



**TARBIJAKAITSE JA  
TEHNILISE JÄRELEVALVE  
AMET**

**KÄSKKIRI**

02.04.2025 nr 1-2/25-025

**Andmekaitse juhendi kinnitamine**

Võttes arvesse avaliku teabe seaduses (eelkõige §-des 35, 38, 39 ja 43), isikuandmete kaitse seaduses (eelkõige §-s 56 lg 1), Euroopa Parlamendi ja nõukogu 27.aprilli 2016 määruses (EL) 2016/679 „Isikuandmete kaitse üldmäärus“ (eelkõige artiklites 5, 6, 12, 32, 33) sätestatu ning majandus- ja taristuministri 07.detsembri 2018 määruse nr 62 „Tarbijakaitse ja Tehnilise Järelevalve Ameti põhimäärus“ § 5 lg 3 p 1 alusel:

1. Kinnitan Tarbijakaitse ja Tehnilise Järelevalve Ameti andmekaitse juhendi (lisatud).
2. Tunnistan kehtetuks 04.09.2021 käskkirja nr 1-2/21-058.

(allkirjastatud digitaalselt)  
Kristi Talving  
peadirektor

Koostaja: Mariko Männa

## **TARBIJAKAITSE JA TEHNILISE JÄRELEVALVE AMETI ANDMEKAITSE JUHEND**

### **ÜLDSÄTTED**

1. Käesoleva juhendi eesmärgiks on kehtestada reeglid Tarbijakaitse ja Tehnilise Järelevalve Ametis (edaspidi Amet või TTJA) andmete kogumiseks ja töötlemiseks, anda tegevussuunised teenistujatele andmekaitse reeglite rikkumise kahtluse korral ja sätestada Ameti ja andmekaitse spetsialisti tegevused rikkumise esinemise korral.
2. Juhendi koostamisel on võetud aluseks andmekaitset reguleerivad õigusaktid ja organisatsioonilised dokumendid.

### **ANDMEKAITSE REEGLID**

3. Andmekaitse nõuete järgimisel lähtutakse Ametis järgmistest põhimõtetest:
  - 3.1. Andmeid kogutakse ja kasutatakse minimaalselt (nii vähe kui võimalik) ja säilitatakse üksnes seni, kuni neid vajatakse. Minimaalsus tähendab seda, et ei koguta rohkem andmeid, kui eesmärgi täitmiseks vaja, nt kodaniku postiaadressi kohta infot ei koguta, kui on teada tema e-posti aadress.
  - 3.2. Piiratakse andmete juurdepääsu (nii organisatsioonisiselt kui -väliselt), st teenistuja pääseb ligi nendele andmetele, mida tal on oma töö tegemiseks vaja ja väline kasutaja näeb infosüsteemi sisselogimisel ainult enda või oma ettevõttega seotud andmeid.
  - 3.3. Tagatakse korrapärane isikuandmete kustutamine pärast säilitustähtaja lõppemist. Andmeid säilitatakse soovitatavalt infosüsteemis, kus toimub kokkulepitud korras andmete hävitamine. Kui andmeid hoitakse nt Exceli tabelis võrgukettal, siis neid tohib seal hoida seni, kuni eesmärk saab täidetud. Peale seda tuleb andmed turvaliselt kustutada ülekirjutamise teel.
  - 3.4. Kasutatakse krüptimist, pseudonüümimist, anonüümimist, st andmed edastatakse kas krüpteeritult või isikuandmed asendatakse selliste andmetega, et isikut ei ole võimalik andmetega siduda.
  - 3.5. Isikuandmeid töödeldakse nii, et kõrvalised isikud ei pääseks andmetele ligi. Töökohalt lahkudes tuleb lukustada arvuti, sh kodukontoris olles. Isikuandmeid sisaldav dokument tuleb pärast printimist koheselt printerist eemaldada.
  - 3.6. Keskkonnaministeeriumi Infotehnoloogiakeskuse (KeMIT), kui Ameti teenusepartner IT-teenuseosutaja, tagab infotehnoloogilised turvameetmed. Ameti teenistujad peavad lähtuma oma tegevuses TTJA infoturbepoliitikast.
  - 3.7. Koolitatakse regulaarselt teenistujaid ja vajadusel koostööpartnereid.
  - 3.8. Eelistatakse lahendusi, kus isikud saavad kergemini oma andmetele ligi (nt e-teenindus).
  - 3.9. Kättesaadavaks on tehtud isikuandmete töötlemise reeglid, mis tagavad andmetöötluse läbipaistvuse ning mis annavad isikule endale võimaluse oma

turvalisuse eest paremini seista (teenistujatel teabehalduse kord ja töökorralduse reeglid, asutusevälistel isikutel välisveeb).

- 3.10. Suuremahuliste dokumentide jagamiseks kasutatakse failivahetuskeskkonda <https://transit.envir.ee/>.
- 3.11. Avalikke pilveteenuseid tohib kasutada sõltuvalt seal hoitavate andmete turvaklassidest (asutusesiseseks kasutamiseks (AK) mõeldud andmeid avalikus pilves hoida ei tohi).
- 3.12. AK-teabe edastamisel tuleb lähtuda TTJA dokumendihalduse korrast ning TTJA infovahendite kasutamise ja andmete töötlemise korrast.
- 3.13. Isikuandmeid ei esitata kolmandatele isikutele, sh ettekannetes ja koosolekutel.

## **TEENISTUJA MEELESPEA**

4. Andmeid ei tohi kasutada muul eesmärgil, kui ainult õigusaktides sätestatud ülesannete täitmiseks. Nt kodaniku, kes esitas selgitustaotluse, andmeid võib kasutada ainult tema päringutele vastamiseks, mitte ühelgi teisel eesmärgil (kampaaniate jm levitamiseks).
5. E-kirja või dokumendi edastamisel jälgi hoolega, et adressaat oleks õige, sest isikute nimed, kellega sa suhtled, võivad olla sarnased. Valele isikule andmete edastamine on andmekaitse reeglite rikkumine ja sellele järgneb rikkumismenetlus.
6. Kui e-kiri või dokument on saadetud valele adressaadile, teavita koheselt adressaati, et see on valesi saadetud ning dokument tuleb kustutada. Kustutamisest tuleb Ametile saata allkirjastatud kinnitus.
7. Teavita juhtunust Ameti andmekaitse spetsialisti. Andmekaitse spetsialisti ülesandeid täidab teabehalduse nõunik.
8. Kui e-kiri saadetakse paljudele adressaatidele, märgi saajaks iseennast ning lisa kindlasti kõik adressaadid pimekoopia reale.
9. Piiratud juurdepääsuga teave (eriliiki isikuandmed, tundlikud andmed) tuleb enne e-kirja saatmist krüpteerida. Krüpteerimiseks pöördu kantseleisse.
10. Isiklikel eesmärkidel ei tohi ametiülesannete täitmisel kogutud andmeid kasutada. Andmeid tohib kasutada ainult sel eesmärgil, mille jaoks need kogutud on.

## **AMETI TEGEVUSED RIKKUMISE KORRAL**

11. Andmekaitse reeglite rikkumise puhul algatab andmekaitse spetsialist rikkumismenetluse, mille käigus:
  - 11.1. tuvastatakse rikkumise asjaolud ja kogutakse selgitusi;
  - 11.2. kirjeldatakse rikkumiste mõju füüsilistele isikutele;
  - 11.3. võetakse kasutusele parandusmeetmed (nii tehnilised kui korralduslikud);
  - 11.4. teavitatakse juhtunust Andmekaitse Inspeksiooni;
  - 11.5. koostatakse peadirektorile juhtunust ülevaade edasiste tegevuste otsustamiseks.
12. Rikkumismenetlusega seotud dokumendid registreeritakse dokumendihaldussüsteemis.