ANDMEKAITSE INSPEKTSIOON
Valvame, et isikuandmete kasutamisel austatakse eraelu ning et riigi tegevus oleks läbipaistev

ANDMEKAITSE JA ANDMETURBE ENESEABI KÜSIMUSTIK

Juhend kehtestatakse isikuandmete kaitse seaduse § 33 lõike 1 punkti 5 alusel.
Kinnitatud 2008. aasta 17. juulil.
Muudetud 2013. aasta 19. veebruaril (muudetud sissejuhatus, infoturbe haldamise osas küsimus 14, viited).

Isikuandmete kaitse seadus (IKS) sätestab isikuandmete töötlemise põhimõtted ning kohaldatavad turvameetmed.

Isikuandmete kaitse seaduse 4. peatükis sätestatud isikuandmete töötlemise nõuded kehtivad kõigi töötlemisetappide kohta.

Isikuandmete töötlemine on iga isikuandmetega tehtav toiming, sealhulgas isikuandmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, ristkasutamine, ühendamine, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest.

Isikuandmete töötlejal tuleb isikuandmete kaitseks kasutusele võtta vajalikud füüsilised, infotehnilised ja organisatsioonilised turvameetmed andmete tervikluse, käideldavuse ja konfidentsiaalsuse osas (IKS § 25).

Andmekaitse Inspektsioon on koostanud isikuandmete töötlejatele alljärgneva eneseabiküsimustiku, mille eesmärgiks on isikuandmete töötlemise alustamisel või muudatuste tegemisel anda võimalus töötlejatel jõuda arusaamisele, milliseid elementaarseid andmeturbemeetmeid on vaja kohaldada ja/või on juba kohaldatud ja kas kasutusele võetud/võetavad meetmed on seaduses sätestatud nõuetele vastavad/piisavad.

Küsimustele saab vastata “jah“, „osaliselt“ või „ei“ vormis. Kui küsimuse vastuseks on „osaliselt“ või „ei“, siis andmetöötluskeskkonnas ei ole piisavalt rakendatud isikuandmete töötlemise nõudeid ja töötlejal tuleb lahendused olukorra parandamiseks selliselt, et nendele küsimustele saab jaatavalt vastata.

Küsimustik on koostatud isikuandmete töötlejatele eneseabi eesmärgil kaardistamaks kasutusele võetavaid ja/või kasutuselolevaid andmeturbemeetmeid.

Küsimustik pole mõeldud Andmekaitse Inspektsioonile esitamiseks, vaid töötlejale eneseabiks.

Küsimustiku täitmisel on soovitatav tutvuda ka teiste Andmekaitse Inspektsiooni koostatud materjalide ja juhenditega, mis on kättesaadavad Inspektsiooni kodulehelt: http://www.aki.ee

Inspektsioon annab nõu telefonil 627 4144 igal tööpäeval kl 10.00-12.00 ja 14.00-16.00.

Küsimusi ja kommentaare ootame ka meiliaadressile info@aki.ee

Infoturbe haldamine (Üldised isikuandmete ja andmeturbega seotud põhiküsimused)	
1. Kas olete määratlenud milliseid isikuandmeid te töötlete?[1]	☐ Jah ☐ Osaliselt ☐ Ei
2. Kas olete kindlaks teinud, et Teil on õigus (seaduslik alus) töödelda isikuandmeid?	☐ Jah ☐ Osaliselt ☐ Ei
3. Kas olete analüüsinud, millised andmekaitse ja andmeturvalisuse riskid on isikuandmete töötlemisega seotud ja kas analüüsi alusel on töötatud välja andmekaitset ja andmeturvalisust puudutav tegevuspoliitika?	☐ Jah ☐ Osaliselt ☐ Ei
4. Kas olete veendunud, et teie poolt töödeldavad isikuandmed on ajakohased, täielikud ja vajalikud teie poolt määratletud eesmärkide saavutamiseks?	☐ Jah ☐ Osaliselt ☐ Ei
5. Kas olete kindel, et isikuandmeid ei kasutata muudel eesmärkidel kui teie poolt määratletud eesmärkide saavutamiseks?	☐ Jah ☐ Osaliselt ☐ Ei
6. Kas teie töökorraldus võimaldab korrigeerida ebaõigeid isikuandmeid?	☐ Jah ☐ Osaliselt ☐ Ei
7. Kas olete kindlaks teinud millisest allikast pärinevad isikuandmed?	☐ Jah ☐ Osaliselt ☐ Ei
8. Kas olete määratlenud, kellele isikuandmeid edastate?	☐ Jah ☐ Osaliselt ☐ Ei
9. Kas olete kindel, et teil on õigus isikuandmeid edastada?[2]	☐ Jah ☐ Osaliselt ☐ Ei
10. Kas olete kindlaks teinud edastatavate isikuandmete saaja õiguse isikuandmeid töödelda?	☐ Jah ☐ Osaliselt ☐ Ei
11. Kas olete taganud andmesubjektile õiguse kontrollida tema kohta käivaid isikuandmeid?	☐ Jah ☐ Osaliselt ☐ Ei
12. Kas on määratud kindlaks isikuandmete töötlemisega seotud ülesanded, vastutusalad, vastutavad isikud ja nende asendamise kord?	☐ Jah ☐ Osaliselt ☐ Ei
13. Kas olete kujundanud oma töökorralduse niisuguseks, et see võimaldaks täita andmekaitse nõudeid?	☐ Jah ☐ Osaliselt ☐ Ei
14. Kas olete registreerinud delikaatsete isikuandmete töötlemise Andmekaitse Inspektsioonis või teavitanud Andmekaitse Inspektsiooni isikuandmete kaitse eest vastutava isiku määramisest?[3]	☐ Jah ☐ Osaliselt ☐ Ei

[1] Vaata juhendmaterjali biomeetriliste isikuandmete töötlemisest.
[2] Vaata juhendmaterjali isikuandmete edastamisest välisriiki.

15. Kas isikuandmete kaitset ja andmeturvet puudutavate juhiste suhtes on korraldatud piisavalt koolitusi ja informatsioon on personalile kättesaadav?	☐ Jah ☐ Osaliselt ☐ Ei
16. Kas on tagatud, et kogu personal ja kõik organisatsiooni tasandid mõistavad oma vastutust isikuandmete kaitse ja andmeturbe suhtes?	☐ Jah ☐ Osaliselt ☐ Ei
17. Kas olete taganud selle, et vaikimis- ja konfidentsiaalsuslepingud on töölepingu ja teenuslepingu osa?	☐ Jah ☐ Osaliselt ☐ Ei
18. Kas on olemas külastusreeglid külaliste tarvis ja kas neid praktikas rakendatakse?	☐ Jah ☐ Osaliselt ☐ Ei
19. Kas on rakendatud piisavaid meetmeid sissemurdmisest ja tulekahjudest tulenevate ning ruumidega seotud kahjude ärahoidmiseks?	☐ Jah ☐ Osaliselt ☐ Ei
20. Kas isikuandmete käideldavus[4] on tagatud infosüsteemi hoolde- ja halduslepingutega?	☐ Jah ☐ Osaliselt ☐ Ei
21. Kas on tagatud see, et isikuandmete töötlemise süsteemi ei pääse ilma asjakohaste volitusteta?	☐ Jah ☐ Osaliselt ☐ Ei
22. Kas pääsemine isikuandmete töötlemise süsteemi eeldab isiklikku kasutajatunnust ja parooli?	☐ Jah ☐ Osaliselt ☐ Ei
23. Kas isikuandmete kasutuse ja töötlemise õiguspärasust kontrollitakse regulaarselt?	☐ Jah ☐ Osaliselt ☐ Ei
24. Kas isikuandmete töötlemise süsteemi tarvis on olemas tagavarasüsteemid ja plaanid?	☐ Jah ☐ Osaliselt ☐ Ei
25. Kas olete taganud selle, et isikuandmete töötlemisega seotud ülesanded ja vastutusalad on konkreetselt määratletud?	☐ Jah ☐ Osaliselt ☐ Ei
26. Kas olete taganud selle, et isikuandmete kaitse ja andmeturbe eest vastutavad isikud ja nende asendamine on kindlaks määratud?	☐ Jah ☐ Osaliselt ☐ Ei
27. Kas andmeturbe alale on määratud vastutav isik?	☐ Jah ☐ Osaliselt ☐ Ei
28. Kui isikuandmete töötlemissüsteemi haldus on antud kolmanda osapoole ülesandeks, kas olete taganud selle, et lepingus on võetud arvesse kõik isikuandmete kaitse ja andmeturbega seotud kohustused?	☐ Jah ☐ Osaliselt ☐ Ei
29. Kas on olemas ja dokumenteeritud IT turbe-dokumentatsioon?	☐ Jah ☐ Osaliselt ☐ Ei

[3] Vaata juhendmaterjali delikaatsete isikuandmete töötlemise registreerimiseks.

[4] Vastavalt IKS §-le 25 on isikuandmete töötleja kohustatud kasutusele võtma organisatsioonilised, füüsilised ja infotehnilised turvameetmed isikuandmete kaitseks käideldavuse osas – juhusliku hävimise ja tahtliku hävimise eest ning õigustatud isikule andmete kättesaadavuse takistamise eest.

Infrastruktuuri turvalisus (Ruumide ja seadmete turvalisuse tagamine, kasutajate autentimine ja toimingute logimine)	
1. Kas andmete töötlemise ruumid ja IT süsteemid on piisavalt kaitstud tule, ülekuumenemise, vee, voolukõikumiste ja voolukatkestuste eest?	☐ Jah ☐ Osaliselt ☐ Ei
2. Kas on rakendatud piisav sissemurdmiste vastane kaitse?	☐ Jah ☐ Osaliselt ☐ Ei
3. Kas juurdepääs tähtsatele IT süsteemidele ja ruumidele on reguleeritud?	☐ Jah ☐ Osaliselt ☐ Ei
4. Kas külastajate, väliste tehnikute, hoolduspersonali jne külastustel saadab neid isik ja kas neid jälgitakse?	☐ Jah ☐ Osaliselt ☐ Ei
5. Kas riistvara ja tarkvara on regulaarselt uuendatavasse inventarinimekirja kantud?	☐ Jah ☐ Osaliselt ☐ Ei
6. Kas kõigile süsteemi kasutajatele on määratud rollid ja profiilid?	☐ Jah ☐ Osaliselt ☐ Ei
7. Kas on kindlaks määratud, millistele andmetele millised kasutajad ligi pääseda tohivad? Kas on rakendatud mõistlikke piiranguid?	☐ Jah ☐ Osaliselt ☐ Ei
8. Kas olete taganud kontrollsüsteemi andmete säilitamise turvalisuse nii, et sealt ei ole võimalik andmeid ilma vastavate volitusteta kustutada, lisada ega muuta?	☐ Jah ☐ Osaliselt ☐ Ei
9. Kas kõik töötajad on läbinud turvaliste paroolide valimise alase väljaõppe (parooli pikkus, keerukus, vahetamine jne)?	☐ Jah ☐ Osaliselt ☐ Ei
10. Kas kõik tööarvutid on töötaja lahkumisel parooliga ekraanisäästjaga kaitstud?	☐ Jah ☐ Osaliselt ☐ Ei
11. Kas olete täpselt määratlenud süsteemi pääsu ja paroolide vahetamisega seotud ülesanded?	☐ Jah ☐ Osaliselt ☐ Ei
12. Kas olete taganud selle, et kontrollsüsteem katkestab ühenduse, kui seda teatud aja vältel ei kasutata?	☐ Jah ☐ Osaliselt ☐ Ei
13. Kas olete taganud selle, et ühe ja sama kasutajanimega süsteemi sisenemiste arv on piiratud?	☐ Jah ☐ Osaliselt ☐ Ei
14. Kas olete taganud selle, et süsteem ei võimalda uusi sisenemiskatseid ja lukustab kasutajatunnuse, kui ebaõnnestunud sisenemiskatsete arv ületab teatud piiri?	☐ Jah ☐ Osaliselt ☐ Ei
15. Kas olete taganud selle, et ebaõnnestunud sisenemiskatsete kohta koostatakse raportid, mis saadetakse kontrolli eest vastutavale isikule?	☐ Jah ☐ Osaliselt ☐ Ei

16. Kas olete taganud selle, et süsteemi programmeerimist/administreerimist ja reaalset kasutamist teostavad erinevad isikud ning programmeerimis- ja kasutuskeskkonnad hoitakse lahus?	☐ Jah ☐ Osaliselt ☐ Ei
17. Kas olete taganud selle, et programmeerijatel puudub juurdepääs süsteemi salvestatud andmetele?	☐ Jah ☐ Osaliselt ☐ Ei
18. Kas delikaatsed isikuandmed ja eriti ohustatud süsteemid (nt sülearvutid) on piisavalt hästi kaitstud (kasutades näiteks krüpteerimist või muid viise)?	☐ Jah ☐ Osaliselt ☐ Ei
19. Kas olete kindlaks määranud, kes otsustab kasutusõiguse andmise?	☐ Jah ☐ Osaliselt ☐ Ei
20. Kas ruumid on jagatud teatud aladeks ja on kindlaks määratud, kellel on õigus missugusele alale pääsemiseks?	☐ Jah ☐ Osaliselt ☐ Ei
21. Kas olete taganud selle, et ligipääsuõigused vastavad töötaja tööülesannetest tulenevatele vajadustele seoses liikumistega ruumides, mis on seotud isikuandmete töötlemisega?	☐ Jah ☐ Osaliselt ☐ Ei
22. Kas olete taganud selle, et ligipääsuõigused tühistatakse töötaja lahkumisel töölt ?	☐ Jah ☐ Osaliselt ☐ Ei
23. Kas olete taganud selle, et avalikult kasutatavatest ruumidest ei pääse ilma volituseta ruumidesse, mida kasutatakse isikuandmete töötlemiseks?	☐ Jah ☐ Osaliselt ☐ Ei
24. Kas külastajate tarvis on koostatud külastuskord, mida ka tegelikkuses järgitakse?	☐ Jah ☐ Osaliselt ☐ Ei
25. Kas külastajate andmed, saabumis- ja lahkumisajad registreeritakse saabumisel ja lahkumisel?	☐ Jah ☐ Osaliselt ☐ Ei
26. Kas isikuandmete töötlejate ja lisapersonali (nagu turva- ja koristusteenuseid osutav personal) sissepääsuõigused ruumidesse on määratletud vastavalt nende poolt sooritatavate ülesannetele?	☐ Jah ☐ Osaliselt ☐ Ei
27. Kas ruumid, kus asuvad süsteemile ligipääsu võimaldavad arvutid ja ruumid, kus hoitakse isikuandmeid sisaldavaid dokumente, on kontrolli all ka peale tööaja lõppu?	☐ Jah ☐ Osaliselt ☐ Ei

Üldandmed asutuse infosüsteemist (Viirusetõrje ja tulemüüri kasutamine, andmete edastamine)	
1. Kas andmesüsteemi kasutamisel toimib kontrollisüsteem, mis talletab sisenemisajad ja kas nimetatud kontrollisüsteem on pidevalt rakendunud?	☐ Jah ☐ Osaliselt ☐ Ei
2. Kas olete taganud selle, et süsteemis on näha sisenenud kasutaja andmed, sisenemise aeg ning ühenduse katkestamise aeg?	☐ Jah ☐ Osaliselt ☐ Ei
3. Kas olete taganud selle, et süsteemi andmeid kustutades, lisades, vaadates või ajakohastades jäävad sinna andmed kasutaja, sooritatud meetme ja selle põhjuse kohta ning tegevuse kuupäev ja aeg?	☐ Jah ☐ Osaliselt ☐ Ei
4. Kas kasutate tulemüüri?	☐ Jah ☐ Osaliselt ☐ Ei
5. Kas tulemüüri seadistust ja toimimist kontrollitakse regulaarselt ja kriitilise pilguga?	☐ Jah ☐ Osaliselt ☐ Ei
6. Kas kasutate kogu süsteemi hõlmavaid viirustõrje programme?	☐ Jah ☐ Osaliselt ☐ Ei
7. Kas kõigi IT turvameetmete osas on sätestatud see, kas neid rakendatakse ühekordselt või regulaarselt (nt viirustõrje tarkvara uuendamine)?	☐ Jah ☐ Osaliselt ☐ Ei
8. Kas olete määranud kindlaks, milliseid andmekandjaid (CD-plaate, magnetlinte, kettaid jne) isikuandmete salvestamiseks kasutatakse?	☐ Jah ☐ Osaliselt ☐ Ei
9. Kas olete taganud selle, et isikuandmetega andmakandjaid hoitakse sellises kohas, kuhu pääs on vaid selleks volitatud isikuil?	☐ Jah ☐ Osaliselt ☐ Ei
10. Kas olete määranud kindlaks, kui tihti vananenud andmekandjaid kasutuselt kõrvaldatakse?	☐ Jah ☐ Osaliselt ☐ Ei
11. Kas on olemas ajakohane nimekiri võrguühenduste ja sidevahendite kohta?	☐ Jah ☐ Osaliselt ☐ Ei
12. Kas olete taganud selle, et on sätestatud kuidas isikuandmetega seotud paberkandjal olevaid dokumente käidelda?	☐ Jah ☐ Osaliselt ☐ Ei
13. Kas on tagatud see, et sisevõrgus puudub kõrvalistel isikutel ligipääs isikuandmetele?	☐ Jah ☐ Osaliselt ☐ Ei
14. Kas on tagatud see, et Internetti, nagu ka muudesse avalikesse andmesidevõrkudesse, ei ole otseühendust muul viisil kui spetsiaalse turvakontrolli kaudu?	☐ Jah ☐ Osaliselt ☐ Ei

Organisatsiooni üldine töökorraldus (Infoturbe siseeeskirjade kehtestamine ja töötajate vastav koolitamine)	
1. Kas olete taganud selle, et peale kasutuselt kõrvaldamist kolmandale isikule üle antud andmekandjast on andmed kustutatud?	☐ Jah ☐ Osaliselt ☐ Ei
2. Kas olete taganud selle, et andmekandjate turvalisuse tagavad lepingud ja kontroll vastavad nõuetele, kui andmekandja toimetatakse väljapoole bürood?	☐ Jah ☐ Osaliselt ☐ Ei
3. Kas olete kindlustanud, et süsteemist ei tehta isikuandmetest asjatuid paberväljatrükke ja et süsteemist tehtud väljatrükkide käitlemine on piisavalt hästi sätestatud?	☐ Jah ☐ Osaliselt ☐ Ei
4. Kas olete taganud, et dokumentide säilitamise, arhiveerimise ja utiliseerimise kohta on olemas piisavalt põhjalikud juhised ning õigusaktid?	☐ Jah ☐ Osaliselt ☐ Ei
5. Kas olete taganud selle, et tegevuse katkemise riskid (näiteks arvutite rikked või voolutoite katkestused) on kaardistatud (teadvustatud) ja nendeks ollakse valmis?	☐ Jah ☐ Osaliselt ☐ Ei
6. Kas on koostatud varukoopiate tegemise alane strateegia?	☐ Jah ☐ Osaliselt ☐ Ei
7. Kas on paika pandud, milliseid andmeid kui kaua säilitatakse?	☐ Jah ☐ Osaliselt ☐ Ei
8. Kas varukoopiate tegemine ja nendelt andmete taastamine on dokumenteeritud?	☐ Jah ☐ Osaliselt ☐ Ei
9. Kas on koostatud hädaolukorras tegutsemise plaan, mis sisaldab tegevusjuhiseid ja kontaktandmeid?	☐ Jah ☐ Osaliselt ☐ Ei
10. Kas kõik töötajad tunnevad hädaolukorra tegevusplaani ja kas see tegevusplaan on kõigile kättesaadav?	☐ Jah ☐ Osaliselt ☐ Ei