Henkilötietojen käsittelyn periaatteet ja käytännöt

Kanneljärven opisto

Tietosuojatiimi
5-14-2018

Sisällysluettelo

1 Johdanto

Tässä asiakirjassa on kuvattu Kanneljärven Opiston henkilötietojen käsittelyä koskevat periaatteet, käytännöt ja toimintaohjeet. Henkilötietoja ovat kaikki sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti. Henkilö voidaan tunnistaa esimerkiksi nimen, henkilötunnuksen tai valokuvan perusteella.

Tietosuojapolitiikka

Tämän asiakirjan tarkoituksena on asettaa korkeat standardit henkilötietojen käsittelylle; luoda opiskelijoille, muille asiakkaille ja henkilöstölle selvä kuva siitä, että heitä koskevia henkilötietoja käsitellään asiallisesti ja turvallisesti sekä varmistaa rekisteröityjen oikeuksien toteutuminen.

Kanneljärven Opiston tietosuojaorganisaatioon kuuluvat tietosuojavastaava, rehtori, opettajien tietosuojaedustajat, it-tuki sekä henkilötietorekisterien vastaavat. Tietosuojaorganisaatio vastaa tietosuojapolitiikan, -käytänteiden ja -ohjeistusten ajan tasalla pitämisestä, laadun varmistuksesta, riskiarvioinneista ja kehittämisestä.

Tietojen hankinta ja käsittely sekä rekisteröidyistä muodostetut tietoryhmät

Pääasialliset lähteet henkilötietojen hankintaan ovat rekisteröity itse sekä laissa määritellyt viranomaiset. Keräämme ja käsittelemme vain sellaisia henkilötietoja, jotka ovat laadukkaan toimintamme kannalta välttämättömiä. Henkilötietoja käsittelevät vain ne henkilöstön edustajat, joiden työtehtäviin tietojen käsittely kuuluu.

Eri henkilötietorekisterien tietojen hankintaan ja käsittelyyn sekä tietoryhmiin liittyvät erityispiirteet on kuvattu erillisissä henkilötietoselosteissa, jotka löytyvät opiston internet-sivuilta.

Tietojen luovuttaminen asiakkaille

Rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä. Jos näitä henkilötietoja käsitellään, rekisteröidyllä on oikeus tarkistaa omat tietonsa sekä tietojen käyttötarkoitus, tietojen keräämistapa sekä käsittelyyn liittyvät periaatteet. (Asetus EU 2016/679 luku III, 2 jakso, 15 artikla)

Tarkastuspyyntö tehdään henkilökohtaisen käynnin yhteydessä tai omakätisesti allekirjoitetulla asiakirjalla. Pyyntö osoitetaan rekisterin yhteyshenkilölle. Tietojen luovuttamisesta päättää rehtori. Tiedot antaa rehtorin määräämä henkilö.

Rekisteröidyllä on oikeus tutustua ja nähdä häntä itseään koskevat tiedot ja pyynnöstä saada niistä kopiot.

Avoimuus rekisteröityjä kohtaan

Kanneljärven Opiston toiminta perustuu avoimuuteen ja luottamuksellisuuteen. Internet-sivuiltamme löytyvien henkilötietoselosteiden avulla pyrimme antamaan selkeän kuvan siitä, mitä henkilötietoja käsittelemme ja mihin tarkoituksiin niitä käytämme.

Tästä syystä olemme sisällyttäneet tähän julkiseen asiakirjaan myös henkilöstön toimintaohjeet.

Yhteistyö eri intressiryhmien ja viranomaisten kanssa

Kanneljärven Opistolla on nimetty tietosuojavastaava, jonka tehtäviin kuuluu lakisääteisten velvoitteiden mukainen viranomaisyhteistyö.

Kansainvälisyys

Kanneljärven Opisto ei pääsääntöisesti luovuteta tietoja EU:n ja ETA:n ulkopuolelle. Poikkeuksena pääsäännöstä ovat opiskelijoiden opintoihin liittyvät opintomatkat ja ulkomailla tapahtuva opiskelu, joiden yhteydessä tietoja luovutetaan vain opiskelijan suostumuksella opintojen järjestämiseen liittyvien velvoitteiden hoitoon.

Tietosuojaa valvova viranomainen

Tietosuojavaltuutettu on viranomainen, joka ohjaa, neuvoo ja valvoo henkilötietojen käsittelyä henkilötietolain mukaisesti. Tietosuojavaltuutettu käyttää päätösvaltaa tarkastusoikeuden toteuttamista ja tiedon korjaamista koskevissa asioissa sekä antaa ratkaisuja rekisterinpidon lainmukaisuudesta ja rekisteröityjen oikeuksien toteutumisesta.

Tietosuojaperiaatteiden päivittäminen

Tietosuojaperiaatteet ovat tämän hetken käytäntömme mukaiset. Päivitämme periaatteita säännöllisesti ja tiedotamme muutoksista yhteistyökumppaneillemme.

2 Tietoturvahuoneentaulu – ohjeet henkilöstölle

Tietoturvan kymmenen käskyä

1. Lukitse työhuoneen ovi aina poistuessasi ja luokan ovi päivän päätteeksi.
2. Suojaa kännykkä ja tietokone hyvällä salasanalla. Älä luovuta salasanaa kellekään.
3. Lukitse näyttö, kun poistut koneelta.
4. Säilytä henkilötietoja sisältävät dokumentit lukitussa kaapissa. Pidä näkyvillä vain työskentelyn aikana.
5. Säilytä ja välitä henkilötietoja vain virallisissa, suojatuissa palveluissa.
6. Älä näytä henkilötietoja muille kuin asianomaiselle.
7. Auta myös opiskelijoita huolehtimaan tietoturvasta.
8. Älä julkaise nimiä ja kuvia ilman lupaa.
9. Pidä luokissa ja työtiloissa opiskelijalistoja tai kuvia vain opiskelijoiden suostumuksella.
10. Siivoa säännöllisesti työpisteesi.

Lisätietoa

1. Lukitse työhuoneen ovi aina poistuessasi ja luokan ovi päivän päätteeksi.

Pitämällä ovet lukossa varmistamme, että henkilötiedot eivät joudu väärin käsiin. Tarkistathan siis aina poistuessasi, että ovi menee lukkoon.

2. Suojaa kännykkä, tietokone ja muistitikut hyvällä salasanalla. Älä luovuta salasanaa kellekään.

Salasanasta ei ole hyötyä, jos se on helposti murrettavissa. Hyvä salasana on helppo muistaa, mutta vaikea arvata tai tietokoneella laskea.

A. Pituus vähintään 8 merkkiä

Mitä pidempi salasana on, sitä vaikeampi se on koneellisesti murtaa.

B. Ei (ainakaan yksi) sana

Älä käytä sanakirjasanaa. Viestintäviraston (ks. lähde) ohjeessa on hyviä vinkkejä:

> Kun poimii pitkän, mutta helposti muistettavan, lauseen sanojen alkukirjaimet, saa muodostettua jo kohtalaisen hyvän salasanan.
> "Joulupukki tulee meille jo jouluaaton iltana, mutta muualla maailmassa usein vasta joulukuun 25. päivän vastaisena yönä!"
> -> *"Jtmjjimmmuvj25vy!"*
> Salasanana voi käyttää myös kokonaista lausetta, joka voi olla ulkopuoliselle aivan käsittämätön, kunhan sen itse muistaa. Esimerkiksi matkustuslippujen verkkopalveluun voisi toimia salalause:
> *Bussilla matkustaa 2 mustaa kissaa ja 3 valkoista koiraa, eli yhteensä 5 eläintä.*

Kaikki järjestelmät eivät välttämättä hyväksy välilyöntejä salasanoissa, mutta lauseen voi kirjoittaa myös "yhteen putkeen" tai yhdistää osat erikoismerkein esimerkiksi:

"Bussilla_matkustaa#2#mustaa_kissaa.."

Nämä sanakirjoista löytymättömät salasanat toimivat sanakirjahyökkäystä vastaan, jossa salasanan arvailuun käytetään valmiita sanaluetteloita. Kahden tai useamman sanan yhdistäminen hidastaa paljastumista vain vähän. Myös kirjainten korvaaminen yleisesti käytetyillä numerovastineilla (i-kirjain korvataan ykkösellä, o-kirjain nollalla jne.) on automatisoitu salasanojen murto-ohjelmiin.

C. Erikoismerkit käytössä

Käytä isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä.

D. Ei arvattavissa

Älä käytä nimiä, päivämääriä tai muita arvattavissa olevia osia salasanassasi. Myös yksinkertaiset (mutta pelottavat yleiset) salasanat kuten *salasana123* tai *kissa000* ovat todella helposti murrettavissa, koska murto-ohjelmat osaavat päätellä ihmisten suosimia geneerisiä salasanoja. Vältä myös näppäimistön geometrisiä kuvioita, kuten *qwerty* tai *12345*.

E. Vinkki: säilö apuohjelmiin

Turvallisimpia keinoja salasanojen hallintaan ovat erilaiset salasanasovellukset (engl. *password manager*), jotka tosin usein ovat maksullisia, jos niitä haluaa käyttää useilla eri laitteilla. Sovellukset luovat automaattisesti vahvoja salasanoja ja halutessa muistavat ne käyttäjän puolesta. Tällaisia sovelluksia ovat esimerkiksi LastPass, F-Secure Key tai vain Windowsille sopiva OneLocker. Sovelluksia käyttäessä riittää, että muistaa sovelluksen salasanan: muut salasanat ovat palvelun tallessa.

Lähde: http://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/12/ttn201412031257.html (luettu 13.4.2018)

Muistathan myös pitää eri salasanaa eri palveluissa: jos yhteen palveluun murtaudutaan, muut tietosi pysyvät edelleen salassa.

3. Lukitse näyttö, kun poistut koneelta.

Lukitseminen sujuu sekunnissa. Paina *ctrl+alt+del* ja sen jälkeen *enter* tai valitse Windows-valikosta profiili ja *lepotila*.

Älä anna opiskelijan käyttää henkilökohtaista tietokonettasi. Opiskelijalla ei saa missään nimessä olla pääsyä sinun tiedostoihisi ja tietoihisi, eikä toisaalta sinulle saa syntyä vahingossa mahdollisuutta päästä käsiksi opiskelijan tietoihin ja tiedostoihin esim. tietokoneen tai inhimillisen virheen vuoksi tallentuvien salasanojen vuoksi.

4. Säilytä henkilötietoja sisältävät dokumentit lukitussa kaapissa. Pidä näkyvillä vain työskentelyn aikana.

Säilytä vain tarpeelliset henkilötiedot ja muista hävittää ne heti, kun et enää tarvitse niitä. Arkistoitujen kokeiden, arvosanavihkojen ja muiden opiskelijatietoja sisältävien lomakkeiden tai muistikirjojen paikka on lukkojen takana aina silloin, kun ne eivät ole käytössä.

5. Säilytä ja välitä henkilötietoja vain virallisissa, suojatuissa palveluissa.

Säilytä vain tarpeelliset henkilötiedot. Säilytä tietoja vain Opiston virallisissa palveluissa: OneDrive-pilvessä, työkoneesi kovalevyllä, Wilmassa, Moodlessa ja lukitussa kaapissasi. Älä siis tallenna opiskelijatietoja esimerkiksi siviilisähköpostiisi tai kaupallisen toimijan pilvipalveluun, koska kuluttajakäytössä olevien palvelujen suojaukset voivat olla heikommat kuin yrityskäyttöön tarkoitetut.

Muistitikutkaan eivät saa sisältää henkilötietoja, mutta niitä voi käyttää esimerkiksi oppimateriaalien säilyttämiseen.

Esimerkiksi sähköpostitse tietoja siirtäessä on varminta häivyttää opiskelijan tiedot kokonaan ja puhua esimerkiksi vain nimikirjaimilla.

6. Älä näytä henkilötietoja muille kuin asianomaiselle.

Jos esimerkiksi näytät opiskelijalle tietoja Wilmasta, varmista, että näytöllä näkyy vain hänen tietonsa. Samoin videotykillä heijastaessa täytyy varoa, ettei näytä esimerkiksi läsnäololistaa opiskelijoille: vaikkapa sairaustiedot kuuluvat vain opettajan silmille.

7. Auta myös opiskelijoita huolehtimaan tietoturvasta.

Opasta opiskelijoita erityisesti hyviin salasanakäytäntöihin sekä yleisistä koneista uloskirjautumiseen ja sivuhistorian tyhjentämiseen.

8. Älä julkaise nimiä ja kuvia ilman lupaa.

Pyydä lupa opiskelijoiden ja henkilöstön tietojen julkaisemiseen. Älä myöskään toimita opiskelijan tietoja Opiston ulkopuolelle ilman hänen lupaansa, ellei kyseessä ole salassa pidettävän tiedon luovuttaminen lain nojalla (esim. lastensuojeluilmoitus).

9. Pidä luokissa ja työtiloissa opiskelija- tai asiakaslistoja tai kuvia vain henkilöiden omalla suostumuksella.

Varmista, että sinulla on opiskelijoiden suostumus tietojen julkaisemiseen myös luokassa. Kysy suostumus esimerkiksi vuoden alussa. Muista myös varmistaa vaikkapa uusia rästilistoja tai luokkakuvia esille laittaessasi, ettei kukaan mukana olevista opiskelijoista vastusta tiedon julkaisemista – opiskelijalla on oikeus muuttaa mieltään.

10. Siivoa säännöllisesti työpisteesi.

Tutustu ohjeistukseen, kuinka kauan mitäkin opiskelijatietoja säilytetään. Esimerkiksi vanhoja kokeita arkistoidaan puoli vuotta tai asuntolatietoja siihen asti, kun opiskelija muuttaa pois. Hävitä tiedostot ja asiakirjat heti, kun niitä ei enää tarvita.

3 Fyysinen tietoturva, tilat

Vieraskäytännöt
Opiskelijoita, asiakkaita tai vierailijoita ei saa päästää valvomatta opettajien työhuoneisiin tai toimistoihin.

Vierailijat käyttävät aina vain vierasverkkoa.

Henkilökunnan avaimia ei saa luovuttaa opiskelijoille eikä vierailijoille. Vierailijoiden avainten luovutukseen ja palauttamiseen kiinnitetään erityistä huomiota.

Tulostaminen
Henkilötietoja sisältävät tulosteet on tulostettava *yksityinen tulostus* -toiminnolla, jolloin tulosteet eivät tulostu käytävän koneille valvomatta.

4 Henkilökohtaiset työasemat ja muistivälineet

Ohjelmistojen käyttöoikeudet
- Työntekijä saa käsitellä vain sellaisia tietoja, joiden käsittelyyn hänellä on oikeus. Pääsy sähköisesti tallennettuihin henkilötietoihin on rajattu käyttöoikeuksilla ja henkilötietojen käsittelystä jää loki-merkintä.

Salaiseksi määritelty aineisto
- Käsiteltävä erityisen huolellisesti
- Ei koskaan sähköpostitse
- Vältetään paperisia versioita, tuloste vain kun se on välttämätöntä

Virustarkistus
- Opiston laitteet on suojattu F-Securen ohjelmistolla, joka tarkistaa koneen automaattisesti. Kone on sammutettava säännöllisesti vähintään kerran viikossa, jotta ohjelmistot päivittyvät.

Kirjoitussuoja
- Paljon opiston ulkopuolella työskentelevien suositellaan hankkivan suojan

Tiedostojen ja sähköpostien siivoaminen
- Poista vanhentuneet ja tarpeettomat sähköpostiviestit ja tiedostot vähintään 6 kk:n välein
- Älä säilytä tiedostoja tietokoneen työpöydällä: tallenna palvelimelle tai pilveen

Tiedostojen varmistus

- Pilvi- ja palvelintiedostoista otetaan automaattiset varmuuskopiot joka yö.

Verkko

- Opistolla käytä vain henkilökuntaverkkoa
- Vältä arkaluontoisten henkilötietojen käsittelyä avoimissa verkoissa. Omasta työpuhelimesta jaettu verkko on turvallisempi ja suositeltavampi kuin avoin verkko.

Henkilötietojen säilytys

- Henkilötietoja sisältäviä asiakirjoja ei saa tallentaa muistitikuille.
- Ensisijainen henkilötietojen säilytys- ja käsittely-ympäristö on Primus/Kurre/Wilma-järjestelmä.
- Välttämättömät paperiset henkilötietoja sisältävät asiakirjat säilytetään asianmukaisesti lukollisessa kaapissa.

4 Internet

Palomuuri

- Palomuurista vastaa Tietokeskus.

Ohjelmien lataaminen

- Opiskelijakoneille ei voi ladata ohjelmistoja. Henkilökunta: varmistathan, että lataat vain turvallisia ohjelmistoja turvallisista lähteistä. Älä asenna, jos et ole varma.

Välimuisti

- Oppilaskoneiden välimuisti ja selaushistoria tyhjenevät automaattisesti. Henkilökunta: tyhjennä säännöllisesti viikottain (huom! joka selaimella on oma välimuisti)

Selain

- Suositelemme käyttämään Chrome-selainta.

Sovelluksien käytön rajoitukset

- Työkonetta käytetään työtehtävien hoitoon. Älä lataa turhia sovelluksia, maksulliset sovellukset vain esimiehen kanssa sopimalla.

5 Ei julkisten tietojen hävittäminen

Henkilötiedot, luottamukselliset tiedot

Noudata henkilötietoselosteissa määriteltyjä aikamääreitä ja käytänteitä. Älä säilytä tarpeettomia henkilötietoja. Paperiset henkilötietoja sisältävät aineistot hävitetään silppurilla tai viedään tietosuojasäiliöön hävitettäväksi.

6 Tietosuojaan liittyvät ongelmatilanteet

Toiminta ongelmatilanteissa

Ongelmatilanteissa ole välittömästi yhteydessä tietosuojavastaavaan tai esimieheen. Mitä nopeammin tieto ongelmatilanteesta saadaan, sitä nopeammin löytyy ratkaisu ja mahdolliset vahingot jäävät pienemmiksi.

Havainto tietosuojariskistä

Mikäli havaitset Opistolla tai opiston toimintaan liittyvissä tilanteissa sellaisia riskitekijöitä, joita ei ole tässä ohjeistuksessa huomioitu, ilmoita asiasta tietosuojavastaavalle tai tiimisi tietosuojavastuulliselle.