

Lisa
RMK ja [Company]
vahelise [Vali kuupäev] lepingu nr
[Sisesta number] juurde

ISIKUANDMETE TÖÖTLEMISE NÕUDED VOLITATUD TÖÖTLEJALE

[Vali kuupäev]

(hiliseima digitaallkirja kuupäev)

1. Üldine
- 1.1. Riigimetsa Majandamise Keskus (RMK) (edaspidi vastutav töötleja) edastab [Company] (edaspidi volitatud töötleja) punktis 2.1 nimetatud andmed ja volitab volitatud töötlejat neid andmeid töötleva ainult juhul, kui andmete töötlemine on lepingust tulenevalt vajalik.
- 1.2. Käesoleva lisa eesmärk on kokku leppida volitatud töötleja õigustes ja kohustuses lepingu täitmise käigus saadud isikuandmete töötlemisel, millest pooled juhinduvad lepingu täitmisel.
- 1.3. Vastuolude korral lepingu ja käesoleva lisa sätete vahel tuleb juhinduda käesoleva lisa sätetest.

2. Isikuandmete töötlemise eesmärk ja kirjeldus

- 2.1. Vastutav töötleja kirjeldab ära isikuandmete töötlustoimingud tabelis 1, milles sätestatakse:
- 2.1.1. andmete töötlemise eesmärgi/eesmärgid, milleks isikuandmeid vastutava töötleja nimel töödeldakse;
- 2.1.2. andmesubjektide kategooriad, kelle isikuandmeid töödeldakse;
- 2.1.3. töödeldavate isikuandmete koosseis;
- 2.1.4. töötlemise alused;
- 2.1.5. andmete säilitustähtajad.

Kommenteerinud [KH1]: Täida tabel 1

Töötlemise eesmärk	Andmete kategooriad	Andmete koosseis	Töötlemise alused	Säilitustähtajad

--	--	--	--	--

Tabel 1. Isikuandmete töötlustoimingute tabel

3. Isikuandmete töötlemise kestus ja säilitamise nõuded

- 3.1. Volitatud töötleja töötleb isikuandmeid üksnes minimaalses vajalikus mahus ja lepingus kindlaksmääratud aja jooksul, välja arvatud juhul, kui volitatud töötleja on kohustatud teavet töötlema volitatud töötleja suhtes kohalduva seaduse alusel.
- 3.2. Käesoleva lisa raames tuleb andmeid säilitada vastavalt tabelis 1 sätestatud ajale. Selle aja möödudes tuleb andmed volitatud töötleja süsteemidest kustutada.
- 3.3. Peale teenuslepingu lõppemist tuleb vastutava töötleja teave volitatud töötleja hallatavatest süsteemidest turvaliselt kustutada, küsides enne selleks vastutavalt töötlejalt kirjaliku kinnituse. Kinnituse küsimisel tuleb kirjeldada plaanitav turvalise kustutuse meetod.

4. Nõuded volitatud töötlejale

- 4.1. Volitatud töötleja on kohustatud kasutama ja töötlema **tabelis 1** olevaid andmeid üksnes lepingu täitmiseks ja vastutava töötleja dokumenteeritud juhiste alusel, välja arvatud juhul, kui volitatud töötleja on kohustatud teavet töötlema volitatud töötleja suhtes kohalduva õiguse alusel. Viimati nimetatud juhul teavitab volitatud töötleja vastutavat töötlejat vastava kohustuse olemasolust enne teabe töötlemist, kui selline teavitamine ei ole olulise avaliku huvi tõttu volitatud töötleja suhtes kohalduva õigusega keelatud.
- 4.2. Volitatud töötleja peab täitma kõiki kehtivaid andmete töötlemisalaseid nõudeid, andmete turvalisust puudutavaid ning andmete kaitse alaseid Euroopa Liidu ja Eesti Vabariigi õigusakte ja muid eeskirju.
- 4.3. Volitatud töötleja on kohustatud aitama vastutavat töötlejat järgmiste nõuete täitmise tagamisel, võttes arvesse andmetöötluste laadi ja volitatud töötlejale kättesaadavat teavet:
 - 4.3.1. kohustus hinnata kavandatavate töötlemistoimingute mõju isikuandmete kaitsele (edaspidi „andmekaitsealane mõjuhinnang“), kui teatava töötlemisviisiga kaasneb tõenäoliselt suur oht füüsiliste isikute õigustele ja vabadustele;
 - 4.3.2. kohustus tagada isikuandmete õigsus ja ajakohasus, teavitades vastutavat töötlejat viivitamata, kui volitatud töötleja saab teada, et tema töödeldavad isikuandmed on ebaõiged või aegunud;
 - 4.3.3. kohustus teavitada vastutavat töötlejat kohe, kui vastutava töötleja nõuded ja juhised lähevad volitatud töötleja arvates vastuollu isikuandmete kaitse üldmäärusega või kohaldatavate liidu või liikmesriigi andmekaitsealaste sätetega.

5. Alamtöötleva kaasamine

- 5.1. Volitatud töötleva ei telli käesolevate nõuete kohaselt vastutava töötleva nimel tehtavate töötlemistoimingute tegemist alamtöötlevalt ilma vastutava töötleva eelneva kirjaliku eriloata. Volitatud töötleva esitab eriloa taotluse vähemalt 14 kalendripäeva enne kõnealuse alamtöötleva kaasamist koos teabega, mis on vajalik, et vastutav töötleva saaks loa kohta otsuse teha. Luba registreeritakse lepingu külge lisana.
- 5.2. Kui volitatud töötleva kaasab konkreetsete töötlemistoimingute tegemiseks (vastutava töötleva nimel) alamtöötleva, teeb ta seda lepinguga, millega kehtestatakse alamtöötlevale sisuliselt samad andmekaitsealased nõuded, mis on volitatud töötleva käesolevate nõuete kohaselt.
- 5.3. Volitatud töötleva tagab, et alamtöötleva täidab volitatud töötleva suhtes käesolevaid nõudeid.
- 5.4. Volitatud töötleva jääb vastutava töötleva ees täielikult vastutavaks alamtöötleva nõuete täitmise eest vastavalt volitatud töötleva sõlmitud lepingule. Volitatud töötleva teavitab vastutavat töötlevat, kui alamtöötleva ei täida oma lepingulisi nõudeid.

6. Tehnilised ja korralduslikud meetmed, sealhulgas tehnilised ja korralduslikud meetmed andmete turvalisuse tagamiseks

- 6.1. Volitatud töötleva kohustub tarvitusele võtma asjakohased tehnilised ja korralduslikud meetmed lepingu alusel toimuva andmete töötlemise loata või ebaseadusliku töötlemise, juhusliku kaotamise või hävitamise või kahjustumise vältimiseks.
- 6.2. Volitatud töötleva tagab organisatsioonisisese metoodilise ja süstemaatilise infoturbe haldamise, eelistatult laialdaselt tunnustatud turvasmetoodika põhjal (nt ISO/IEC 27001, SOC2, CIS Security Controls, Eesti riiklik infoturbe standard E-ITS vms), sh rakendades:
 - 6.2.1. infoturbe riskihalduse;
 - 6.2.2. varahalduse, sh arvestades RMK varadega;
 - 6.2.3. infoturbe rollide ja vastutuse kindlaksmääramine;
 - 6.2.4. pääsuõiguste halduse;
 - 6.2.5. turvaintsidentide halduse;
 - 6.2.6. jätkuvuse halduse, sh oma tarneahela ulatuses;
 - 6.2.7. tööjaamade ja teiste IT-seadmete ja tarkvarade tugevdamise ja konfiguratsioonihalduse;
 - 6.2.8. kahjurvara tõrje;
 - 6.2.9. krüptograafiliste meetmete halduse;
 - 6.2.10. auditiligi ja turvaseire olemasolu;
 - 6.2.11. nõrkuse ja paigalduse;
 - 6.2.12. füüsiliste turvameetmete halduse;
 - 6.2.13. turvameetmete perioodilise läbivaatuse (vähemalt kord aastas).
- 6.3. Kõik need infoturbe protsessid peavad tagama RMK varade konfidentsiaalsuse, tervikluse, käideldavuse ja organisatsiooni kohanemisvõime muutuvus küberohtude keskkonnas.

7. Andmete turvalisus edastamisel ja talletamisel

- 7.1. Volitatud töötleja on kohustatud hoidma lepingu täitmise käigus teatavaks saanud andmeid rangelt konfidentsiaalsena ning mitte kasutama ega avaldama andmeid, mis tahes muul kui käesolevas lepingus sätestatud eesmärgil.
- 7.2. Konfidentsiaalse teabe edastamisel arvutivõrgu kaudu peab teave olema krüpteeritud turvalise krüptomeetme abil vastavalt kokkulepitud andmeedastuse viisile, kas:
 - 7.2.1. rakenduste vahelisel suhtlusel üle API kasutades turvalist šifrikomplektiga TLS (HTTPS) veebiseanssi;
 - 7.2.2. inimkasutajale andmete jagamisel üle veebiliidese kasutades turvalist šifrikomplektiga TLS (HTTPS) veebiseanssi;
 - 7.2.3. kaugpääsuga andmete jagamisel kasutades VPN ühendust turvalise konfiguratsiooniga;
 - 7.2.4. e-kirjaga andmete edastamisel kasutades krüpteeritud manuseid (.doc).
- 7.3. Konfidentsiaalse teabe talletamisel (andmed jõudeolekus) peab rakendama turvalisi krüptomeetmeid. Näiteks kogu ketta krüpteerimine, mälupulga krüpteerimine, krüpteeritud andmebaas või andmebaasi kirjed.
- 7.4. Turvaline krüptomeetme on lahendus, mis rakendab turvalist krüptoalgoritmi, võtmepikkust, krüptovõtme käsitlust, tarkvara jms. Valikul peab lähtuma uusimast RIA avaldatud krüptograafiliste algoritmide elutsükli uuringust (https://www.ria.ee/amet-uudised-ja-kontakt/uudised-pressikontakt/uuringud-ja-analuusid?view_instance=2¤t_page=1&sort_property=1&sort_direction=desc#krüptouuringud).
- 7.5. Volitatud töötlejal pole lubatud edastada andmeid väljapoole Euroopa Liidu liikmesriikide ja Euroopa Majandusühendusse kuuluvate riikide territooriumit ilma vastutava töötleja sellekohase selgesõnalise kirjaliku nõusolekuta.

8. Pääsuhalduse meetmed

- 8.1. Volitatud töötleja on kohustatud oma töötajatele andma töödeldavatele isikuandmetele juurdepääsu üksnes ulatuses, mis on vajalik lepingu täitmiseks, haldamiseks ja selle täitmise üle tehtavaks järelevalveks. Volitatud töötleja tagab, et isikuandmeid töötleva hakkavad volitatud isikud on kohustatud järgima isikuandmete töötlemise nõudeid või nende suhtes kehtivaid asjakohaseid seadusjärgseid konfidentsiaalsuskohustusi.
- 8.2. Juurdepääs RMK varadele, sh teabele on lubatud [tee valik]:
 - 8.2.1. X ja Y rakenduste vahel üle API;
 - 8.2.2. veebiliidese kaudu RMK rakenduses X;
 - 8.2.3. VPN ja RDP/SSH kaugpääsu lahenduste kaudu;
 - 8.2.4. [mõni muu variant].
- 8.3. Vastutava töötleja konfidentsiaalse teabega dokumentatsioon peab olema vastavalt märgistatud, kui vastav märgistus on juba seotud alusdokumentatsioonil või kui need juhised on vastutava töötleja poolt antud. Dokumentatsioonil saab kasutada märgistust: asutusesiseks kasutamiseks ning vastav viide õigusaktile või "RMK siseseks kasutamiseks".
- 8.4. Vastutava töötleja süsteemides talletatud ja üksnes seal töötlemiseks mõeldud teavet ei tohi kopeerida volitatud töötleja süsteemidesse, kui ei ole kirjalikult kokku lepitud teisiti.
- 8.5. Vastutava töötleja konfidentsiaalsele teabele juurdepääsu jagamisel tuleb arvestada konkreetsete töötajate teadmisyajadusega ning rakendada minimaalõiguste printsiipi.

Kommenteerinud [KH2]: Tee valik ja teised valikud eemalda

Kommenteerinud [KH3]: Märgi X ja Y asemele konkreetsete rakendused

- 8.6. Juurdepääsu võimaldavat teavet (nt paroolid, PIN-koodid, salajased või privaatvõtmed, tookenid jne) tohib talletada ainult krüpteeritud kujul (nt tarkvaraline paroolihoidla, vault) või füüsiliselt kaitstud hoidlas (nt seifis).
- 8.7. Juurdepääsul peab kõikidele kasutajatele jõustama mitmetasemelised autentimisviisid ja keelama üksnes ühetasemelised autentimisviisid.
- 8.8. Vastutava töötleja süsteemides loodud kasutajakontosid võib kasutada ainult volitatud töötleja töötaja, kellele nimeline konto on loodud ja kellele on pääsuõigused üle antud. Konto jagamine on keelatud.
- 8.9. Volitatud töötleja peab vastutavat töötlejat viivitamata teavitama kasutajakonto sulgemise vajadusest, kui mõni volitatud töötleja töötajatest on töölt lahkunud, ei ole enam seotud lepingu täitmisega või pääsuandmed on sattunud ohtu (nt lekkinud).

9. Töötuskoha füüsilise turbe meetmed

- 9.1. Vastutava töötleja konfidentsiaalset teavet tohib töödelda ainult nendes ruumides, kus on tagatud piisav kaitse füüsiliste turvaohude eest, näiteks seadme vargus või volitamata juurdepääs, ekraani või klaviatuuri jälgimine jms.
- 9.2. Käesoleva lepinguga seotud vastutava töötleja konfidentsiaalset teavet tohib töödelda üksnes volitatud töötleja ametlikes ja turvatud kontoriruumides. Töötajate kaugtöö ei ole lubatud.

Kommenteerinud [KH4]: Igakordselt otsustada, kas see punkt jääb sisse.

10. Andmete kvaliteedi tagamise meetmed

- 10.1. Volitatud töötleja peab vastutava töötleja konfidentsiaalset teavet töötleva viisil, et andmete õigsus, täielikkus ja ajakohasus oleks tagatud. Võimalusel peab rakendama sisendandmete valideerimist, töödeldud andmete testimist ja kindlustama volitatud töötleja poolt kasutatava tarkvara korrektne toimimine.

11. Sündmuste logimine ja seire

- 11.1. Volitatud töötleja tagab konfidentsiaalse teabe töötlemisega seotud revisjonlogi (audit logi) olemasolu ja pideva turvaseire.
- 11.2. Logisid peab säilitama 2 aastat.

12. Jätkuvuse ja muudatuse meetmed

- 12.1. Volitatud töötleja teavitab vastutavat töötlejat kirjalikult kõigist muudatustest, mis võivad mõjutada volitatud töötleja võimet või väljavaateid pidada kinni käesolevast lisast ja vastutava töötleja kirjalikest juhistest. Pooled lepivad kõigis käesolevat lisa puudutavates täiendustes ja muudatustes kokku kirjalikult.
- 12.2. Volitatud töötleja tagab oma teenuste kättesaadavuse, arvestades võimalike probleemidega enda tarneahelas.
- 12.3. Vastutava töötleja pooltel pärimisel annab volitatud töötleja teavet oma toodetes kasutatavatest süsteemi-komponentidest ja turvafunktsioonidest.
- 12.4. Teenuseid mõjutavatest muudatustest ja võimalikest plaanilistest katkestustest antakse vastutavale töötlejale teada enne muudatust või katkestust.

13. Turvameetmete teavitus ja kontroll

- 13.1. Vastutav- ja volitatud töötleja peavad suutma tõendada käesolevate nõuete täitmist.

- 13.2. Volitatud töötleja peab võimaldama vastutaval töötlejal või tema poolt volitatud audiitoril teha auditeid ja kontrollide ning panustama nendesse.
- 13.3. Vastutav- ja volitatud töötleja teevad auditi käigus saadud teabe ja auditite tulemused taotluse korral kättesaadavaks pädevale järelevalveasutusele.
- 13.4. Volitatud töötleja tagab oma töötajate teavitamise käesolevatest turvameetmetest.
- 13.5. Volitatud töötleja tagab iseseisvalt enda ja alltöövõtjate organisatsioonis pideva turvameetmete rakendatuse kontrolli.
- 13.6. Volitatud töötleja organisatsioonisest infoturbealaldust peab auditeerima sõltumatu osapool vähemalt üks kord aastas. Selle korraldab volitatud töötleja.
- 13.7. Tunnustatud turvasertifikaadi (nt ISO/IEC 27001, SOC2) või auditaruande (E-ITS auditi aruanne) korral ei pea eraldiseisvat sõltumatud auditit lisaks läbi viima, kui sertifikaat või auditi aruanne:
 - 13.7.1. on kehtiv;
 - 13.7.2. käsitusala katab ära RMK varadega seotud teenused või tooted;
 - 13.7.3. tehakse vastutavale töötlejale kättesaadavaks.
- 13.8. Võimalikud erandid ja kõrvalekalded nimetatud meetmetest tuleb kirjalikult kooskõlastada vastutava töötlejaga enne erandi rakendamist.
- 13.9. RMK võib igal ajal kontrollida ja auditeerida nimetatud turvameetmete rakendatust ja volitatud töötleja peab seda toetama.

14. Andmetega seotud rikkumisest teavitamine

- 14.1. Volitatud töötleja teavitab vastutavat töötlejat andmetega seotud rikkumistest või kui on alust kahtlustada, et selline rikkumine on aset leidnud, ilma põhjendamatu viivitusega alates hetkest, kui volitatud töötleja või tema poolt kasutatav alamtöötleja saab teada andmetega seotud rikkumisest või on alust kahelda, et selline rikkumine on aset leidnud, kuid mitte hiljem kui kakskümmend (20) tundi pärast sellest teada saamist.
- 14.2. Volitatud töötleja teeb vastutava töötlejaga igakülgset koostööd turvaintsidentide käsitlemisel, sh analüüsimisel, isoleerimisel ja normaalse olukorra taastamisel.
- 14.3. Volitatud töötleja peab oma sisemised lahendused ja protsessid korraldama selliselt, et intsidenti korral vastutava töötlejaga seotud äriprotsessid ja -teenused toimiks võimalikult vähese häiringuga.
- 14.4. Vastutava töötleja nõudmisel peab volitatud töötleja ilma põhjendamatu viivitusega edastama vastutavale töötlejale kogu andmetega seotud rikkumist puudutava asjakohase informatsiooni.
- 14.5. Teates tuleb kirjeldada vähemalt järgmist:
 - 14.5.1. toimunud andmetega seotud rikkumise laad, andmesubjekti kategooriad ja ligikaudne arv ning isikuandmete liigid ja ligikaudne arv;
 - 14.5.2. eeldatav kuupäev ja kellaaeg;
 - 14.5.3. isikuandmetega seotud rikkumise tõenäolised tagajärjed;
 - 14.5.4. volitatud töötleja asjakohase kontaktisiku nimi ja kontaktandmed, kellelt saab täiendavat informatsiooni;
 - 14.5.5. meetmeid, mida volitatud töötleja rikkumise lahendamiseks on tarvitusele võtnud või võtab, et vältida andmetega seotud rikkumisi tulevikus, ja vajaduse korral ka meetmeid, mille abil leevendada rikkumise võimalikke negatiivseid mõjusid;
 - 14.5.6. esitada muud teavet, mis on mõistlikult nõutav, et vastutav töötleja saaks täita kohaldatavaid andmekaitsealaseid nõudeid, sealhulgas riigiasutustega seotud teavitamise ja avaldamise kohustusi, näiteks teavet, mis on nõutav andmesubjekti tuvastamiseks;

- 14.5.7. Juhul kui kogu teavet ei ole võimalik esitada korraga, peab esialgne teade sisaldama sel ajal kättesaadavat teavet ning täiendav teave esitatakse viivitusega pärast selle saamist.
- 14.6. Teavet andmetega seotud rikkumistest ja turvaintsidentide kohta loetakse konfidentsiaalseks ja see tuleb edastada krüpteeritult.
- 14.7. Teavitus tuleb edastada:
- 14.7.1. E-posti aadress: andmekaitse@rmk.ee;
- 14.7.2. telefon: +372 676 7000.
- 14.8. Vastutav töötaja teavitab vajadusel kolmandaid osapooli, avalikkust ja järelevalveasutusi, sh Andmekaitse Inspektsiooni, Riigi Infosüsteemi Ametit ja Politseija Piirivalveametit. Volitatud töötaja ei teosta avalikku suhtlust osas, mis võimaldab tuvastada vastutavat töötajat ja tema kliente.

15. Lõppsätted

- 15.1. Kui volitatud töötaja ei täida käesolevatest nõuetest tulenevaid kohustusi, võib vastutav töötaja anda volitatud töötajale korralduse peatada isikuandmete töötlemine seniks, kuni volitatud töötaja järgib käesolevaid nõudeid või leping lõpetatakse. Volitatud töötaja teavitab vastutavat töötajat viivitamata, kui ta ei suuda käesolevaid nõudeid mis tahes põhjusel täita.
- 15.2. Vastutaval töötajal on õigus lõpetada leping, kui:
- 15.2.1. vastutav töötaja on volitatud töötaja poolse isikuandmete töötlemise punkti 15.1 kohaselt peatanud ja kui käesolevaid nõudeid ei hakata järgima mõistliku aja jooksul või hiljemalt ühe kuu jooksul pärast peatamist;
- 15.2.2. volitatud töötaja rikub oluliselt või jätkuvalt käesolevaid nõudeid või isikuandmete kaitse üldmäärusest tulenevaid nõudeid.
- 15.3. Volitatud töötajal on õigus lõpetada leping isikuandmete töötlemise osas pärast seda, kui ta on vastutavat töötajat punkti 4.3.3 kohaselt teavitatud, et tema juhised lähevad vastuollu kohaldatavate õigusnõuetega, kuid vastutav töötaja nõuab nende juhiste järgimist.
- 15.4. Pärast lepingu lõpetamist kustutab volitatud töötaja vastutava töötaja valikul kõik vastutava töötaja nimel töödeldud isikuandmed ja kinnitab vastutavale töötajale, et ta on seda teinud, või tagastab kõik isikuandmed vastutavale töötajale ja kustutab olemasolevad koopiad, välja arvatud juhul, kui seaduses kohaselt nõutakse isikuandmete säilitamist. Volitatud töötaja jätkab nendele nõuetele vastavuse tagamist seni, kuni andmed kustutatakse või tagastatakse.