ANDMEKAITSE INSPEKTSIOON

Lp juhatuse liikmed

Meie 12.04.2024 nr 2.1.-1/24/272-552-3

OÜ Koodimasin
tugi@sisseastumine.ee;
info@stuudium.com

Tähelepanu juhtimine

AKI sai pöördumise, milles juhiti tähelepanu sisseastumine.ee lehele, mida haldab OÜ Koodimasin. Keskkonnas lapse andmetele ligipääsu saamiseks saadetakse e-postkasti aadressile kiri pealkirjaga "Sisseastumine.ee - sinu konto salasõna" ning kirja sisus on kasutajatunnus (e-posti aadress) ja salasõna (genereeritud). Keskkonda sisse logides ei ole võimalik salasõna muuta ega kontot kustutada, mistõttu ei ole e-kirjaga sellise info saatmine turvaline ja võimaldab ligipääsu kolmandatele isikutele.

Esmalt selgitab AKI, et ainult salasõna saatmist andmetöötleja poolt isiku enda märgitud e-posti aadressile ei saa käsitleda automaatselt isikuandmete avaldamisena kolmandatele isikutele. Ka on selgitanud andmetöötleja oma vastuses isikule: „*Nagu eelnevalt mainitud, siis e-kirjad ei liigu läbi interneti "avalikult", vaid on krüpteeritud otse meili saatja (Sisseastumine.ee) ja vastuvõtja (teie meilipostkast) serverite vahel. Kolmandatel osapooltel ei ole võimalik "võrguliiklust jälgides" e-kirjade sisu lugeda; meilipostkastile on ligipääs ka teie meiliteenuse pakkujal; eeldatavasti on sõnumisaladuse kaitse tagatud teie meiliteenuse pakkuja tingimustes*.“

Andmetöötleja on selgitanud, et salasõna saab muuta uue genereeritud salasõna vastu, s.t välistatud ei ole täielikult võimalus salasõna muuta: „*Kasutajatel on ka võimalik salasõna muuta — muutmine tähendab, et luuakse uus automaatselt genereeritud turvaline salasõna. Seda saab teha https://sisseastumine.ee/s/login lehel “Unustasid salasõna” lingil klõpsates. Soovi korral võite saabunud e-kirja iga kord pärast sisse logimist postkastist ära kustutada*.“ Siiski nähtub vastusest, et salasõna sisu ei saa isik ise määrata ning ka uus salasõna saadetakse isiku e-posti aadressile.

AKI nõustub kaebaja tähelepanekuga, et selline meetod keskkonnas andmetele ligipääsu võimaldamiseks ei pruugi tagada piisavat turvalisust ja ei ole arvestatud tehnoloogia arenguid. Lisaks tuleb arvestada, et keskkonnas töödeldakse alaealiste isikute andmeid, kes ei saa ise oma andmete töötlemise üle otsustada.

Tõhusama turvalisuse tagamiseks peaks vastutav töötleja hindama töötlemisega seotud ohtusid ja rakendama asjaomaste ohtude leevendamiseks meetmeid. Võttes arvesse teaduse ja tehnoloogia viimast arengut ja meetmete rakenduskulusid, tuleks kõnealuste meetmetega tagada vajalik turvalisuse tase, sealhulgas konfidentsiaalsus, mis vastaks ohtudele ja kaitstavate isikuandmete

laadile.[1] Seega peab ka OÜ Koodimasin, kes haldab sisseastumine.ee keskkonda, tagama seal isikuandmetele piisava turvalisuse.

Selgitame, et Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679 ehk isikuandmete kaitse üldmääruse (IKÜM) art 32 lg 1 kohaselt peab vastutav töötleja rakendama ohule vastava turvalisuse taseme tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid, sh tagama isikuandmeid töötlevate süsteemide ja teenuste kestev konfidentsiaalsus, terviklikkus, kättesaadavus ja vastupidavust. Sama kohustus tuleneb isikuandmete töötlemise põhimõtetest, täpsemalt IKÜM art 5 lg 1 punktist f, mille kohaselt tuleb isikuandmeid töödelda viisil, mis tagab nende asjakohase turvalisuse ning kaitseb loata või ebaseadusliku töötlemise eest. Seega on sobivate turvameetmete valimine andmetöötleja otsustada ning määrus ei ütle ette, kuidas täpselt seda tuleb teha. Oluline on, et isikuandmetele oleks siiski tagatud piisavad turvameetmed.

Praegusel juhul olete loonud automaatselt raskesti meelde jääva salasõna ning saadate salasõna isiku e-postkasti. Meilile saatmine on ebaturvaline meetod võrreldes mõne teise sisselogimisvõimalusega ja ei ole enam levinud praktika. Seetõttu me ei soovita seda ja eelistada võiks teisi paremaid alternatiive (nt linki, kust isik kohe ise salasõna ära muudaks või esmasel sisselogimisel on nõutud oma unikaalse salasõna loomine) jm meetodeid. Eelnevalt puudub e-posti aadressi kinnitamine, mis võib aga tekitada olukorra, kus vale aadressi sisestamisel saab salasõna õigustamatult kolmas isik. Salasõna kasutamisel tuleks hinnata, kas oleks võimalik saata see kasutajatele ka krüpteeritult, võimaldades ligipääsu ainult konkreetsel isikul. Samuti tuleks põhjalikult kaaluda, kas salasõna saaks anda kasutajale ka ilma e-postile saatmiseta. Praeguse meetodite puhul tuleks mõelda ka võimalusele isikuid teavitada enda valitud e-posti aadressi sisestamisel, et sellele saadetakse salasõna, et kasutajatel oleks võimalus kohe valida turvalisem e-postkast salasõna saatmiseks, ning lisada juurde ka juhend, kuidas salasõna saab muuta. Salasõna seadmine peaks olema isiku mõjusfääris ja keskkond peab hoidma paroole piisavalt räsituna, et tagada suurem turvalisus, kasutades ka nn soolamist.[2]

Veebilehelt on näha, et sisselogimine on võimalik ka oma Google või Microsofti kontoga[3]. Kuna selline lahendus annab kolmandatele osapooltele (sh väljaspool EL-i) isikuandmetele ligipääsu, tuleb hinnata IKÜM alusel kolmandatasse riikidesse andmete edastamise riski. Vajadusel tuleb võtta kasutusele riski maandavad meetmed. Samuti tuleb kaaluda, kas selline lahendus on üldse vajalik ning kas sel viisil on võimalik tagada IKÜM nõuete järgimine, sh peab olema isikutele nende andmete töötlus läbipaistev.

Kuna keskkond sisaldab väga paljude õpilaste ja nende vanemate andmeid, tasuks salasõnaga sisselogimine jätta vaid alternatiiviks neile, kes ei saa seda teha ennast autentides (nt Smart-ID, mobiil-ID või ID-kaardi kaudu) või kasutada nende puhul kaheastmelist sisselogimist (kinnitusmeili või sõnumi kaudu).

Samuti tuleks üle vaadata muud turvameetmed, mis keskkonnas olevate andmete kaitseks on seatud ning kas on vaja midagi täiendada, nt seansi pikkus enne automaatset väljalogimist, logide teke, kahtlustäratavate sisselogimiste tuvastamine (nt välisriigid) ja automaatne teavitus, salasõnade räsitud kujul hoidmine jms.

Lisaks juhime tähelepanu sisseastumine.ee keskkonnas kajastatud olevatele **andmekaitsetingimustele**[4], mis vajavad üle vaatamist ja täiendamist. Hetkel on andmete töötlemisega seonduva kohta edastatud väga minimaalne ülevaade. Selgelt peaks kindlasti ka kirjas olema vastutav ja volitatud töötlejad[5] ning kontaktandmed, kelle poole millise isikuandmete kaitsega seotud küsimusega pöörduda. Samuti nt informatsioon kaua isikuandmeid keskkonnas

[1] IKÜM põhjenduspunkt 83.
[2] Riigi Infosüsteemi Ameti blogi. Räsist ja räsimisest. - https://blog.ria.ee/rasist-ja-rasimisest/
[3] https://sisseastumine.ee/s/login
[4] https://sisseastumine.ee/s/tingimused
[5] Vastutava, volitatud ja kaasvastutava andmetöötleja ja nende omavaheliste suhete kohta saab lugeda täpsemalt siit: https://www.aki.ee/isikuandmed/andmetootlejale/andmetootleja-vastutus-ja-kohustused

säilitatakse. Inimeste teavitamist reguleerivad täpsemalt IKÜM artiklid 12-14 ning välja peab olema toodud nendes punktides viidatud teave. Nendes artiklites viidatud sisu peab kajastuma lihtsas ja selges keeles ka andmekaitsetingimustes. Seega peab ka sisseastumine.ee lehel isikuandmete töötlemise kohta olema veebilehel vajalik informatsioon selgelt kirjas, mis aitaks tagada paremini IKÜM art 5 lg 1 p a läbipaistvuse põhimõtet.

Andmekaitsetingimused aitavad inimesel omada ülevaadet, mida tema andmetega tehakse ja andmetöötleja saab paremini kontrollida andmetöötluse protsesse. Andmekaitsetingimuste koostamine võimaldab ühte dokumenti koondada vastused, mida inimesel kui andmesubjektil on õigus küsida oma isikuandmete töötlemise kohta. Ühtlasi hõlbustab andmekaitsetingimuste koostamine andmetöötleja enda jaoks õigusliku aluse leidmist ja töötlemise vajaduse hindamist, kuivõrd tingimuste koostamine eeldab töötlemistoimingute läbi mõtlemist ning üleüldise töötlemise vajaduse hindamist.[6]

Keskkond peab kokkuvõttes üle vaatama inspektsiooni soovitused ja oma praktika arvestades järgnevat:

- eelistama salasõna kasutamisele muid autentimisvõimalusi[7]
- salasõna kasutamisel kasutama mitmeastmelist autentimist
- tagama tugevad salasõna reeglid
- salasõnu tuleks kaitsta tugeva räsi algoritmi abil
- võimalusel hoidma salasõnu ja muid andmeid andmebaasis eraldi kohas
- meiliaadressile misiganes isikuandmeid saates enne kasutama selle kinnitamisnõuet ja salasõnade kasutamisel neid mitte isikule saata või eelistada linke
- nõudma ajutise salasõna loomisel selle kohest muutmist sisse logimisel
- kasutama automaatset välja logimist teatud aja möödudes
- vaatama üle, et andmekaitsetingimustes oleks kogu kohustuslik teave

Inspektsioonil on õigus igal ajal teha täiendavat kontrolli, et veenduda sisseastumine.ee kaudu isikuandmete töötlemisel kooskõlas isikuandmete kaitse üldmäärusest tulenevate nõuetega.

Lugupidamisega

Greete Kaljuste
jurist
peadirektori volitusel

[6] Vt täpsemalt: https://www.aki.ee/isikuandmed/andmetootlejale/andmekaitsetingimuste-koostamisest ja AKI juhend „Isikuandmete töötleja üldjuhend“ - https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf.
[7] https://www.ria.ee/kuberturbe-nouanded/nouanded-internetikasutajale/parool