lige adgang

Uddannelse, job og fællesskaber for alle

IT Sikkerhedspolitik

2024

Foreningen Lige Adgang

+45 93 89 43 83 info@ligeadgang.dk www.ligeadgang.dk Bygmestervej 10, 2400 KBH NV

Procedure i tilfælde af sikkerhedsbrud

I tilfælde af et sikkerhedsbrud i CRM-systemet Kople eller foreningens cloudserver, herunder sikker mail, vil alle partnere, som foreningen har databehandleraftaler med, samt Datatilsynet, blive underrettet. Underretningen sker skriftligt og hurtigst muligt efter opdagelsen af sikkerhedsbruddet, dog senest 72 timer efter foreningen er blevet bekendt med bruddet.

Introduktion og oplæring af medarbejdere

Alle nye medarbejdere, der arbejder med følsomme persondata, særligt dem der arbejder med foreningens mentor- og studenterjobprojekter med adgang til Kople, gennemgår sidemandsoplæring og introduceres til foreningens forskellige vejledninger om journalføring og opgaveoprettelse i Kople samt brugen af foreningens 'Secure Mail' kontor til skriftlig kommunikation med partnere og relevante borger-sager.
En gang om året gennemføres der awareness-træning med alle medarbejdere involveret i foreningens mentorarbejde, så både nye og gamle medarbejdere kollektivt gennemgår retningslinjer og procedurer for sikker og ansvarlig håndtering af følsomme persondata både indenfor og udenfor Kople og eventuelt andre relevante datastyringssystemer. Under denne awareness-træning indsamles relevante erfaringer fra de involverede medarbejdere, og på baggrund af denne feedback opdateres eksisterende vejledninger, og retningslinjer og procedurer kvalitetssikres i samarbejde med projektledere og foreningens direktør.

Opbevaring og sletning af persondata

Persondata (foreningens egne og information om partnere m.v.) opbevares generelt kun i foreningens formelle systemer (e-mails, OneDrive, Teams) indenfor Office 365 med tilhørende sikkerhed og automatiske opdateringer. Følsomme persondata opbevares kun i foreningens sikre CRM-database Kople og SUGAR.

Profiler på mentorer og mentees slettes systematisk efter endt samarbejde. Dette sker indenfor 6 måneder, da igangsatte processer kan fortsætte op til 6 måneder efter kontraktudløb, medmindre andet er aftalt med databehandleren. Profiler på mentorer og

mentees slettes også straks, hvis foreningen modtager en mundtlig eller skriftlig anmodning fra mentor eller mentee.
Mentorer, der har været inaktive i foreningens mentorkorps i en kortere eller længere periode, skal årligt beslutte, om de stadig ønsker at være registreret i foreningens mentor-database og dermed om foreningen må beholde eller skal slette deres persondata.
I tilfælde, hvor følsomme persondata skal deles med partnere, sker dette altid i overensstemmelse med den specifikke databehandleraftale og kun via sikker mail. Alle e-mails sendt og modtaget via sikker mail gennemgås og slettes halvårligt. Ansvar for sletning af disse e-mails påhviler projektlederne indenfor de specifikke projekter.

Brug af persondata til udvikling, test og lignende formål

I tilfælde hvor udvikling, test og lignende behov opstår, oprettes og anvendes dummy-profiler baseret på fiktive personer. Foreningen anvender aldrig persondata, herunder følsomme persondata, på mentorer eller mentees til disse formål.

Brug af netværk

Medarbejdere i foreningen må aldrig bruge åbne netværk til at få adgang til persondata, herunder følsomme persondata. Kun lukkede og sikre netværk må bruges til at få adgang til Office 365, SUGAR og Kople.

På foreningens kontor anvendes fysiske eller Wi-Fi-forbindelser til de lukkede netværk 'FSA' eller 'FSA Guest'. Hvis adgang til Office 365, SUGAR og Kople er nødvendig, må dette kun ske via sikre netværk, herunder brug af arbejdstelefon som mobil hotspot, og kun hvis det mobile internetdeling er passwordbeskyttet. Ved brug af andre netværk skal adgang til Office 365, SUGAR og Kople også kun ske via et sikkert og lukket netværk.

Overførsel af persondata på forskellige kommunikationsenheder

Det er ikke tilladt at få adgang til Office 365 eller SUGAR via personlige kommunikationsenheder såsom private telefoner eller tablets. Det er tilladt at få adgang til disse programmer via arbejdstelefoner.

To-faktor autentifikation (2FA)

Alle medarbejdere skal anvende to-faktor autentifikation (2FA) ved adgang til Office 365, SUGAR og Kople. Foreningen anvender Microsoft Authenticator til 2FA, hvilket sikrer et ekstra lag af sikkerhed ved login. Medarbejdere skal sørge for, at deres Microsoft Authenticator-app er opdateret og korrekt konfigureret på deres arbejdsenheder.

Automatiske opdateringer

Foreningen sørger for, at alle systemer og software, herunder Office 365, SUGAR og Kople, holdes opdaterede med de nyeste sikkerhedsopdateringer. Automatiske opdateringer er aktiveret for at sikre, at systemerne altid har den nyeste beskyttelse mod sikkerhedstrusler.

Årlig gennemgang og opdatering af IT-sikkerheds- og GDPR-politik

IT- sikkerhedspolitikken gennemgås og revideres ved jævne mellemrum, herunder opdateringer af arbejdsprocesser, retningslinjer og beskrivelser. Politik og procedurer gennemgås og opdateres blandt andet ved større ændringer i IT-infrastrukturen, indførelse af nye systemer eller teknologier, ændringer i lovgivningen, eller efter oplevelsen af sikkerhedshændelser. Gennemgangen foretages af foreningens direktør i samarbejde med foreningens eksterne IT-leverandør KIMO Consult og involverer mindst en projektleder indenfor mentorområdet med kendskab og erfaring med daglig brug af foreningens databaser, Kople og Sugar.

Den årlige gennemgang dokumenteres ved at opdatere IT-sikkerheds- og GDPR-politikken, som gemmes og distribueres til alle medarbejdere i organisationen i et nyt format med det aktuelle kalenderår på dokumentets forside.

Password-politik

Alle medarbejdere ændrer deres adgangskoder til Office 365, SUGAR og Kople hvert år. Påmindelser om dette sendes via e-mail til alle medarbejdere. Personlige adgangskoder skal være mindst 8 tegn lange og indeholde både bogstaver, tal og symboler. Foreningens direktør sikrer sammen med foreningens eksterne IT-leverandør KIMO Consult, at alle medarbejdere i organisationen ændrer deres adgangskoder i overensstemmelse med foreningens password-politik. Dette sker i forbindelse med den årlige gennemgang og opdatering af foreningens samlede IT-sikkerheds- og GDPR-politik.

Sikring af sletning/destruktion af datamedier

Sletning/destruktion af datamedier udføres som følger:

- Bærbare og stationære computere sendes til reinstallation hos KIMO Consult, når medarbejdere skifter eller før donation eller destruktion.
- Fabriksindstilling på arbejdstelefoner ved overlevering mellem medarbejdere.
- Forbud mod opbevaring af persondata, herunder følsomme persondata, på eksterne enheder såsom USB-sticks, eksterne harddiske osv.

Fortrolighed

Alle medarbejdere samt studenter og virksomhedspraktikanter i organisationen underskriver en fortrolighedsaftale ved deres ansættelse i foreningen. Fortrolighed understreges også løbende i forbindelse med håndtering af følsomme persondata.