Outlook

Re: Päring isikuandmete hoidmise kohta Google Drive'is

From info - AKI <info@aki.ee>
Date Tue 2026-04-14 14:14
To info@sakrum.ee <info@sakrum.ee>

Lugupeetud Sakrum KMTK OÜ!

Olete pöördunud Andmekaitse Inspektsiooni (AKI) poole küsimusega, mis puudutab kolmanda osapoole juures (konkreetselt Google Drive'i teenus) andmete hoiustamise, kasutajakontode autentimise turvalisuslahenduste ja failide edastamisel krüpteerimise kohta.

Esimese küsimuse osas mainin seda, et me ei saa anda konkreetset vastust, kas ühte või teist andmetöötlejat võib kasutada. Sellise järelduse saab anda vaid järelevalvemenetluse tulemusel.

Iga andmetöötleja vastutab selle eest, et kolmandad osapoole teenused, mida kasutatakse andmete töötlemisel (sh andmete hoiustamisel), vastaksid turvanõutele, mida organisatsioon ise on ette näinud enda kaardistatud riskidest tulenevalt. Siin juhul tuleb arvestada ka seda, et mis sorti isikuandmetega on tegemist. Kas on tegemist ainult üldiste isikuandmetega (näiteks ees- ja perekonnanimi, kontaktandmed, isikukood jne) või on ka andmete hulgas eriliigilisi andmeid (nt andmed, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilised, biomeetrilisi või terviseandmeid jne). Lisaks igasuguse kolmanda osapoole teenuse puhul tuleb arvesse võtta ka teenuse olemust (kas andmeid hoiustatakse isikliku konto või ettevõtte hallatava konto vahendusel) ning kas on oht, et andmed võivad liikuda väljapoole Euroopa Liitu.

Kasutajakontode autentimise puhul peab samuti andmetöötleja (ehk asutus) ise hindama, mis riskid erinevate lahenduste puhul kaasnevad ja mis on lahendused nende riskide leevendamiseks.

Kasutajakontode turvalisuse puhul oleme seisukohal olnud pikemalt aega, et seni on siiski kõige turvalisem kasutada mitmetasandilist autentimist ja failide krüpteerimist koos. Isikuandmete edastamisel tuleb igal juhul tagada, et andmed oleksid edastamise käigus kaitstud. Parimaks praktikaks on failide krüpteerimine. Krüpteerimiseks on mitmeid sobivaid lahendusi, näiteks andmete krüpteerimine adressaadi isikukoodi alusel DigiDoc konteineris või failipõhine paroolikrüpteering.

Failide krüpteerimine tagab selle, et ka juhul, kui andmed satuvad edastamise käigus kolmandate isikute kätte (nt ekslikult vale e-maili sisestamisel), ei ole need loetavad ega kasutatavad. Seega ei asenda kasutajakontode tugev kaitse (nt paroolid ja kaheastmeline sisselogimine) failide krüpteerimist, vaid need meetmed täiendavad üksteist. Riskipõhise lähenemise kohaselt on krüpteerimine oluline lisameede eelkõige isikuandmete edastamisel ja säilitamisel, et tagada andmete konfidentsiaalsus ning vastavus andmekaitsenõuetele.

Täpsemalt saate AKI soovitusi andmete turvalisuse kohta lugeda siit:
https://www.aki.ee/isikuandmed/andmetootlejale/andmeturve

Lugupidamisega

Andmekaitse Inspektsioon

ERAELU KAITSE JA RIIGI LÄBIPAISTVUSE EEST
Tatari 39 | 10134 Tallinn | Eesti
LinkedIn | YouTube

ANDMEKAITSE INSPEKTSIOON

From: info@sakrum.ee
Sent:
To: info - AKI
Subject: Re: Päring isikuandmete hoidmise kohta Google Drive'is

Tere

Kirjutame Teile, et küsida nõu väikeettevõtte andmete turvalise hoidmise kohta.
Soovime oma ettevõttes kasutada Google Drive'i, et hoida dokumente, kus on kirjas inimeste nimed ja isikukoodid.
Sooviksime teada:

1. Kas selliste andmete hoidmine Google Drive'is on seadusega kooskõlas?

2. Kas lisaks kasutajakontode kaitsmisele (tugevad paroolid ja kaheastmeline sisselogimine) peab faile veel eraldi krüpteerima?

Lugupidamisega
Egle Davõdov
5072138
Sekretär-asjaajaja
Sakrum: keha ja meele tervisekeskus
Tartu tn 25, Võru
sakrum.ee

SAKRUM
KEHA JA MEELE
TERVISEKESKUS