.

Kontrollküsimustik tarkvaraarenduse tellijale
isikuandmete kaitse üldmääruse nõuetega arvestamisel

Koostajad: Eesti Infotehnoloogia ja Telekommunikatsiooni Liit ühiselt Andmekaitse Inspektsiooniga
Versioon 1.0
Kuupäev 19.04.2018

Soovitusliku juhendmaterjali eesmärk: tõsta nii avaliku kui ka erasektori hankijate teadlikkust isikuandmete kaitse üldmääruse (EL) 2016/679 (edaspidi *üldmäärus*) rakendamisest, et hankija mõtleks kohe alguses läbi, milliseid isikuandmeid ja mis eesmärgil arendatava tarkvara abil töötlema hakatakse ning milliseid isikuandmeid on vajalik töödelda tarkvara arendustegevuse käigus. Hankija kohustus on informeerida arendajat kõigist isikuandmete töötlemisega seonduvatest tingimustest. Hankija kui isikuandmete vastutav töötleja peab tarkvaraarenduste tellimisel lähtuma vaikimisi eeldusest, et arendaja ei pea saama hankija valduses olevatele isikuandmetele juurdepääsu. Kui mingil ERANDLIKUL põhjusel peab arendaja isikuandmeid arendustegevuse käigus siiski töötlema, peavad isikuandmete töötlemise juhised ja muud tingimused olema kirjeldatud hankija ja arendaja vahel sõlmitud vastutava-volitatud töötleja lepingus.

Selles juhendmaterjalis toodud küsimuste läbi mõtlemine peaks olema tarkvaraarenduse tellimise ettevalmistamise osa.

Enne tarkvaraarenduse tellimist mõtle läbi ja analüüsi järgmisi küsimusi:

1. Kas arendustegevuse ja/või hilisema teenuse kasutamise käigus toimub isikuandmete, sh eriliigiliste isikuandmete, töötlemine? Kas arendustegevuse käigus on isikuandmete töötlemine vältimatu või on tarkvaraarenduse teostamine võimalik ka isikustamata testandmetega? Lähtuda tuleb eeldusest, et tarkvaraarenduse teostamiseks ei ole hankija valduses olevate isikuandmete töötlemine vajalik.
2. Milliseid isikuandmeid töödeldakse? Milliseid isikuandmeid on tarkvaraarenduse teostamiseks hädavajalik töödelda? Selle küsimuse puhul tuleb hinnata nii isikute kategooriaid, kelle andmeid töödeldakse (näiteks kliendid, patsiendid, enda töötajad) kui ka töödeldavate isikuandmete liike, st kas tegemist on nn tavaliste isikuandmetega (nt inimese nimi, sünniaeg, isikukood, kontaktaktandmed), tundlikumate isikuandmetega (näiteks kasutajanimed, salasõnad, maksevahendite andmed, majanduslikku seisundit näitavad andmed, ameti- ja kutsesaladust puudutav teave, sideandmed) või eriliigiliste isikuandmetega.
3. Kas tarkvaraarendaja saab olema arenduse teostamise käigus isikuandmete volitatud töötleja?
4. Kui arendaja on volitatud töötleja, siis kas ja mis alustel on tal omakorda õigus kaasata lepingu täitmisse teisi volitatud töötlejaid (näiteks arendustöödes, majutusteenuse ostmisel)?
5. Kas hankija kui vastutava töötleja poolt on koostatud volitatud töötlejaga sõlmimiseks üldmääruse artikli 28 lõike 3 nõuetele vastav leping, mis sisaldab juhiseid isikuandmete töötlemiseks?
6. Kui hankija on määranud andmekaitsespetsialisti, siis kuidas on andmekaitsespetsialist projekti kaasatud?
7. Kas hankijal on paigas infoturbeintsidendi või isikuandmetega seotud rikkumistest teavitamise kord? Volitatud töötleja peab aitama vastutaval töötlejal teavitamiskohustust täita (üldmääruse artikli 28 lõike 3 punkt f).
8. Kas hankija on isikuandmete töötlemise kohta koostanud mõjuhinnangu (üldmääruse artikkel 35) ning millised on sellest tulenevad täiendavad tingimused tarkvaraarenduse tulemile?
9. Kuidas kontrollib hankija täitja vastavust üldmääruse nõuetele? Kas nõutakse sertifikaate, kinnitusi ja/või vastavust standarditele?
10. Kas ja kuidas on lähteülesandes arvestatud vaikimisi ja lõimitud andmekaitse põhimõtetega (üldmääruse artikkel 25)?