TÖÖSTUSJULGEOLEK: SALASTATUD TEABE KAITSE ERASEKTORIS

Ettevõtted peavad üha enam kaitsma salastatud teavet vaenulike riikide tööstusluure eest ning riik kaitsma riigisaladust, mis usaldatakse välisettevõtetele.

Pöördu Välisluureametis paikneva riigi julgeoleku volitatud esindaja (RJVE) poole, kui Eesti ettevõttele edastatakse salastatud välisteavet või kui Eesti riigisaladust edastatakse välisettevõttele.

Salastatud lepingu sõlmimisel mõtle varakult läbi salastatud teabe kasutuslugu ehk millisel tasemel ning kes, kus ja kuidas salastatud teavet töötlema hakkab.

Tehnoloogia kiiret arengut ja tänast julgeolekuolukorda arvestades on erasektori osatähtsus salastatud teabe kaitsel muutunud olulisemaks kui kunagi varem. Eesti riik vajab heidutuse ja kaitsevõime tugevdamiseks uusi tehnoloogiaid ning neid välja arendavad ettevõtted peavad suutma kaitsta nii Eesti riigisaladust kui ka meie liitlaste salastatud teavet. Tööstusluureohule on Välisluureamet oma aastaraamatute vahendusel läbivalt tähelepanu juhtinud, kirjeldades nii Venemaa kui ka Hiina eriteenistuste tegevust. Tööstusjulgeoleku reeglite järgimine mängib võtmerolli meie ning laiemalt meie liitlaste julgeoleku tagamisel.

Välisluureametis paikneva riigi julgeoleku volitatud esindaja (ingl k *National Security Authority*) ülesandeks on kaitsta Eesti kõige tundlikuma info liikumist välismaale ning välisriikide saladuste liikumist Eestisse. Sellest lähtuvalt aitame Eesti ettevõtetel üles ehitada salateabe vahetamise võimalusi ning nõustame Eesti riigiasutusi ja Kaitseväge, kuidas nad peavad toimima välisriikide ettevõtetega, kui tekib vajadus Eesti saladusi nendega jagada. Meil on rida kliente ja kaasuseid, kus kõige tundlikuma teabe edastamisel nõustame kliente, kuidas toimida:

1. Eesti ettevõtted soovivad osaleda suurprogrammi nagu Euroopa Kaitsefondi (EDF) või programmi Horizon Europe salastatud projektides relvasüsteemide või kübertehnoloogiate väljatöötamisel;
2. Eesti ettevõtted soovivad ise algatada rahvusvahelisi salastatud projekte, näiteks iduettevõtted Tallinna rajatava NATO DIANA innovatsioonikiirendi programmi raames;
3. Eesti riigiasutused soovivad kasutusele võtta välisettevõtete toodetud salastatud IT-süsteeme või selle komponente;
4. Kaitsevägi soovib hankida välisettevõtte poolt toodetud relvasüsteemi, mis sisaldab välisriigi salastatud tehnoloogiat.

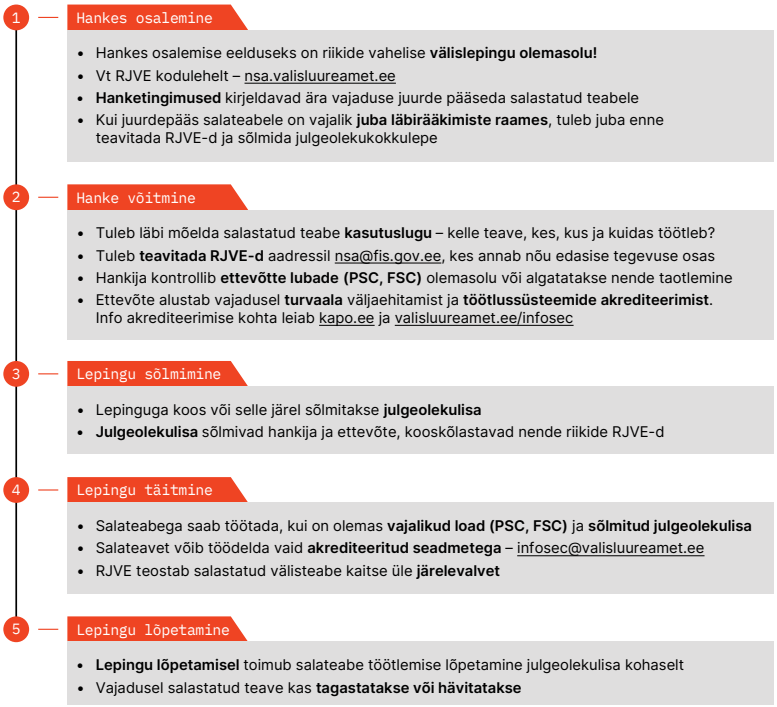
Seda kõike saab edukalt teha, kui oma planeerimises õigel ajal arvestada salateabe kaitse põhimõtete ja protseduuridega. Eelnevalt nimetatud tegevuste reguleerimiseks sõlmitavat eraõiguslikku lepingut nimetatakse salastatud lepinguks. Iga selline

salastatud leping peab sisaldama julgeolekulisa (nt ingl k *Security Aspects Letter või Programme/Project Security Instructions*), mis reguleerib salastatud teabe kaitset, näiteks isikute ringi, kes tohivad salateabele ligi pääseda ja teabe vahetamist ning sisaldab kirjeldusi, mis on salateave (*Security Classification Guide*).

Julgeolekulisas sisalduvad julgeolekureeglid peavad olema kooskõlas kehtiva riigisisese õigusega ning riikide ja rahvusvaheliste organisatsioonidega sõlmitud välislepingutega. Salateabe vahetamise välislepingud leiad riigi julgeoleku volitatud esindaja kodulehelt – nsa.valisluureamet.ee.

Ettevõtet toetav riigiasutus (näiteks Kaitseministeerium) taotleb Kaitsepolitseiametilt juurdepääsuloa (*Personnel Security Clearance*, PSC) ettevõtte igale töötajale, kes peab salastatud teabele juurde pääsema. Nii tagatakse, et salateave ei jõuaks pahatahtlike inimesteni. Kui ettevõte peab salastatud teavet hoiustama oma asutuses, siis taotleb toetav riigiasutus Kaitsepolitseiametilt ettevõttele töötlemisloa (*Facility Security Clearance*, FSC) andmist. Kui tegu on Euroopa Liidu või NATO teabega, siis pärast Kaitsepolitseiameti poolt läbi viidud julgeolekukontrolli väljastab RJVE täiendava juurdepääsu- või töötlemissertifikaadi. Juurdepääsuloa saamine võtab kuni 4 kuud ja töötlemisloa saamine kuni 7 kuud. Seega tuleks lubade taotlemist alustada võimalikult varakult, juba paralleelselt lepingu sõlmimisega.

Salastatud teabe töötlemiseks kasutatav IT-süsteem peab täitma teatud nõuded ehk elektrooniliselt saab salastatud teavet töödelda vaid akrediteeritud töötlussüsteemiga. Selleks taotleb toetav riigiasutus Välisluureametilt ettevõtte töötlussüsteemile vastavussertifikaadi andmist. Akrediteerimise protsess võtab IT-süsteemist sõltuvalt kuni neli kuud, mille tõttu tasub tehnilist ettevalmistust alustada võimalikult varakult. Täpsemalt võib lugeda salastatud IT-süsteemide küberturbe kohta www.valisluureamet.ee/infosec.



Salastatud teabe kaitsega seotud tegevused rahvusvahelise hankemenetluse etappides