Lisa 8

Isikuandmete töötlemise organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete ankeet

Uuringu nimetus: Tööst põhjustatud haiguste ja kutsehaiguste diagnoosimise ning tööst põhjustatud tervisekahjustuste kahjuhüvitamise süsteemi uuring

Eesti Rakendusuuringute Keskus Centar

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?	Reguleeritud töölepingutega, füüsiliste juurdepääsuvõtmete jagamine fikseeritakse kirjalikult.
1.2	Kuidas on reguleeritud koristaja(te) ja/või tehniliste töötajate pääs isikuandmete töötlemise ruumidesse?	Koristajal on juurdepääs ruumidesse töövälisel ajal.
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 – tööruumid on alati lukustatud, volitatud isikutel puudub võimalus ruumidesse sisenemiseks ilma volitustega isikuta.
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

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 kõvakettal – digitaalkujul andmekandjad
2.2	Kus ja kuidas hoitakse isikuandmetega paberdokumente?	Paberil isikuandmetega dokumente käesolevas uuringus ei hoita. Süstemaatilist paberdokumentidel andmete kogumist ei toimu. Juhul, kui on mõne uuringu käigus vaja paberil isikuandmeid koguda, siis töötatakse välja spetsiaalne andmekaitse lahendus.
2.3	Kus ja kuidas hoitakse isikuandmetega teisaldatavaid andmekandjaid (*CD/DVD, USB mälupulk, mälukaart, väline kõvaketas vms*)?	Teisaldatavatel andmekandjatel isikuandmeid ei hoita
2.4	Kas kasutate viirus- ja nuhkvaratõrje programme?	Viiruste ja nuhkvara avastamiseks/tõkestamiseks kasutatakse tarkvara Windows Security, mis tagab rünnete ja viiruste efektiivse tuvastamise.
2.5	Sisevõrgu kaitse Internetiga või kolmanda poole võrguga on tagatud …..	Tulemüüri kasutamisega (Windows Firewall).
2.6	Kas on olemas infosüsteemi andmete varukoopiate tegemise alane strateegia?	Andmed varundatakse pilve (isikuandmete jm tundlike andmete varundamisel pilve ainult tarkvaras Veracrypt krüpteeritud kujul).
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*	Töökohaarvutites – toimub regulaarne varundamine krüptitud (Veracrypt) konteineris asutusest väljaspool asuvasse virtuaalserverisse.
3.2	Millise rakendustarkvaraga Te <u>isikuandmeid</u> töötlete? *(Palume esitada informatsiooni, mis puudutab vaid isikuandmete töötlemist)*	Kasutusel on laiatarbetarkvara *(teksti- ja tabeltöötlustarkvara, nt MS Word, MS Excel)* ning statistikatarkvara R.
3.3	Kas on tagatud digitaalsete isikuandmete algandmete kaitse, st usaldatavuse?	Algandmeid ei muudeta, analüüsiks vajalike teisenduste tegemisel luuakse andmestikku täiendavad tulbad. Säilitatakse andmeanalüüsi kood, milles on näha algandmete baasil tehtud teisendused ja arvutused.

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)*?	Krüpteeritud andmete konteiner ühendatakse lahti, kui kasutaja logib välja, kasutajasessioon lõpeb, ekraanisäästja käivitub või arvuti siseneb energiasäästurežiimi
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)*?	Ei
3.9	Kas ja kuidas rakendate kaugtööd?	Kaugtööd rakendatakse, seda tehakse ainult töökoha poolt antud ja nõuetekohaselt seadistatud arvutites
3.10	Kas isikuandmete andmehõiveks kasutate pilvandmetöötlust?	Jah (elektroonilised küsitlused viiakse läbi Limesurvey keskkonnas)
Kui kasutate pilvandmetöötlust		
3.11	Mis tüüpi pilvetöötlemist te kasutate?	Avalik pilv
3.12	Millist pilvandmetöötluse liiki kasutatakse?	Onedrive: Pilve teenuse pakkuja haldab riistvara ja operatsioonisüsteemi, rakendust, andmeid Limesurvey küsitluskeskkond: Pilve teenuse pakkuja haldab riistvara ja operatsioonisüsteemi, rakendust haldame ja andmeid hoiame meie
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.	Eesti
3.15	Kas pilvandmetöötluse pakkuja tagab piisava andmekaitse taseme?	Pilvetöötluse pakkuja tagab piisava taseme. Pilves säilitatakse isikustatud andmeid ainult krüpteeritud kujul. Lokaalses arvutis on isikustatud

		andmed krüpteerimata kujul töötluse ajal – muul ajamomendil on andmefail alati krüpteeritud ja ligipääsupiirangutega kaitstud. Esimene aste kasutaja personaalne kasutajanimi ja parool, teine aste – isikustatud andmefail on krüpteeritud registreeritud andmetöötleja füüsilisel turvavõtmel asuva parooli ja meelde jäetud parooli kombinatsiooniga, kolmanda turvameetmena kasutakse seda, et arvuti juurest lahkudes lülitub minuti jooksul alati sisse screensaver, mis on vaid parooliga avatav. Neljanda astmena ühendatakse krüpteeritud konteiner automaatselt lahti, kui kasutaja logib välja, kasutajasessioon lõpeb, ekraanisäästja käivitub või arvuti siseneb energiasäästurežiimi.
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?	Krüpteeritult (ID-kaardiga või Veracryptiga)
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 registris
5.	**Turvapoliitika** Eesmärk: organisatsiooni töökorraldus, mis võimaldab täita infoturbemeetmeid (varundamine, hävitamine, siseeskirjade kehtestamine ja töötajate vastav koolitamine)	
5.1	Millisele andmekandjale või süsteemile Teie **<u>infosüsteemi</u>** isikuandmetest varukoopia tehakse?	Onedrive
5.2	Kuidas on korraldatud varundatud andmete *(koopiate)* turvaline hoidmine?	Onedrive on seadistatud selliselt, et andmeid hoitakse EL riikides asuvates serverites
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	Eraldi tegevuskava ei ole. Tööarvuti rikke korral taastatakse andmekogu algseis pilves säilitatavast krüpteeritud konteinerist või teisest tööarvutist.

	kas on olemas infosüsteemi töö (andmekogu algseisu) taastamise kava?	
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 üle, dokumenteerides seadme nimetuse, tüübi, vastutaja seadme eest ja seadme valmistaja.	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