

[Advokaadibüroo tuletab meelde - Kas tööandja võib sinu e-kirju lugeda?](#)

2 aastat tagasi Autor: [AM](#)



(Sisuturundus)

Kas tööandjal on õigus sinu töö juures kirjutatud e-kirju lugeda? Kas inimese isikukood on delikaatne ehk eriliigiline informatsioon? Mis saab, kui rikud andmekaitse nõudeid?

Kõigile neile ning teistelegi levinud küsimustele anname selles artiklis vastused.

Levinud küsimused eraelu kaitse kohta

Kas tööandja võib sinu e-kirju lugeda?

[Advokaadibüroo](#) selgitab, et osades organisatsioonides on töötajatel tavaks kasutada tööandja domeeniga e-postiaadresse selleks, et saata ning vastu võtta isiklikke kirju. See on lubatud vaid juhul, kui tööandja ei ole kehtestanud sellevastast reeglit. Kusjuures tööandjal on täielik õigus kehtestada nõue, mis ei anna töötajatele luba erakirjade saatmiseks tööandja domeeni kasutada.

Juhul, kui tööandja lubab töö e-posti kasutada tööväliseks suhtluseks, tuleb vastavad kirjad teisaldada kas eraldi kausta (näiteks pealkirjaga "Isiklik") või need kustutada. Ka selle kohta tuleb kehtestada eraldi reegel.

Tööandjal on lubatud töötaja kirjadega põhjendatud juhtudel tutvuda, kuid sealjuures ei tohi ta liialt töötaja põhiõigusi riivata. Töötaja peaks alati meeles pidama, et tööandja domeeniga e-postkast kuulub tööandjale.

Kas inimese isikukoodi loetakse delikaatseks ehk eriliigiliseks teabeks?

Ei, isikukood kuulub tavaliste isikuandmete hulka. [Tavaliste isikuandmete](#) hulka kuuluvad muuseas ka nimi, asukohateave, inimese füüsilised, vaimsed, füsioloogilised, kultuurilised ja majanduslikud tunnused ning võrguidentifikaatorid.

Isikukood avaldatakse siis, kui näiteks samanimeliste inimeste puhul on vaja konkreetset isikut tuvastada. Selle asemel võib kasutada ka vaid sünniaega. Samuti on isikukood laialdaselt kasutusel avaliku sektori infosüsteemides ja andmete riskkasutuses, et tagada andmete kvaliteet ja täpsus.

Tundlike isikuandmete hulka loetakse andmeid, mis valmistavad inimese privaatelule suuremat ohtu ning mis ei kuulu eriliiki isikuandmete hulka. Tundlikud isikuandmed võivad olla näiteks krediitkaardiandmed, krediidireiting ja digitaalsed usaldusteenuse andmed, mis on vajalikud digitaalseks allkirjastamiseks. Samuti kuuluvad tundlike isikuandmete hulka sõnumisaldusega kaetud

sideandmed ning info isiku varalise seisu kohta.

Tundlike andmete kasutamise puhul on ka risked inimese eraelu kaitsele kõrgemad ning seega tuleb nende kaitseks rakendada kohaseid turvameetmeid.

Eriliiiki isikuandmed on sellised isikuandmed, mida nimetati varasemalt delikaatseteks isikuandmeteks. Näiteks kuuluvad sinna alla andmed, millest ilmnevad inimese poliitilised vaated, usulised veendumused, rassiline päritolu ning ka biomeetrilised andmed, mida kasutatakse isiku kordumatuks tuvastamiseks.

Eriliiigilisi isikuandmeid on lubatud töödelda ainult inimese konkreetse nõusoleku alusel või juhul kui seadus näeb nende andmete töötlemise konkreetset ette.

Mida tähendab isikuandmete töötlemine?

Isikuandmete töötlemine tähendab inimese isikuandmete kogumist, säilitamist, kasutamist ja dokumenteerimist. Isikuandmeid võidakse töödelda näiteks olukordades, kus firma säilitab klientide e-posti aadressid või töötajate CV-d.

Lisaks loetakse [isikuandmete](#) töötlemiseks turvakaameraga salvestamist, ja koduste aadresside ning telefoninumbrite kogumist ja säilitamist. Tavapäraselt on isikuandmete töötlemisel muuhulgas järgmised tunnused, mis annavad aimu, et isikuandmete kaitsega tuleb tõsisemalt tegeleda: :

1. **Süstemaatiline andmetöötlus** – süstemaatiline andmetöötlus tähendab, et andmeid töödeldakse metoodiliselt ja planeeritult.
2. **Korrapärane andmetöötlus** – korrapärase andmetöötluse puhul toimub andmete töötlemine teatud ajavahemike tagant või pidevalt ning ei ole seega juhuslik.
3. **Ulatuslik andmetöötlus** – ulatuslik andmetöötlus võib tähendada jälgitavate inimeste arvu, geograafilist ulatust või jälgimise aega. Näited sellest on kliendiandmete töötlemine pangas, ühistranspordi valideerimislahendused ning telefoniteenuste kasutajate andmete töötlemine.

Andmekaitse [rikkumiste arv](#) on võrreldes selle ja eelmise aasta esimest poolt küll vähenenud, kuid määratud trahvide suurus on märgatavalt kasvanud. Põhjuseks on rikkumiste tõsiduse suurenemine.

Karistused on tõusutrendis, kuid see ei ole ilmtingimata halb asi. Isikuandmete kaitse järelvalve püüab trahvidega motiveerida organisatsioone tagama inimeste privaatsusõigust iga hinna eest.

Mis juhtub, kui andmekaitse nõuete vastu eksitakse?

Andmekaitse [rikkumiste arv](#) on võrreldes selle ja eelmise aasta esimest poolt küll vähenenud, kuid määratud trahvide suurus on märgatavalt kasvanud. Põhjuseks on rikkumiste tõsiduse suurenemine.

Karistused on tõusutrendis, kuid see ei ole ilmtingimata halb asi. Isikuandmete kaitse järelvalve püüab trahvidega motiveerida organisatsioone tagama inimeste privaatsusõigust iga hinna eest.

7,5 miljoni naelane trahv

Ettevõtet Clearview AI trahviti selle aasta mais lausa 7,5 miljoni Inglise naelaga. Nimelt kasutas firma ülemaailmse näotuvastuse andmebaasi loomiseks avalikult kättesaadavaid pilte inimestest. Neid võeti muuhulgas ka sotsiaalmeediast.

Piltide kasutamisest inimesi aga ei teavitatud, mistõttu oli tegemist isikuandmete tahtliku kuritarvitamisega. Sama ettevõtet trahvis lisaks Ühendkuningriigi järelevalveasutusele ka Kreeka ning Itaalia andmekaitseasutus.

Kokkuvõte

Teades oma õigusi ning kohustusi, saad olla teadlik nende täitmisest. Vahet pole, kas tegemist on ettevõtte või asutusega, andmekaitse rikkumisi võetakse tõsisemalt kui kunagi varem. Seega on parem karta kui kahetseda ning andmekaitse nõuded läbi lugeda.

- [Uudised](#)
- [Sisuturundus](#)