija likuma 31. panta I punktā noteiktās datu aizsardzības un drošības prasības, attiecīgās pārvaldes iestādes izmanto mākoņdatošanas pakalpojumus, ko sniedz kvalificēts privāts pakalpojumu sniedzējs un kas piešķirti saskaņā ar iepriekš minētā 2015. gada 27. marta dekrēta III nodaļā paredzētajiem nosacījumiem, un kas atbilst šā panta I punktā minētajiem kritērijiem vai vismaz līdzvērtīga līmeņa Eiropas sertifikācijai.

III. - Operatīvās un sakaru informācijas sistēmas, zinātniskās un tehniskās informācijas sistēmas un informācijas sistēmas, kuras ietver, pieprasa vai satur klasificētus informācijas nesējus vai informāciju, kas ietverta aizsardzības informācijas un sakaru sistēmā, kā arī informācijas un komunikācijas sistēmas, kuras izmanto Aizsardzības kodeksa D. 3126-2. pantā un iepriekš minētā 2014. gada 30. aprīļa dekrēta 1. pantā minētie dienesti, ir izslēgtas no šā panta darbības jomas.

3. pants

I. - Ja administrācija minētā 2024. gada 21. maija likuma 31. panta spēkā stāšanās dienā jau ir uzsākusi projektu, kurš atbilst minētajā pantā paredzētajiem nosacījumiem un kurā tiek izmantots mākoņdatošanas pakalpojums, ko sniedz privāts pakalpojumu sniedzējs, kurš neīsteno šā dekrēta 2. pantā noteiktos drošības un datu aizsardzības kritērijus, tā saskaņā ar premjerministra rīkojumā noteiktajām procedūrām var pieprasīt atkāpi no minētajā pantā noteiktajiem pienākumiem.

Šis atkāpes ilgums nedrīkst pārsniegt 18 mēnešus, ja Francijā ir pieņemams mākoņdatošanas pakalpojumu piedāvājums šā panta II punkta nozīmē. Ja dienā, kad pieprasīta atkāpe, Francijā nav pieejams pieņemams mākoņdatošanas pakalpojumu piedāvājums, atkāpes ilgums nedrīkst pārsniegt vienu gadu pirms iespējama jauna pieprasījuma.

Šo atkāpi piešķir ar pamatotu lēmumu, ko pieņem par projektu atbildīgais ministrs un apstiprina premjerministrs.

To publisko saskaņā ar Sabiedrisko attiecību kodeksa III grāmatā noteiktajiem nosacījumiem.

II. – Mākoņdatošanas pakalpojumu piedāvājuma pieņemamības novērtējums iepriekš minētā 2024. gada 21. maija likuma 31. panta III punkta nozīmē ir balstīts uz šādiem kritērijiem:

- funkcionālās vajadzības, ko piedāvājums spēj nodrošināt, ņemot vērā attiecīgās administrācijas uzdevumus,
- finanšu nosacījumi,
- datu drošības un aizsardzības darbības un tehniskie nosacījumi attiecībā uz piedāvājuma sniedzēja apstrādātajiem datiem saskaņā ar šā dekrēta 2. pantā noteiktajām prasībām,
- līguma beigu nosacījumi un atgriezeniskuma garantijas,
- kontroles, ilgtspējas un neatkarības nosacījumi iepriekš minētā 2016. gada 7. oktobra likuma 16. panta nozīmē.

Sagatavots:

Premjerministra vārdā —