



Nodrošinājuma valsts aģentūra

Rīgā

20.09.2019.

Iekšējie noteikumi Nr. 15/2019

## Personas datu aizsardzības politika

Izdoti saskaņā ar  
Valsts pārvaldes iekārtas likuma  
72.panta pirmās daļas 2.punktu

### I. Vispārīgie jautājumi

1. Iekšējie noteikumi nosaka Nodrošinājuma valsts aģentūras (turpmāk – Aģentūra) pārziņā esošo personas datu apstrādes aizsardzības tehniskos un organizatoriskos drošības pasākumus.

2. Iekšējos noteikumos ir lietoti šādi termini:

2.1. informācijas sistēma – strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kuru lietojot tiek nodrošināta iestādes funkciju izpildei nepieciešamās informācijas apstrāde;

2.2. Aģentūras informācijas resurss – Aģentūras pārziņā esoša informācijas sistēma vai resurss, tai skaitā Aģentūras ārējā un iekšējā tīmekļa vietne, kā arī videonovērošanas sistēma;

2.3. sensitīvie dati – īpašu kategoriju dati atbilstoši Eiropas Parlamenta un Padomes (ES) 2016. gada 27. aprīļa regulas 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 – Regula) 9.pantam;

2.4. sodāmības dati – personas dati par sodāmību un pārkāpumiem vai ar tiem saistītiem drošības pasākumiem atbilstoši Regulas 10.pantam;

2.5. datu aizsardzības speciālists – ar Aģentūras direktora rīkojumu noteikts Aģentūras nodarbinātais, kurš pilda Regulas 39.pantā noteiktos uzdevumus;

2.6. Aģentūras informācijas resursa pārvaldnieks – ar Aģentūras direktora rīkojumu noteikts Aģentūras nodarbinātais, kurš atbilstoši Iekšlietu ministrijas iekšējiem normatīvajiem aktiem organizē informācijas resursa pārvaldību un attīstību, kā arī definē tā funkcionalitātes un pieejamības prasības.

3. Šie iekšējie noteikumi attiecas uz Aģentūras pārziņā esošo personas datu apstrādi:

- 3.1. elektroniski Aģentūras informācijas resursos;
- 3.2. papīra formā, elektroniski datorā ārpus informācijas sistēmām vai elektroniskajā pastā (turpmāk – e-pasts);
- 3.3. Iekšlietu ministrijas resursu vadības sistēmā “Horizon”;
- 3.4. Iekšlietu ministrijas informācijas sistēmā “Lietvedība”;
- 3.5. citās Iekšlietu ministrijas Informācijas centra (turpmāk – Centrs) vai citu iestāžu un privāto tiesību juridisko personu, kuras veic publiskās pārvaldes uzdevumus, pārziņā esošās informācijas sistēmās (turpmāk – ārējas informācijas sistēmas).

4. Aģentūras datu aizsardzības speciālists sadarbībā ar Aģentūras kvalitātes un risku vadītāju organizē Novērtējuma par ietekmi uz datu aizsardzību veikšanu atbilstoši Regulas prasībām Personas datu apstrādes reģistrā iekļautajiem mērķiem ne retāk kā reizi trijos gados, un pārskatīšanu pēc būtiskām izmaiņām Aģentūras informācijas resursos vai personas datu apstrādes procesos un procedūrās, kas ietekmē personas datu aizsardzības riskus.

## **II. Personas datu apstrādes un glabāšanas kārtība**

5. Dokumentu, kas satur personas datus un ar kuru tajā brīdī nenotiek darbs, glabā vietā, kur tas nav pieejams personai, kurai tas nav paredzēts.

6. Izdrukājot dokumentu, kas satur personas datus, uz koplietošanas printera vai multifunkcionālās iekārtas, Aģentūras nodarbinātā pienākums ir nekavējoties paņemt izdruku, vai problēmu gadījumā – atkārtot izdruku tikai pēc problēmas novēršanas, un pārliecināties, ka izdruka nav pieejama personai, kurai tā nav paredzēta.

7. Skenējot dokumentu, kas satur personas datus, pēc iespējas izmanto tādu režīmu, kurā dokumentu saņem tikai individuāls adresāts. Aizliegts skenēto dokumentu atstāt tīkla diskā, kur tas pieejams personai, kurai tas nav paredzēts.

8. Dokumentu, kas satur personas sensitīvos vai sodāmības datus, ārējā sarakstē aizliegts pārsūtīt, izmantojot nedrošu sakaru līdzekli. Šādu dokumentu pārsūta:

- 8.1. pa pastu vai ar kurjeru;
- 8.2. informācijas sistēmā “Lietvedība”;
- 8.3. Oficiālo elektronisko adresu informācijas sistēmā;
- 8.4. Iekšlietu ministrijai vai tās padotībā esošajām iestādēm uz konkrēta nodarbinātā darba e-pasta adresi, vai arī uz minētās iestādes vai struktūrvienības oficiālo e-pasta adresi;
- 8.5. citos gadījumos uz e-pastu, tikai izmantojot šifrēšanu ar saņēmēja publisko atslēgu vai atslēgu, kas tiek paziņota adresātam, izmantojot citu sakaru līdzekli.

9. Personas sensitīvos vai sodāmības datus uz ārējā datu nesēja glabā šifrētā

veidā, bet, ja tas nav iespējams, to aizsargā ar drošu paroli. Lietojot pārnēsājamo datu nesēju (portatīvo datoru, zibatmiņu u.tml.), kurā ir personas sensitīvie vai sodāmības dati, ārpus Aģentūras telpām, nodrošina personas datu šifrēšanu. Par attiecīgās šifrēšanas programmatūras uzstādīšanu Aģentūras nodarbinātais savlaicīgi vēršas Centra pakalpojumu dienestā, nosūtot pieteikumu uz e-pasta adresi [pd@ic.iem.gov.lv](mailto:pd@ic.iem.gov.lv).

10. Atstājot darba vietu, Aģentūras nodarbinātā pienākums ir aizvērt atvērto informācijas sistēmu vai bloķēt piekļuvi datoram, lai novērstu nepiederošas personas piekļušanu datiem.

11. Apstrādājot personas sensitīvos vai sodāmības datus, nodrošina, lai dati, no kuriem personu var identificēt, netiek apstrādāti vairāk kā nepieciešams konkrētā uzdevuma izpildei.

12. Aģentūras nodarbinātais darbu ar personas datiem veic darba vietā atbilstoši darba kārtības noteikumiem, vai arī nodrošina šādu nosacījumu izpildi:

12.1. attālināts darbs ārpus darba vietas ar personas sensitīviem vai sodāmības datiem ir pieļaujams ar Aģentūras direktora rakstisku atļauju, bet ar pārējiem personas datiem – ar tiešā vadītāja atļauju;

12.2. minētā atļauja nav nepieciešama, ja personas datu apstrāde ārpus darba vietas tieši izriet no amata pienākumiem (piemēram, glabājamo lietu pieņemšana to atrašanās vietā, nekustamo īpašumu apsekošana un apsaimniekošanas darbi nekustamajā īpašumā);

12.3. personas datu apstrādē ārpus darba vietas tiek nodrošināta līdzvērtīga aizsardzība kā darba vietā, lai samazinātu to izpaušanas risku.

### **III. Videonovērošanas datu aizsardzība**

13. Aģentūra veic pastāvīgu videonovērošanu personas datu apstrādes vietās, kas iekļautas ar Aģentūras direktora rīkojumu apstiprinātajā Personas datu apstrādes reģistrā (turpmāk – objekti) ar mērķi:

13.1. novērst un atklāt ar īpašuma aizsardzību saistītus likumpārkāpumus;

13.2. novērst un atklāt ar Aģentūras nodarbināto drošību un ierobežotas pieejamības informācijas konfidencialitātes aizsardzību saistītus pārkāpumus apmeklētāju pieņemšanas vietās.

14. Ar videonovērošanas sistēmu strādā vai nu Aģentūras nodarbinātais, kuram tas ietilpst amata pienākumos, vai arī apsardzes ārpakalpojumu sniedzēja darbinieks atbilstoši noslēgtā līguma nosacījumiem. Videonovērošanas sistēmu izvieto tā, lai ierakstiem nevar piekļūt nepiederoša persona.

15. Videonovērošanas ierakstu izmanto tikai objekta drošības incidenta (vai aizdomu par iespējamu incidentu) izmeklēšanai atbilstoši šo iekšējo noteikumu 13.punktā noteiktajiem mērķiem, neizpaužot to trešajai personai bez Aģentūras direktora atļaujas.

16. Par incidentu izmeklēšanai nepieciešamā videonovērošanas ieraksta saglabāšanu uz ārējā nesēja un turpmāko rīcību ar to atbild Aģentūras Izņemto lietu, piedziņas un materiālās apgādes departamenta Materiāli tehniskās apgādes pārvaldes Apsardzes nodaļas vadītājs vai viņa uzdevumā – par objektu atbildīgais minētās nodaļas apsardzes inspektors.

#### **IV. Fotografēšana, filmēšana un informācijas publicēšana**

17. Veicot video filmēšanu vai fotografēšanu svinīga pasākuma, semināra, konferences, mācību vai tamlīdzīga pasākuma dokumentēšanai, Aģentūras nodarbinātais informē klātesošās personas par fotografēšanas vai filmēšanas mērķi un respektē personu tiesības nepiekrīst un izvairīties no fotografēšanas vai filmēšanas.

18. Veicot video filmēšanu vai fotografēšanu mantas iznīcināšanas vai citu darba procesu dokumentēšanai, administratīvā pārkāpuma lietā izņemtās vai arestētās mantas vai lietiskā pierādījuma kriminālprocesā stāvokļa fiksēšanai, nekustamā īpašuma stāvokļa apsekošanai un tamlīdzīgi, Aģentūras nodarbinātais informē klātesošās personas par tās mērķi un pēc iespējas izvēlas tādus rakursus, lai bez nepieciešamības netiktu filmētas vai fotografētas klātesošās personas. Šādu fotografēšanu vai video filmēšanu atļauts veikt, izmantojot personīgās ierīces, tikai tad, ja nav pieejama Aģentūrai piederoša ierīce un netiek bez darba nepieciešamības izpausti personas dati.

19. Aģentūras tīmekļa vietnē un iekštīkla vietnē publicētā informācija var saturēt fotogrāfijas, kurās var identificēt Aģentūras nodarbinātos un citas personas. Aģentūras nodarbinātais, kurš ievieto informāciju, pārlicinās, ka netiek ievietota fotogrāfija, kas neatbilst ētiskiem apsvērumiem, it īpaši, ja tā saistīta ar ārpusdarba aktivitātēm.

20. Publicējot informāciju Aģentūras tīmekļa vietnē un iekštīkla vietnē, Aģentūras nodarbinātais, kurš sagatavo informāciju, pārlicinās, ka tā nesatur personas sensitīvos vai sodāmības datus.

21. Par Aģentūras tīmekļa vietnes kopējo tēlu un vizuālo materiālu publicēšanu atbild Aģentūras sabiedrisko attiecību speciālists. Ja Aģentūra saņem personas datu subjekta iebildumu, Aģentūras sabiedrisko attiecību speciālists sadarbībā ar datu aizsardzības speciālistu nekavējoties atkārtoti izvērtē publicētās informācijas, tai skaitā fotogrāfijas, atbilstību šo iekšējo noteikumu prasībām un neatbilstošos personas datus dzēš.

#### **V. Aģentūras nodarbinātā pienākumi un atbildība**

22. Personas datus atļauts nodot citām personām ārpus Aģentūras tādiem mērķiem, kas minēti ar Aģentūras direktora rīkojumu apstiprinātajā Personas datu apstrādes reģistrā. Aģentūras nodarbinātais, kurš organizē personas datu sagatavošanu atbilstoši Aģentūras direktora vai tiešā vadītāja dotajam

uzdevumam vai noslēgtajiem sadarbības līgumiem, ir atbildīgs par personas datu drošu nodošanu trešajai personai.

23. Aģentūras datu aizsardzības speciālistam, vai Aģentūras direktora uzdevumā – citam Aģentūras nodarbinātajam, ir tiesības izlases veidā kontrolēt Aģentūras nodarbinātā no darba vietas veiktās darbības internetā un darba e-pastā, lai nepieļautu personas datu un citas ierobežotas pieejamības informācijas nepamatotu izpaušanu un informācijas sistēmu drošības apdraudējumu.

24. Aģentūras direktoram, datu aizsardzības speciālistam, vai informācijas resursa pārvaldniekam ir tiesības pieprasīt Centram veikt Aģentūras informācijas resursa auditācijas pierakstu izlases kontroli un ziņot Aģentūrai par aizdomīgām darbībām, kas saistītas ar personas datu apstrādi.

25. Aģentūras nodarbinātajam ir pienākums informēt datu aizsardzības speciālistu par iespējamām problēmām informācijas sistēmu darbībā vai drošības incidentu, kas var radīt apdraudējumu Aģentūras informācijas resursu konfidencialitātei, integritātei vai pieejamībai, vai citu iespējamu personas datu aizsardzības pārkāpumu. Ziņošanai izmanto e-pasta adresi [das@agentura.iem.gov.lv](mailto:das@agentura.iem.gov.lv), tālruni vai Aģentūras iekštīkla vietnē <https://intra.nva.iem.gov.lv> pieejamo tiešsaistes formu ziņošanai par incidentiem vai problēmām.

26. Saņemot informāciju par iespējamo pārkāpumu, datu aizsardzības speciālista pienākums ir to izmeklēt, un pārkāpuma gadījumā ziņot Aģentūras direktoram. Aģentūras direktors izvērtē pārkāpumu un pieņem lēmumu par nepieciešamām sankcijām, nepieciešamību ziņot Datu valsts inspekcijai un nepieciešamajiem preventīvajiem pasākumiem.

Saskaņots ar Iekšlietu ministriju 2019. gada 6.septembrī

Direktors

Ē.Ivanovs