KINNITATUD
AS Atea tegevjuhi käskkirjaga nr 03.12.2020
nr 2-1/19/2020

ATEA AS ISIKUANDMETE TÖÖTLEMISE EESKIRJAD

I OSA
ÜLDSÄTTED

1. Isikuandmete töötlemise eeskirja (edaspidi tekstis – Eeskiri) eesmärk on sätestada isikuandmete töötlemine Atea AS-s (edaspidi – Ettevõte), tagades Eesti Vabariigi isikuandmete kaitse seaduse (edaspidi – IKS), Euroopa Parlamendi ja Nõukogu (EL) 2016. a. 27. aprilli määruse 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (Isikuandmete kaitse üldmäärus, edaspidi tekstis – GDPR) ja teiste õigusaktide, mis määravad kindlaks isikuandmete töötlemise ja kaitse, järgimise ja rakendamise.

2. Eeskirja eesmärk on sätestada peamised isikuandmete töötlemise, andmesubjekti õiguste rakendamise tehnilised ja andmekaitse korralduslikud meetmed.

3. Eeskirja sätted ei saa laiendada või kitsendada IKS-i ja GDPR-i kohaldamise valdkonda ning need ei saa olla vastuolus IKS-is ja GDPR-is sätestatud isikuandmete töötlemise nõuete ja teiste isikuandmete töötlemist sätestavate õigusaktidega.

4. Käesolevat Eeskirja peavad järgima kõik Ettevõtte töötajad (edaspidi – Töötajad), Ettevõttes praktikal olevad üliõpilased, kõik Ettevõtte elektroonilist ja muud süstematiseeritud teavet ja infosüsteeme kasutavad isikud ning Ettevõtte projektides osalevad muud füüsilised isikud (nt füüsilistest isikutest alltöövõtjad).

5. Eeskiri on koostatud, juhindudes IKS-ist ja GDPR-ist, Ettevõtte normatiivaktidest, teistest õigusaktidest, mis sätestavad isikuandmete kaitset ja õigust koguda isikuandmeid.

II OSA
KASUTATAVAD MÕISTED

6. Eeskirjas kasutatavad mõisted:

6.1. **Isikuandmed** – igasugune teave tuvastatud või tuvastatava füüsilise isiku (andmesubjekti) kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal

6.2. **Andmekaitseametnik** – isik, kes teavitab vastutavat töötlejat või volitatud töötlejat ja andmeid töötlevaid töötajaid nende kohustustest, jälgib GDPR-i, muude EL-i või siseriiklike andmekaitsesätete ja vastutava töötleja või volitatud töötleja isikuandmete kaitse põhimõtete täitmist, teostab kontaktisiku funktsioone kui järelevalveasutus pöördub andmetöötlusega seotud küsimustes.

6.3. **Andmete saaja** – juriidiline või füüsiline isik, kellele esitatakse Ettevõttes olevad isikuandmed, kuid kellele Ettevõte kui vastutav töötleja ei pane ülesandeks selliseid andmeid töödelda või Ettevõte kui volitatud töötleja ei anna kohustuseks selliseid andmeid töödelda (alltöötlus).

6.4. **Andmete kasutaja** – Ettevõtte töötaja, kes töötab töölepingu alusel, füüsilisest isikust ettevõtja, Ettevõttes praktikal olev üliõpilane või Ettevõttes käimasolevasse projekti kaasatud isik või kolmanda isiku esindaja, kellel on õigus andmeid kasutada teatavate ettenähtud funktsioonide täitmiseks.

6.5. **Andmesubjekti nõusolek –** vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega. Isikuandmete töötlemise nõusolek tuleb anda selgelt ehk kirjalikult, sellega võrdsustatud või muus vormis, mis tõendab andmesubjekti tahet.

6.6. **Andmete esitamine** – isikuandmete avaldamine, edastades või muul moel muutes neid kättesaadavaks (välja arvatud avalikustamine massiteabevahendite kaudu).

6.7. **Andmete töötlemine** – isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine.

6.8. **Andmete volitatud töötleja** – füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötleja nimel.

6.9. **Andmete vastutav töötleja** – juriidiline või füüsiline isik, avaliku sektori asutus, amet või muu organ, kes üksi või koos teistega määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid.

6.10. **Elektrooniline teave** – teave, mida hallatakse ja töödeldakse infotehnoloogia (edaspidi – IT) vahenditega (arvutid, tahvelarvutid, nutitelefonid, tööjaamad jne). Tegemist on infosüsteemide andmete, failide, dokumentide ja muu teabega, mis luuakse, mida säilitatakse ja edastatakse IT vahendite abil.

6.11. **Infotehnoloogia** (IT) – tähendab elektroonilise teabe (andmete) haldamise ja töötlemise tehnoloogiat, sealhulgas telekommunikatsiooni, arvutiriistvara, tarkvara ning muid tootmise ja haldamise kõrgtehnoloogiaid.

6.12. **Eriliiki isikuandmed** – andmed, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilised andmed, füüsilise isiku kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed, terviseandmed või andmed füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta..

6.13. **Muu süstematiseeritud teave –** teave paberkandjal, mis on süstematiseeritud ja mida töödeldakse automatiseerimata viisil.

6.14. **Arvutid** – arvutid, nende osad, lisaseadmed (monitorid, skannerid, printerid ja koopiamasinad, klaviatuurid, hiired, kõlarid, kõrvaklapid, videokaamerad, fotoaparaadid jne), arvutivõrguseadmed, arvuti- ja võrguseadmete kinnituskapid, katkematud vooluallikad jne.

6.15. **Konfidentsiaalsus** – teabe konfidentsiaalsustunnus, mis nõuab, et teave oleks kättesaadav ainult selleks volitatud isikutele.

6.16. **Ligipääsetavus** – teave võib olla teatud isikute poolt kättesaadav, kasutatav, töödeldav igal ajahetkel.

6.17. **Tarkvara** – arvutiprogrammid, mis on ette nähtud riistvara kasutamiseks ja kasutaja ülesannete lahendamiseks arvuti kaudu (operatsioonisüsteemid, programmeerimissüsteemid, bürooprogrammide paketid, viirusetõrje, arhiveerimise ja muud programmid);

6.18. **Turvalisus** – teabe konfidentsiaalsuse, terviklikkuse ja kättesaadavuse tagamine.

6.19. **Terviklikkus** – algse teabe tõepärasus, usaldusväärsus ja autentsus; selline teave ja selle allikas peavad olema kaitstud igasuguse juhusliku, eksliku, volitamata / ebaseadusliku muutmise või kadumise eest, kõik muudatused on teada.

7. Muud Eeskirjas kasutatavad mõisted vastavad mõistetele, mis on sätestatud GDPR-is.

III OSA
ISIKUANDMETE TÖÖTLEMISE EESMÄRGID, PÕHIMÕTTED JA ÕIGUSLIKUD ALUSED

8. Ettevõte kui isikuandmete vastutav töötleja sätestab alljärgnevad isikuandmete töötlemise eesmärgid:

8.1. Sisemise haldamise eesmärk – tööandja teostatav töötajate andmete haldamine, töölepingute nõuetekohane täitmine. Sel eesmärgil töödeldakse andmeid juriidilise kohustuse, õigustatud huvi, andmesubjektiga sõlmitud lepingu alusel;

8.2. Sisekommunikatsiooni eesmärk – Ettevõtte töötajate isikuandmete töötlemine, et tagada töötajate efektiivne suhtlemine ja siseteabe levitamine: intranet (SharePoint), Skype for Business, Teams, sisetelefon, muud sisekommunikatsioonikanalid, siseürituste korraldamine töötajatele jne. Sel eesmärgil töödeldakse andmeid õigustatud huvi, nõusoleku alusel (kui see on vajalik);

8.3. Väliskommunikatsiooni eesmärk – Ettevõtte töötajate, aga ka teiste isikute isikuandmete töötlemine, et Ettevõte saaks teostada põhikirjas nimetatud tegevusi ja mis tahes muud seaduslikult teostatavat tegevust: osalemine välisüritustel, turundusprojektid, teiste ettevõtete / asutuste / organisatsioonide või muude isikutega sõlmitud lepingute täitmine. Sel eesmärgil töödeldakse andmeid õigustatud huvi, andmesubjektiga sõlmitud lepingute, nõusoleku alusel (kui see on vajalik);

8.4. Töötajate tervise ja ohutuse tagamise eesmärk – Ettevõte kui tööandja töötleb andmeid töötajate tervise ja muu tööohutuse kohta. Sel eesmärgil töödeldakse andmeid juriidilise kohustuse alusel;

8.5. Töötajate värbamise eesmärk – Ettevõte töötleb töölesoovijate andmeid, mis on vajalikud Ettevõttele sobiva töötaja valimiseks vabale ametikohale. Sel eesmärgil töödeldakse andmeid andmesubjekti nõusoleku (kui Ettevõte pöördub töölesoovija poole) või andmesubjektiga lepingueelsete suhete alusel (kui töölesoovija pöördub Ettevõtte poole), GDPR artikli 6 lõige 1 punkt b alusel;

8.6. IT halduse eesmärk – Ettevõte töötleb töötajate ja teiste isikute erinevaid andmeid, mida luuakse ja kogutakse, kui sellised isikud liituvad ja kasutavad Ettevõtte IT tööriistu, arvutiseadmeid, infosüsteeme jne. Sel eesmärgil töödeldakse andmeid õigustatud huvi alusel;

8.7. tehniliste probleemide lahendamine – kõik tehnilised probleemid registreeritakse Ettevõttes ja neid hallatakse selliste sisesüsteemide kaudu nagu ServiceNow, SysAid jne. Sel eesmärgil töödeldakse andmeid õigustatud huvi alusel;

8.8. ärisuhete hoidmine partnerite, klientide, tarnijatega, lepingute nõuetekohane täitmine – lepingud, muud lepingutega seotud dokumendid (aktid, sertifikaadid, arved, kirjad jne), Microsoft Dynamics NAV. Sel eesmärgil töödeldakse andmeid õigustatud huvi alusel;

8.9. isiku ja vara kaitse eesmärk, seaduserikkumiste tuvastamine – et saavutada nimetatud eesmärgid, teostab Ettevõte videovalvet ja salvestamist vastavalt kehtivale korrale. Sel eesmärgil töödeldakse andmeid õigustatud huvi alusel;

8.10. ruumidesse juurdepääsu kontrollimine, vara kaitse tagamine – juurdepääsu Ettevõtte ruumidele kontrollitakse elektrooniliste vahenditega. Sel eesmärgil töödeldakse andmeid õigustatud huvi alusel.

9. Ettevõte võib seada ka muid andmetöötluse eesmärke, mida tuleb kirjeldada Ettevõtte isikuandmete töötlemise ja haldamise eesmärgil kasutatavas süsteemis OneTrust *(ATEA Privacy Management Tool – APMT).* Isikuandmete töötlemiseks mis tahes eesmärgil peab

kehtima vähemalt üks GDPR-is sätestatud seaduslikust andmete töötlemise alustest, mis on konkreetselt täpsustatud APMT-s.

10. Töötajate isikuandmete kategooriad, töötlemise eesmärgid, õiguslik alus, töötlemise tähtaeg ja koht on välja toodud Ettevõtte sisevõrgus jaotises „GDPR“.

11. Isikuandmeid tuleb töödelda, järgides alljärgnevaid põhimõtteid:

11.1. andmesubjekti suhtes töödeldakse neid seaduslikul, ausal ja läbipaistval viisil (seaduslikkuse, aususe ja läbipaistvuse põhimõte);

11.2. neid kogutakse kindlaks määratud, selgelt sõnastatud ning seaduslikel eesmärkidel ega töödelda edaspidi nende eesmärkidega kokkusobimatul viisil; edasist andmete töötlemist arhiveerimise eesmärgil avalikes huvides ei loeta esialgse eesmärgiga (eesmärgi piirangu põhimõte) vastuolus olevaks;

11.3. kogutavad andmed on asjakohased, sobivad ja ainult need, mida vajatakse eesmärkide, mille jaoks neid töödeldakse, saavutamiseks (andmete koguse vahendamise põhimõte);

11.4. Andmed on õiged ja vajadusel ajakohastatud; eesmärk on võtta tarvitusele kõik mõistlikud meetmed tagamaks, et töötlemise eesmärgi seisukohast ebaõiged andmed kustutatakse või parandatakse viivitamata (õigsuse põhimõte);

11.5. andmed säilitatakse sellisel kujul, et andmesubjekti isikusamasust poleks võimalik kindlaks teha kauem, kui see on vajalik neil eesmärkidel, milleks isikuandmeid töödeldakse; isikuandmeid võib pikema aja jooksul säilitada, kui isikuandmeid töödeldakse vaid arhiveerimise eesmärgil avalikes huvides, rakendades asjakohaseid tehnilisi ja korralduslikke meetmeid, mida nõuab GDPR, et kaitsta andmesubjekti õigusi ja vabadusi (säilitamisaja piiramise põhimõte);

11.6. andmeid töödeldakse sel viisil, et rakendades vastavaid tehnilisi või organisatsioonilisi meetmeid, oleks tagatud isikuandmete turvalisus, kaasa arvatud kaitse andmete ilma loata töötlemise eest või andmete ebaseadusliku töötlemise eest ja juhusliku kaotamise, hävitamise või kahjustumise eest (terviklikkuse ja konfidentsiaalsuse põhimõte);

11.7. Ettevõte vastutab selle eest, et järgitaks käesoleva Eeskirja alapunkte 11.1-11.6 ja ta peab suutma tõestada, et neid järgitakse (vastutuse põhimõte).

IV OSA
ISIKUANDMETE TÖÖTLEMISE JA KAITSE PEAMISED NÕUDED

12. Ettevõtte töötajad on oma töökohustuste täitmisel ja isikuandmete töötlemisel kohustatud järgima isikuandmete töötlemise peamisi nõudeid:

12.1. isikuandmeid töödeldakse, järgides Eeskirjas nimetatud põhimõtteid;

12.2. infosüsteemide väljatöötamise, juurutamise, hooldamise ja nõustamise teenuste osutamise lepingute täitmisel ei tohi testida tegelikke isikuandmeid, suheldes tekkinud probleemide küsimustes, esitatakse dokumentatsioonis ekraanipilt (inglise keeles *printscreen*), millest tuleb isikuandmed eemaldada või neid varjata;

12.3. enne isikuandmete saatmist e-posti teel tuleb andmed krüpteerida, avamisvõti esitada eraldi e-kirjaga või muu sidekanali (näiteks SMS) kaudu.

13. Isikuandmeid kogutakse Ettevõttes, saades neid:

13.1. otse andmesubjektilt;

13.2. isikuandmete esitamise lepingu alusel (mitmekordse isikuandmete kogumise korral);

13.3. andmete vastutavalt töötlejalt, esitades taotluse, milles peab olema märgitud isikuandmete kasutamise eesmärk, andmete esitamise ja vastuvõtmise õiguslik alus ning taotletud isikuandmete ulatus (ühekordse isikuandmete kogumise korral);

13.4. isiku nõusolekul;

13.5. kommertslepingutest, kui neis nimetatakse teise poole vastutavate töötajate või teiste isikute kontaktandmed;

13.6. andmed loob Ettevõte.

14. Isikuandmete säilitamise tähtajad ja pärast selle tähtaja möödumist tehtavad toimingud on määratud kindlaks isikuandmete töötlemist reguleerivate õigusaktidega, kui andmeid töödeldakse juriidilise kohustuse alusel.

15. Isikuandmeid ei säilitata kauem, kui seda nõuavad andmete töötlemise eesmärgid. Kui isikuandmed ei ole enam vajalikud nende töötlemise eesmärkidel, need hävitatakse, välja arvatud need andmed, mis tuleb säilitada õigusaktidest tulenevaid tähtaeguja Ettevõtte sisenormdokumente järgides.

16. Lepingutes sätestatud isikuandmete töötlemine:

16.1. lepingutes sätestatud isikuandmed säilitatakse pärast lepingu täitmist arhiveerimise eesmärkidel, need hävitatakse, juhindudes õigusaktidest tulenevatest säilitamise tähtaegadest ja Ettevõtte sisenormdokumentidest;

16.2. isikuandmete, mida töödeldakse sõlmitud Andmetöötluslepingute alusel, säilitamise tähtaja määrab andmetöötlusleping.

17. Andmesubjektide isikuandmed, kui on lõppenud ette nähtud isikuandmete säilitamise tähtaeg, kustutatakse Ettevõtte töödeldavatest andmebaasidest, kui andmesubjektide isikuandmed on edastatud andmete saajatele – andmesubjekte teavitatakse isikuandmete töötlemise lõpetamisest.

18. Õigusaktidega kehtestatud juhtudel ja korras võib Ettevõte edastada tema poolt töödeldavaid isikuandmeid kolmandatele isikutele, kellele Ettevõte on seaduse või muude õigusaktidega kohustatud isikuandmeid edastama andmesaaja nõudmisel (ühekordse edastuse korral) või Ettevõtte ja andmete saaja vahel sõlmitud isikuandmete edastamise lepingu alusel (mitmekordse edastuse korral), samuti Ettevõtte poolt sõlmitud kommertslepingute alusel ning sõlmides andmetöötluslepinguid.

19. Andmete saaja taotlused ja andmeedastuslepingud peavad vastama GDPR artikli 6 nõuetele.

V OSA
ERINÕUDED ISIKUANDMETE TÖÖTLEMISEKS

20. Ohutu juurdepääs teabele tagatakse järgmiste meetmetega:

20.1. viiakse läbi IT süsteemide muudatuste haldamine;

20.2. juurdepääsud antakse, juhindudes põhimõttest „vaja teada“;

20.3. perioodiliselt viiakse läbi juurdepääsu informatsiooniressursside ning läbipääsukaartide ülevaatus;

20.4. turva- (lukustus-) süsteem kontrollib Ettevõtte ruumidesse sisenemist;

20.5. kasutatakse signalisatsiooni (sissemurdmine, tulekahju);

20.6. paberkandjatel isikuandmeid hoitakse ainult lukustatavates sahtlites ja/või kappides;

20.7. järgitakse puhta laua ja ekraani poliitikat;

20.8. arvutivõrgus tuvastatakse kasutajaid kooskõlas nende arvutile omistatud IP aadressiga; oma arvutisse ja serveritesse logivad tarbijad sisse, kasutades neile antud kasutajanimesid ja isiklikke paroole, autentimise ja autoriseerimise kontrolli teostavad arvuti ja serveri operatsioonisüsteemid ja rakenduslikud tarkvarad;

20.9. serveriruumidesse sissepääsu omavad ainult Ettevõtte direktori käskkirjaga volitatud isikud;

20.10. juurdepääs serverite operatsioonisüsteemide juhtimisele ning konfigureerimisele on lubatud ainult süsteemide administraatoril;

20.11. kui arvutit ja/või mobiilseadet ei kasutata, siis peavad nende ekraanid olema lukustatud;

20.12. välised andmekandjad on krüptitud, krüpteerimata andmekandjatel isikuandmeid ei säilitata;

20.13. sülearvutites olev teave on kaitstud operatsioonisüsteemi kasutaja nime ning parooliga, kõvaketas on krüptitud.

21. Kasutajate tuvastamine:

21.1. paroole kasutatakse kõigil tasanditel – alates arvuti sisse lülitamisest kuni programmi käivitamiseni ja andmebaasi sisse logimiseni;

21.2. paroolidele kehtestatakse erinõuded (parooli perioodiline kohustuslik muutmine, parooli pikkuse ja keerukuse piirangud, vanu paroole ei ole lubatud kasutada);

21.3. kasutatakse kahetasemelist autentimist.

22. Mitte süsteemsete vahenditega töödeldav teave (nt Wordi, Exceli, PowerPointi meetoditega loodud elektrondokumendid, Outlooki programmis kirjavahetused) peab olema klassifitseeritud dokumendi sisu arvestades.

23. Isikuandmed (välja arvatud eriliigilised isikuandmed) peavad olema klassifitseeritud kui Confidential \ Personal data ja neid võib saata ainult krüptitud kanaliga (TLS protokoll), veendudes, et isikuandmete saaja võtab andmed vastu sama turvaliselt, kasutades TLS protokolli.

24. Eriliigilised isikuandmed peavad olema klassifitseeritud kui Strictly confidential \ Personal data ja neid võib säilitada ainult krüptitult. Taolise iseloomuga teavet ei tohi üldistada ilma teabe omaniku kinnituseta. Kinnituse olemasolul võidakse andmeid saata ainult krüptitud kujul (TLS protokoll), veendudes, et isikuandmete saaja võtab andmed vastu sama turvaliselt, kasutades TLS protokolli.

25. Kõik ettevõtte veebilehed ja infosüsteemid, millesse logitakse sisse brauseri kaudu, peavad omama juurutatud SSL sertifikaati.

26. Töötajate arvutites olevad arvutitoimikud, kuhu isikuandmed kogutakse, ei tohi olla ligipääsetavad teistele arvutikasutajatele.

27. Andmete turvalisuse tagamiseks tehakse kasutatavate andmebaaside varukoopiad, mida hallatakse, juhindudes LST ISO/IEC 27001:2013 standardi nõuetest. Isikuandmeid sisaldavad varukoopiad krüptitakse.

28. Kui muutuvad dokumente ja toimikuid töötlevad Ettevõtte töötajad või nende volitused, siis antakse personali-, finants- ja raamatupidamistoimikud ning muud arhiivi- ja arvutitoimikud uuele töölevõetud ja isikuandmete töötlemisega tegelema määratud Töötajale üle üleandmise-vastuvõtmise aktiga.

29. Enne seda, kui Ettevõtte töötajate isikutoimikud antakse säilitamiseks üle dokumentide arhiveerimisega tegelevale ettevõttele, kellega on sõlmitud dokumentide töötlemise (arhiveerimise) leping, hoitakse neid Ettevõtte arhiivis lukustatavas dokumendihoidlas. Neid andmeid antakse kolmandatele isikutele tutvumiseks ainult neil juhtudel, kui see on lubatud seaduste ja muude õigusaktide järgi, või ainult Ettevõtte direktori või tema volitatud isiku otsuse alusel.

30. Trükkimine dokumendilehe teisele poolele on rangelt keelatud. Mittevajalikud dokumendid tuleb hävitada.

31. Mittevajalikud dokumendid või dokumendid, mille säilitamise tähtaeg on lõppenud, Ettevõtte dokumendid, mis sisaldavad isikuandmeid, ja nende koopiad tuleb hävitada nii, et neid dokumente ei oleks võimalik taastada ega nende sisu ära tunda.

32. Mitmekordse salvestusvõimalusega andmekandjatele (nt SSD, HDD, USB võtmed, väliskettad, mälukaardid, mobiiltelefonid) salvestatud teave hävitatakse, kasutades spetsiaalse tarkvaraga seadet või hävitatakse andmekandja füüsiliselt.

33. Mittevajalikud CD ja DVD andmekandjad tuleb hävitada füüsiliselt.

34. Enne arvuti teisele isikule kasutada andmist tuleb arvuti ümber installeerida.

35. Arvutiseadmed tuleb ümbertöötlemisse anda ilma andmekandjateta.

36. Enne mobiiliseadmete (nt telefonide, tahvelarvutite) teisele isikule kasutada, remonti või ümbertöötlemisse andmist tuleb seadme mälu puhastada ning taastada seadme tehaseparameetrid (inglise keeles *factory reset, master reset*) ja mälukaardid välja võtta.

37. Andmesubjektide esitatud dokumendid ja nende koopiad, rahastamise, raamatupidamise, arhiveerimise või muud toimikud, mis sisaldavad isikuandmeid, säilitatakse lukustatavates kappides, seifides või ruumides. Dokumente, mis sisaldavad isikuandmeid, ei ole lubatud hoida kõigile ligipääsetavas nähtavas kohas, kus selleks õigust mitteomavad isikud võivad nendega takistamatult tutvuda.

38. Andmekaitse tagatakse, juhindudes:

38.1. IKS-ist;

38.2. GDPR-ist;

38.3. standardist ISO/IEC 27001:2013;

38.4. muudest õigusaktidest, mis reguleerivad andmetöötluse seaduslikkust ja andmekaitse haldust.

VI OSA
NÕUDED ISIKUTELE, KES TÖÖTLEVAD ISIKUANDMEID

39. Ligipääsu isikuandmetele võib anda vaid sellele Töötajale, kes vajab isikuandmeid tema ametijuhendis või teiste õigusaktidega sätestatud funktsioonide täitmiseks, st juhindudes põhimõttest „vaja teada“.

40. Isikuandmetega saab teha ainult neid toiminguid, mille teostamiseks on Töötajale antud õigused. Töötaja, kes töötleb isikuandmeid, on kohustatud:

40.1. koguma isikuandmeid kindlaksmääratud ja seaduslikel eesmärkidel, mis on sätestatud õigusaktides, ja töötlema nende eesmärkidega kooskõlastatud viisil;

40.2. kogudes ja töödeldes isikuandmeid, järgima eesmärgipärasuse ja proportsionaalsuse põhimõtet, mitte nõudma andmesubjektidelt andmeid, mis ei ole vajalikud, mitte koguma ja mitte töötlema mittevajalikke andmeid;

40.3. säilitama isikuandmeid sellisel kujul, et andmesubjektide isikusamasust ei saaks tuvastada kauem, kui seda on vaja, eesmärgi, mille jaoks neid andmeid koguti ja töödeldakse, täitmiseks;

40.4. järgima isikuandmete töötlemise ning turvalisuse nõudeid, mis on sätestatud IKS-is, Eeskirjas ja muudes õigusaktides;

40.5. järgima konfidentsiaalsuspõhimõtet ja hoidma saladuses igasugust isikuandmetega seotud teavet, millega ta tutvus, täites oma funktsioone, välja arvatud siis, kui selline teave tuleb avalikustada vastavalt kehtivatele seadustele või teistele õigusaktidele. Kohustus säilitada isikuandmetega seotud saladust kehtib ka siis, kui minnakse üle teisele ametikohale või lõpevad töösuhted Ettevõttega;

40.6. järgima Eeskirjas sätestatud organisatoorseid ja tehnilisi isikuandmete turvalisuse meetmeid, et vältida isikuandmete juhuslikku või ebaseaduslikku hävitamist, muutmist, avalikustamist ja muud isikuandmete ebaseaduslikku töötlemist, kaitsma dokumente, andmekandjaid ja andmebaasides hoitavaid andmeid ning vältima mittevajalike koopiate tegemist;

40.7. mis tahes viisil mitte avalikustama, mitte andma edasi ega tegema ükskõik milliste vahendite kaudu kättesaadavaks võimalust tutvuda isikuandmetega ühelegi isikule, kes ei ole volitatud töötlema isikuandmeid;

40.8. teavitama viivitamata otsest ülemust ja andmekaitseametnikku mis tahes kahtlasest olukorrast, mis võib ohustada Ettevõtte poolt töödeldavate isikuandmete turvalisust;

40.9. tundma huvi isikuandmete kaitse aktuaalsete küsimuste ja probleemide vastu, tõstma isikuandmete kaitse kvalifikatsiooni;

40.10. järgima muid Eeskirjas ja isikuandmete kaitset reguleerivates õigusaktides sätestatud nõudeid.

41. Kõik Töötajad peavad allkirjastama vastava konfidentsiaalsuskohustuse vormi, mida säilitatakse Töötaja isikutoimikus.

42. Töötaja kaotab õiguse töödelda isikuandmeid pärast Ettevõttega töösuhte lõppemist või Ettevõtte juhi otsusel või kui ta määratakse täitma isikuandmete töötlemisega mitteseotud funktsioone.

VII OSA
ISIKUANDMETE SAAMINE JA ESITAMINE, KASUTADES RIIKLIKKE INFOSÜSTEEME JA REGISTREID

43. Olenevalt täidetavatest ülesannetest ja funktsioonidest on töötajatel juurdepääs ühele või mitmele riiklikule infosüsteemile, kust saadakse ja kuhu edastatakse isikuandmeid ulatuses, mis on vajalik juriidilise kohustuse täitmiseks.

VIII OSA
ANDMEKAITSEAMETNIK

44. Ettevõtte juht määrab andmekaitseametniku (dpo@atea.lt).

45. GDPR-i § 39 sätestatud peamised andmekaitseametnikule määratud ülesanded on:

45.1. Ettevõtte juhtkonna ja andmeid töötlevate töötajate teavitamine nende kohustustest GDPR-i ja teiste Euroopa Liidu õigusaktide, mis sätestavad isikuandmete töötlemist, sätete alusel;

45.2. GDPR-i, teiste Euroopa Liidu või riiklike andmekaitsealaste õigusaktide ja Ettevõtte isikuandmete töötlemise reeglite täitmise jälgimine, sealhulgas vastutuse määramine, vastutustundlike töötajate teadlikkuse tõstmine ja koolitamine ning sellega seotud auditid;

45.3. Andmekaitse mõju hindamise nõustamine ja seire;

45.4. Koostöö järelevalveasutusega;

45.5. Tegutsemine järelevalveasutuse kontaktisikuna andmetöötlusega seotud küsimustes, sealhulgas eelnev konsulteerimine ja nõustamine kõigis muudes küsimustes.

46. Andmekaitseametniku õigused ja kohustused on üksikasjalikult kirjeldatud GDPR-is, Ettevõtte sisedokumendis GDPR-RD01, kui sellel ametikohal on Ettevõtte töötaja, või teenuse osutamise lepingus, kui andmekaitseametniku ametikohal olev isik on ettevõtteväline teenuseosutaja.

IX OSA
LÕPPSÄTTED

47. Isikuandmeid elektroonilise side valdkonnas töödeldakse vastavalt Eesti Vabariigi elektroonilise side seadusele, IKS-ile , GDPR-ile ja Eesti Vabariigi küberturvalisuse seadusele.

48. Isiku, kelle andmeid töödeldakse, õigused sätestab IKS ja GDPR.

49. Töötajatele tutvustatakse käesolevat Eeskirja Ettevõttes sätestatud korras.

50. Ettevõtte poolt teostatud videovalve andmete töötlemise nõuded, andmesubjektide õigused, nende rakendamise kord ja andmesubjektide taotluste läbivaatamise kord kinnitatakse eraldi dokumentidega ja avaldatakse Ettevõtte veebilehel.

51. Eeskirja järgimise järelevalve ja kontrolli eest vastutavad Ettevõtte allüksuste juhid, Ettevõtte juht.