Lisa 3

Isikuandmete töötlemise organisatsioonilise, füüsiliste ja infotehniliste turvameetmete kirjeldamise ankeet

Turu-uuringute AS

1.	**Töövahendite ja infovara turve** Eesmärk: ruumide ja seadmete turvalisuse tagamine	
1.1	Kas ligipääs isikuandmete töötlemise ruumidesse on tagatud juhendite, eeskirjade, korralduste ja käskkirjade järgimisega ning ligipääsu andmist, võtmist ja muutmist fikseeritakse kirjalikult?	On reguleeritud töölepingus, spetsiaalset kanderaamatut pääsu andmise, võtmise ja muutmise kohta ei peeta.
1.2	Kuidas on reguleeritud koristaja(te) ja/või tehniliste töötajate pääs isikuandmete töötlemise ruumidesse?	Neile võimaldatakse juurdepääs ruumidesse töövälisel ajal, kuid neil puudub võimalus isikuandmetele ligi pääseda. Nendega on sõlmitud konfidentsiaalsuskohustuse leping
1.3	Kas isikuandmete töötlemise ruumide kohta kehtib alati nn „suletud uste ja akende poliitika“ (*st ruumi uksed on lukustatud ning aknad on suletud, kui kedagi ruumis ei viibi, sh ka hetkelisel väljumisel*)?	Jah, alati
1.4	Millega tagatakse, et vastuvõturuumist ning teistest avalikest ruumidest puudub pääs ilma volituseta isikutel isikuandmete töötlemiseks kasutatavatesse ruumidesse?	Tööruumide lukustamisega *(kui oma personali sees ei ole, siis kindlasti lukus)* Läbipääsu kontrollsüsteem *(koodlukk)* või distantsilise läbipääsu süsteemi *(puutevaba (kiip)kaart)* rakendamisega
1.5	Kas ruumid, kus töödeldakse isikuandmeid on varustatud valvesignalisatsiooniga ning on kontrolli all ka peale tööaja lõppu?	Jah
1.6	Kas ruumid, kus töödeldakse isikuandmeid, on varustatud tuletõrjesignalisatsiooniga?	Jah, tuletõrjesignalisatsioon on olemas

2.	**Dokumentide ja andmekandjate turve** Eesmärk: ära hoida andmete omavoliline lugemine, kopeerimine ja muutmine	
2.1	Milliseid andmekandjaid Te kasutate isikuandmete töötlemisel? *Valida võib mitu vastusevarianti*	Failid arvuti/serveri kõvakettal – digitaalkujul andmekandjad
2.2	Kus ja kuidas hoitakse isikuandmetega paberdokumente?	Paberkujul ei hoitagi, kõik on digitaalne
2.3	Kus ja kuidas hoitakse isikuandmetega teisaldatavaid andmekandjaid (*CD/DVD, USB mälupulk, mälukaart, väline kõvaketas vms*)?	Neid ei kasutata
2.4	Kas kasutate viirus- ja nuhkvaratõrje programme?	Viiruste ja nuhkvara avastamiseks/tõkestamiseks kasutatakse spetsiaaltarkvara, mis tagab rünnete ja viiruste efektiivse tuvastamise WIN 10 Defender, C-cleaner, Vanematel masinatel Avirat
2.5	Sisevõrgu kaitse Internetiga või kolmanda poole võrguga on tagatud …..	Ruuteri või tulemüüri kasutamisega Sisevõrgu segmenteerimisega *(parema kontrolli ja viiruste/rünnete kaitstuse tagamiseks)*
2.6	Kas on olemas infosüsteemi andmete varukoopiate tegemise alane strateegia?	Jah, varukoopiaid tehakse regulaarselt
3.	**Infosüsteemi turve** Eesmärk: kasutusõiguste määratlemine ja kontroll ning kasutajate autentimine ja toimingute logimine	
3.1	Te töötlete digitaalkujul isikuandmeid…… *Märkige ära kõik vastusevariandid, mis Teie süsteemi kohta kehtivad*	Lokaalses võrgus ja kogu süsteem asub tervenisti *(sh server, töökohaarvutid ja võrguseadmed)* TU AS kontrolli all asuvates tööruumides – toimub regulaarne varundamine krüptitud konteineris krüptitud kanaleid pidi asutusest väljaspool asuvasse virtuaalserverisse. Pilve kasutatakse ainult andmete varundamiseks (mitte töötlemiseks). Isikustatud andmeid töödeldakse ainult lokaalses arvutis. Isikustatud andmed on lokaalses arvutis krüpteerimata kujul töötluse ajal – muul ajamomendil on andmefail alati krüpteeritud ja ligipääsupiirangutega kaitstud. Esimene aste – arvuti BIOS ei käivitu ilma salasõna kasutamata, teine aste – kasutaja personaalne kasutajanimi ja parool, kolmas aste – isikustatud andmefail on krüpteeritud registreeritud andmetöötleja ID kaardiga, neljanda turvameetmena kasutakse seda, et arvuti juurest lahkudes lülitub minuti jooksul alati sisse screensaver,

		mis on vaid parooliga avatav. Viienda astmena on isikustatud andmefail alati ise ka salasõnaga kaitstud.
3.2	Millise rakendustarkvaraga Te isikuandmeid töötlete? *(Palume esitada informatsiooni, mis puudutab vaid isikuandmete töötlemist)*	Kasutusel on laiatarbetarkvara *(teksti- ja tabeltöötlustarkvara, nt MS Word, MS Excel, SPSS, LibreOffice jms)*
3.3	Kas on tagatud digitaalsete isikuandmete algandmete kaitse, st usaldatavuse?	Lisaks punktis 3.1 kirjeldatule tagatakse andmetöötlustarkvaraga ja veebirakendusega, mis peavad arvet *(juurdepääsu logi)* selle üle, kes andmeid lisas, muutis, vaatas või kustutas.
3.4	Kas süsteemi sisenemiseks ehk kasutaja autentimiseks kasutatakse turvamehhanisme?	Jah, selleks on iga kasutaja personaalne kasutajanimi ja parool
3.5	Kas kasutusel on paroolkaitse reeglid?	Jah, kehtivad paroolikaitse reeglid
3.6	Kas on kindlaks määratud, millistele andmetele omavad erinevad kasutajad ligipääsuõigust?	Jah, süsteemikasutajal on juurdepääs ainult tööks vajalikele andmetele
3.7	Kas on tagatud infosüsteemiga ühenduse katkemine, kui seda teatud aja vältel ei kasutata *(nt 5 minuti jooksul)*?	Jah
3.8	Kas on tagatud, et infosüsteem ei võimalda uusi sisenemiskatseid ja lukustab kasutajatunnuse, kui ebaõnnestunud sisenemiskatsete arv ületab teatud piiri *(nt kui on parooli sisestatud 3 korda valesti)*?	Jah
3.9	Kas ja kuidas rakendate kaugtööd?	Kaugtööd rakendatakse ja selleks kasutatakse turvatud kanaleid
3.10	Kas isikuandmete andmehõiveks kasutate pilvandmetöötlust?	Jah kasutame pilve, aga seda vaid andmete varundamiseks, mitte töötlemiseks.
Kui kasutate pilvandmetöötlust		
3.11	Mis tüüpi pilvetöötlemist te kasutate?	Avaliku pilve ja privaatpilve kombinatsioon

3.12	Millist pilvandmetöötluse liiki kasutatakse?	Pilveteenuse pakkuja haldab nii riistvara, operatsioonisüsteemi kui rakendust. TU AS kasutab pilveteenust ainult andmete varundamiseks. Isikustatud andmete töötlus toimub ainult TU AS lokaalsetes arvutites.
3.13	Kuidas on reguleeritud teenuse kasutaja (vastutav töötleja) ehk Teie ja teenuse pakkuja (volitatud töötleja) suhe?	Lepinguga, sh EULA (end-user license agreement ehk lõppkasutaja litsentsileping)
3.14	Nimetage pilvandmetöötluse **teenuse pakkuja** asukoha riik.	Iirimaa, Rootsi kuningriik
3.15	Kas pilvandmetöötluse pakkuja tagab piisava andmekaitse taseme (vt taotluse küsimus 9)?	Pilvetöötluse pakkuja tagab piisava taseme.
4.	**Turvameetmed andmete edastamisel andmesidevahenditega ja andmekandjate transportimisel** Eesmärk: vältida isikuandmete omavolilist lugemist, kopeerimist, muutmist või kustutamist ning saada teada, millal, kellele ja millised isikuandmed edastati	
4.1	Millisel kujul Te isikuandmeid kolmandatele osapooltele edastate?	Krüpteeritud andmed (digitaalkujul) nende edastamisega üle turvatud võrgu, selleks on loodud vastav juurdepääsuliides
4.2	Kuidas isikuandmeid sisaldavaid paberdokumente ja teisaldatavaid andmekandjaid transporditakse *(nt töötlemiskoha muutumisel, kolimisel või erinevate töötlemiskohtade vahel vms)*?	Neid ei transpordita
4.3	Kuidas peate arvet, kellele, millal ja milliseid isikuandmeid edastate?	Andmete edastamise kohta infosüsteemist peetakse vastavat automaatset *logi,* kus nähtub üheselt, kellele ja millisel põhjusel on andmeid edastatud *(nt kasutusel oleva tarkvara kaudu andmete edastamisel)*
5.	**Turvapoliitika** Eesmärk: organisatsiooni töökorraldus, mis võimaldab täita infoturbemeetmeid (varundamine, hävitamine, siseeskirjade kehtestamine ja töötajate vastav koolitamine)	
5.1	Millisele andmekandjale või süsteemile Teie **infosüsteemi** isikuandmetest varukoopia tehakse?	Incremental backup koos erinevate versioonide haldusega, Amazon Iirimaal asuvates serverites

5.2	Kuidas on korraldatud varundatud andmete *(koopiate)* turvaline hoidmine?	Varukoopia asub Amazoni Iirimaal asuvates serverites (S3)
5.3	Kuidas Te hävitate isikuandmeid sisaldavaid paberdokumente?	Paberdokumente ei töödelda
5.4	Kas Teie asutusel on tegevuskava, juhuks kui infosüsteemi (andmekogu) töö on häiritud või on katkenud pikemaks perioodiks (üle 24 tunni) ning kas on olemas infosüsteemi töö (andmekogu algseisu) taastamise kava?	Jah

6.	**Muud**	
6.1	Kinnitan, et meil on infosüsteemidesse autentimise ja isikuandmetele juurdepääsu reguleerimise juures võetud aluseks töötajate tööülesanded ning töötajatel puudub ligipääs oma tööülesannete täitmiseks mittevajalikele isikuandmetele	Jah
6.2	Kinnitan, et organisatsioonis peetakse arvestust isikuandmete töötlemisel kasutatavate seadmete ja tarkvara üle, dokumenteerides seadme nimetuse, tüübi, asukoha, seadme valmistaja nime ning tarkvara nimetuse, versiooni, valmistaja nime ja kontaktandmed	Jah
6.3	Kinnitan, et olen teadlik sellest, et pilvandmetöötluse kasutamisel tuleb vajadusel taotleda Andmekaitse Inspektsioonilt luba isikuandmete edastamiseks ebapiisava andmekaitse tasemega riiki	Jah
6.4	Kinnitan, et meil ei säilitata isikuandmeid kauem, kui näevad ette õigusaktides sätestatud säilitustähtajad. Juhul, kui õigusaktides organisatsiooni poolt töödeldavatele isikuandmetele säilitamise tähtaegu ei ole määratud, ei säilitata isikuandmeid kauem kui hetkeni, millal on isikuandmete algse kogumise eesmärk saavutatud	Jah
6.5	Kinnitan, et meil tehakse kõikvõimalik tagamaks kogutud isikuandmete õigsus ja viimane seis. Juhul, kui organisatsiooni töötajatele saab teatavaks asjaolu, et kõik või osa organisatsiooni valduses olevatest isikuandmetest on ebaõiged, suletakse ebaõiged isikuandmed ning võetakse viivitamatult kasutusele vajalikud abinõud ebaõigete isikuandmete täiendamiseks ja parandamiseks	Jah
6.6	Kinnitan, et ebaõigete isikuandmete täiendamise või parandamise korral säilitatakse ka ebaõiged isikuandmed märkusega nende kasutamise aja kohta. Isikuandmed, mille õigsus on vaidlustatud, suletakse kuni isikuandmete õigsuse kindlakstegemiseni või õigete andmete väljaselgitamiseni	Jah
6.7	Kinnitan, et isikuandmete parandamise korral teavitatakse viivitamata kolmandaid isikuid, kellelt isikuandmed saadi või kellele isikuandmeid edastati, kui see on tehniliselt võimalik ega too kaasa ebaproportsionaalselt suuri kulutusi	Jah

6.8	Kinnitan, et kõikide isikutega (füüsilised-, juriidilised- ja avalik-õiguslikud juriidilised isikud), kes pääsevad või võivad pääseda ligi isikuandmetele, on sõlmitud konfidentsiaalsuskohustuse leping või konfidentsiaalsuskohustuse nõue on mõne muu dokumendi lahutamatuks osaks (töölepingu vms)?	Jah
6.9	Kinnitan, et kõik isikud, kes puutuvad kokku oma tööülesannete täitmisel isikuandmetega on tutvunud kõikide isikuandmete kaitset puudutavate õigusaktide ja dokumentidega	Jah
6.10	Kinnitan, et kõik isikud, kes puutuvad kokku oma tööülesannete täitmisel isikuandmetega on läbinud infoturbealase koolituse	Jah