APSTIPRINĀTS
ar Valsts ieņēmumu dienesta
08.10.2020. rīkojumu Nr. 279

Valsts ieņēmumu dienesta personas datu apstrādes drošības politika

I. Lietotie termini

1. Valsts ieņēmumu dienesta personas datu apstrādes drošības politikā (turpmāk – drošības politika) lietotie termini:

1.1. **personas datu apstrāde** – jebkura ar personas datiem veikta darbība, ko veic ar automatizētiem līdzekļiem vai kura veido daļu no kartotēkas, ja apstrādi neveic ar automatizētiem līdzekļiem;

1.2. **personas datu drošība** – personas datu konfidencialitātes (personas datus apstrādā tā, lai piekļuve tiem ir tikai personas datu lietotājam ar atbilstošām pilnvarām), veseluma (personas datus saglabā pilnīgi un neizmainīti, neatkarīgi no apstrādes metodēm) un pieejamības (personas datu lietotājs ar atbilstošām pilnvarām var piekļūt personas datiem un apstrādāt tos noteiktā laikā un vietā tikai noteiktā darba uzdevuma izpildei) nodrošināšana;

1.3. **personas datu lietotājs** – Valsts ieņēmumu dienesta ierēdnis vai darbinieks, kurš, pildot amata pienākumus saskaņā ar ierēdņa vai darbinieka amata aprakstu, veic personas datu apstrādi;

1.4. **tehnoloģiskie resursi** – Valsts ieņēmumu dienesta informācijas sistēmas sastāvdaļa, kurā ietilpst sistēmprogrammas, lietojumprogrammas, palīgprogrammas, datnes, personālie datori, serveris, datortīkls, aparatūra un citas iekārtas, kas nodrošina personas datu apstrādes informācijas sistēmas (turpmāk – informācijas sistēma) darbību;

1.5. **informācijas sistēmas kontroles** – metodes un pasākumi informācijas sistēmas risku mazināšanai;

1.6. **informācijas resursu turētājs** – Valsts ieņēmumu dienesta ierēdnis vai darbinieks, kurš atbilstoši kompetencei atbild par personu datu apstrādi un aizsardzību attiecīgajā patstāvīgajā struktūrvienībā, nosaka personas datu drošības prasības un apstiprina vai noraida personas datu lietotāju piekļuves tiesību pieprasījumus;

1.7. **personas datu aizsardzības pārkāpums** – personas datu drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga apstrādājamo personas datu neatļauta izpaušana vai piekļuve tiem, iznīcināšana, nozaudēšana vai pārveidošana, un datu apstrādes principu pārkāpumi, kas noteikti Eiropas Parlamenta un Padomes 2016.gada 27.aprīļa Regulas (ES) Nr.2016/679 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) (turpmāk – Vispārīgā datu aizsardzības regula) 5.pantā vai likuma "Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā" 4.pantā.

II. Drošības politikas nolūks un pamatnostādnes

2. Drošības politika ir izstrādāta un to īsteno saskaņā ar Valsts ieņēmumu dienestam normatīvajos aktos noteiktajiem uzdevumiem un mērķiem, Vispārīgo datu aizsardzības regulu, Fizisko personu datu apstrādes likumu, likumu "Par personas datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā" un citiem Latvijas Republikā spēkā esošajiem normatīvajiem aktiem, ņemot vērā starptautisko informācijas sistēmu drošības standartu rekomendācijas.

3. Drošības politikas mērķis ir nodrošināt tādu personas datu apstrādi un personas datu apstrādes tehnoloģiju vidi, lai personas dati un tehnoloģiskie resursi būtu aizsargāti pret ārējiem un iekšējiem drošības riskiem un vienlaikus nodrošinātu datu subjekta tiesības uz savu personas datu aizsardzību un brīvībām un Valsts ieņēmumu dienesta nepārtrauktu un kvalitatīvu darbību atbilstoši normatīvajos aktos noteiktajiem uzdevumiem un mērķiem.

4. Drošības politika nosaka galvenos drošības pamatnosacījumus personas datu apstrādei un personas datu apstrādes tehnoloģiju videi un darba organizācijai, lai nodrošinātu personas datu aizsardzību.

5. Drošības politika ir saistoša visiem Valsts ieņēmumu dienesta personas datu lietotājiem.

III. Drošības politikas īstenošanas pamatprincipi

6. Valsts ieņēmumu dienestā ir noteikts un pastāvīgi tiek pilnveidots iestādes normatīvo dokumentu kopums, tai skaitā personas datu aizsardzības jomā, kura īstenošana nodrošina drošības politikā noteiktā nolūka sasniegšanu.

7. Veicamo drošības pasākumu izmaksas ir samērojamas ar iespējamiem zaudējumiem, kas varētu rasties, īstenojoties personas datu apstrādē izmantojamās informācijas sistēmas drošības riskiem (netiek nodrošināta informācijas resursu pieejamība, konfidencialitāte vai veselums).

8. Valsts ieņēmumu dienests veicina katra personas datu lietotāja izpratni par pienākumiem personas datu aizsardzības nodrošināšanā, regulāri veicot personas datu lietotāju atbilstošas uzdevumu izpildes kontroli, izglītošanu un apmācību.

9. Valsts ieņēmumu dienests nodrošina pastāvīgu drošības politikas īstenošanas pasākumu koordinēšanu un pārraudzīšanu.

10. Konstatējot personas datu aizsardzības pārkāpumu, Valsts ieņēmumu dienests nodrošina personas datu aizsardzības pārkāpuma izmeklēšanu, pierādījumu vākšanu, novēršanu un citu personas datu aizsardzības pārkāpuma pārvaldīšanai

nepieciešamo pasākumu veikšanu un Vispārīgajā datu aizsardzības regulā noteiktajos gadījumos Datu valsts inspekcijas un datu subjekta informēšanu.

11. Ja personas datu lietotājs neievēro drošības politikas un citu saistīto ārējo un iekšējo normatīvo aktu izvirzītās prasības, iestādes vadītājs to sauc pie disciplināratbildības.

IV. Personas datu drošības organizācija

12. Par vispārēju personas datu drošību un aizsardzību Valsts ieņēmumu dienestā atbilstoši kompetencei atbild Valsts ieņēmumu dienesta ģenerāldirektors un viņa vietnieki.

13. Personas datu aizsardzību patstāvīgajā struktūrvienībā nodrošina patstāvīgās struktūrvienības vadītājs.

14. Personas datu lietotājs ir atbildīgs par Vispārīgās datu aizsardzības regulas un citu saistīto normatīvo aktu ievērošanu, tai skaitā iekšējo noteikumu personas datu aizsardzības un informācijas sistēmas lietošanas jomā ievērošanu.

15. Patstāvīgās struktūrvienības vadītājs un informācijas resursu turētājs nodrošina kontroles pasākumus pārraudzībā esošo personas datu apstrādei.

16. Personas datu apstrādes novērtējumu par ietekmi uz datu aizsardzību un informācijas sistēmas auditu veic, lai izvērtētu noteikto drošības prasību ievērošanu Valsts ieņēmumu dienestā un to īstenošanu informācijas sistēmā.

17. Valsts ieņēmumu dienests, ņemot vērā tehnoloģisko resursu līmeni, īstenošanas izmaksas un personas datu apstrādes veidus un nolūku, kā arī dažādas iespējamības un smaguma pakāpes risku attiecībā uz datu subjekta tiesībām uz datu aizsardzību un brīvībām, īsteno atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu riskam atbilstošu drošības līmeni.

V. Personas datu klasifikācija

18. Personas datu klasifikācijas mērķis ir apzināt Valsts ieņēmumu dienesta rīcībā esošo personas datu nozīmību, lai to drošības un aizsardzības pasākumi būtu adekvāti aizsargājamo personas datu vērtībai.

19. Personas datus klasificē atbilstoši konfidencialitātei, un tiem piešķir vērtības (kritiskuma) pakāpi atkarībā no kaitējuma, kas varētu tikt nodarīts datu subjekta tiesībām uz savu personas datu aizsardzību un brīvībām, ja nav nodrošināta personas datu konfidencialitāte, veselums un pieejamība.

20. Kā augsta riska personas datus klasificē personas datus, kas personas datu aizsardzības pārkāpuma gadījumā datu subjektam var izraisīt fizisku, materiālu vai nemateriālu kaitējumu, piemēram, kontroles zaudēšanu pār saviem personas datiem vai šo datu izmantošanas tiesību ierobežošanu, diskrimināciju, identitātes zādzību vai viltošanu, finansiālu zaudējumu, kaitējumu reputācijai vai jebkādu citu datu subjektam īpaši nelabvēlīgu ekonomisko vai sociālo situāciju, kā arī īpašu kategoriju (sensitīvos) personas datus un personas datus par sodāmību un pārkāpumiem.

VI. Novērtējums par ietekmi uz datu aizsardzību

21. Novērtējuma par ietekmi uz datu aizsardzību, tai skaitā risku analīzes, mērķis ir novērtēt personas datu apstrādes atbilstību Vispārīgajai datu aizsardzības regulai un citiem saistītajiem normatīvajiem aktiem personu datu aizsardzības jomā un drošības apdraudējuma īstenošanās varbūtību un ietekmi uz datu subjekta tiesībām uz savu datu aizsardzību un brīvībām.

22. Personas datu apstrādes un personas datu apstrādes tehnoloģiju vides risku vadības pasākumus un izmantojamās procedūras nosaka Valsts ieņēmumu dienesta ģenerāldirektors, kurš ieceļ informācijas sistēmu drošības pārvaldniekus tehnoloģiju vides risku vadības pasākumu un izmantojamo procedūru nodrošināšanai.

23. Novērtējumu par ietekmi uz datu aizsardzību, tai skaitā risku analīzi, personas datu apstrādes nolūkam un personas datu apstrādes tehnoloģiju videi veic ne retāk kā vienu reizi trīs gados.

24. Novērtējuma par ietekmi uz datu aizsardzību, tai skaitā risku analīzes, rezultātus izmanto, plānojot un nosakot drošības līdzekļu ieviešanu vai kompensējošo pasākumu veikšanu, papildus veicot risku uzskaitījumu un riska izvērtējumu, kā arī pasākumus riska mazināšanai, nosakot uzdevumus, to izpildes termiņus un par izpildi atbildīgo personas datu lietotāju.

VII. Personas datu drošības pārvaldības principi

25. Valsts ieņēmumu dienesta iekšējos noteikumos personas datu aizsardzības un informācijas sistēmu lietošanas jomā:

25.1. ir noteiktas un ieviestas procedūras un informācijas sistēmas kontroles, lai nodrošinātu, ka:

25.1.1. piekļuve personas datiem ir tikai autorizētiem un identificētiem personas datu lietotājiem;

25.1.2. ir noteikta personas datu lietotāju tiesību piešķiršanas, uzturēšanas, anulēšanas un inventarizācijas kārtība;

25.1.3. personas datu lietotāju tiesības piešķir, ievērojot principu, ka tiek dotas tikai tādas tiesības, kas nepieciešamas amata pienākumu izpildei;

25.1.4. personas datu lietotāji, kam tiek dota piekļuve personas datiem, ir apmācīti darbam ar personas datiem un informācijas sistēmu, ar izpratni par drošības pamatnostādnēm un informācijas sistēmas lietošanas nosacījumiem;

25.1.5. informācijas sistēmas konfigurācija un funkcionalitāte ir tāda, lai mazinātu neautorizētas personas datu piekļuves un modificēšanas iespējas;

25.1.6. informācijas sistēmā izmanto šifrēšanas līdzekļus, lai nodrošinātu pārraidāmo personas datu aizsardzību un pēc nepieciešamības arī glabājamo personas datu aizsardzību;

25.1.7. informācijas sistēmas personas datu apmaiņa, tai skaitā personas datu iesniegšana, ir organizēta tā, lai iesaistītās puses nevarētu noliegt personas datu sūtīšanas vai saņemšanas faktu (*non-repudiation*);

25.1.8. informācijas sistēmā izmanto tehnoloģiskos risinājumus un ievēro procedūras, lai nodrošinātu informācijas sistēmas darbības uzraudzību, kontrolējot to parametrus un veicot auditācijas pierakstu analīzi;

25.1.9. tiek ievērota informācijas sistēmas izmaiņu kārtība – produkcijā ieviež tikai akceptētas un testētas izmaiņas;

25.1.10. ir noteikta kārtība personas datu aizsardzības pārkāpumu, informācijas sistēmas incidentu un problēmu reģistrēšanai un pārvaldībai, lai mazinātu to ietekmi un atkārtošanās risku;

25.2. ir noteikti informācijas sistēmas fiziskās aizsardzības pasākumi, kas aizsargā no nevēlamiem apkārtējās vides (ugunsgrēks, plūdi, temperatūras svārstības u.c.), tehniskiem (neatbilstoša elektroenerģijas padeve u.c.) un cilvēkfaktoriem (tīši vai netīši bojājumi, zādzība u.c.), un loģiskās aizsardzības pasākumi;

25.3. ir noteikta:

25.3.1. personas datu glabāšanas un aprites kārtība;

25.3.2. personas datu lietotāju tiesības, pienākumi un atbildība;

25.3.3. personas datu apstrādes izmaiņu identificēšanas un reģistrēšanas kārtība;

25.3.4. personas datu izsniegšanas kārtība datu subjektam un saņēmējam, tai skaitā trešajai personai;

25.3.5. videoierakstu un audioierakstu veikšanas, uzglabāšanas, izsniegšanas un dzēšanas (iznīcināšanas) kārtība;

25.3.6. personas datu dzēšanas (iznīcināšanas) vai publiskas nepieejamības nodrošināšanas kārtība;

25.3.7. novērtējuma par ietekmi uz datu aizsardzību veikšanas kārtība;

25.3.8. personas datu aizsardzības pārkāpumu izmeklēšanas kārtība.

VIII. Informācijas sistēmas darbības nepārtrauktības un avārijas atjaunošanas plānošana un pārvaldība

26. Lai nodrošinātu informācijas sistēmas darbības nepārtrauktību un atjaunošanu avārijas gadījumā, Valsts ieņēmumu dienesta iekšējos noteikumos informācijas sistēmu drošības jomā ir noteikta informācijas sistēmas darbības nepārtrauktības nodrošināšanas un atjaunošanas procedūra.

27. Informācijas sistēmas darbības nepārtrauktības nodrošināšanas un atjaunošanas procedūras ietvaros Valsts ieņēmumu dienests veic regulāru informācijas sistēmas personas datu rezerves kopēšanu, nodrošinot personas datu rezerves kopijas glabāšanu citā ģeogrāfiskā atrašanās vietā, un informācijas sistēmas atjaunošanas pārbaudes, lai gūtu pārliecību par atjaunotās informācijas sistēmas darbspēju un datu integritāti.

IX. Noslēguma jautājums

28. Valsts ieņēmumu dienesta Slepenības un drošības režīma nodrošināšanas daļa pārskata drošības politiku vismaz reizi divos gados.