Retningslinjer for klassifisering og lagring av informasjon, samt daglig informasjonssikkerhet

Innhold

1. Formål

Fagskolen Diakonova må ifølge personopplysningslovgivningen ha kontroll på sin håndtering av personopplysninger og taushetsbelagt informasjon. Alle medarbeidere skal opptre på en slik måte i det daglige at de ivaretar god informasjonssikkerhet i virksomheten. Formålet er å sikre vern av enkeltmenneskers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger.

Instruksen er teknologinøytral, som innebærer at det ikke vil medføre å følge et spesifikt teknologisk produkt eller programvare. Instruksen gjelder uavhengig av hvordan informasjonen er lagret/oppbevart, enten det er på papir, lyd og bilde eller digitalt i en eller annen form.

2. Ansvar og målgruppe

- Ansatte (fulltid, deltid og midlertidig ansatte)
- Innleide konsulenter/oppdragstakere
- Alle som har tilgang til, og/eller bearbeider og forvalter informasjon gjennom IKT-infrastrukturen som Fagskolen Diakonova bruker

Den enkelte virksomhets ledelse er ansvarlig for at alle medarbeidere er kjent med og følger retningslinjer for informasjonssikkerhet.

Den enkelte bruker er personlig ansvarlig for sin håndtering av all informasjon. Brudd på denne instruksen og/eller annet regelverk, vil kunne sanksjoneres på ulike måter avhengig av type brudd.

3. Klassifisering av informasjon

Klassifisering	Beskrivelser	Eksempel	Tilgang/overføring av data
Åpen informasjon	Åpen informasjon som er tilgjengelig for alle uten særskilte tilgangsrettigheter. Informasjon som ikke kan skade noen.	• Åpne nettsider og sosiale medier • Offentlig tilgjengelig informasjon, inkludert publiserte retningslinjer • Offentlig kontaktinformasjon om ansatte på Fagskolen Diakonovas nettsider	**Åpen**
Gul data	Intern benyttes om informasjon som er begrenset til å være tilgjengelig for medarbeidere blant annet for å gjennomføre pålagte oppgaver. Informasjon på avveie kan gi moderate økonomiske skader og/eller svekket omdømme for Fagskolen, enkeltindivider eller samarbeidspartnere hvis den kommer uautoriserte i hende.	• Enkelte arbeidsdokumenter • Personopplysninger om ansettelsesforhold, f.eks. ansattnummer • Interne regler, policy osv.	Begrenset tilgang til interne medarbeidere. Informasjonen kan være tilgjengelig med kontrollerte tilgangsrettigheter for eksterne som har tjenstlig behov for informasjon. Informasjon kan sendes via e-post både internt og eksternt. Papirkopier skal ikke henlegges utenfor Fagskolens lokaler uten tilsyn.

Klassifisering	Beskrivelser	Eksempel	Tilgang/overføring av data
Røde data	Informasjon som kan medføre skade for Fagskolen Diakonovas formål, samarbeidspartnere, enkeltindivider og/eller offentlige interesser og samfunnet om den kommer på avveie og uautoriserte i hende. Informasjon som er omfattet av lovbestemt og avtalemessig taushetsplikt.	• Personopplysninger som f.eks. fødselsnummer • Taushetsbelagte opplysninger • Dokumentasjon av tekniske løsninger, driftsrutiner eller prosedyre som kan utnyttes i angrep på IT-systemer • Informasjon om sårbarheter som ved utnyttelse kan medføre store skader, for eksempel risikovurdering eller revisjonsrapporter	Informasjon skal kun være tilgjengelig for medarbeidere med kontrollerte rettigheter og som har behov for denne informasjonen for å utføre en pålagt oppgave. I spesielle tilfeller kan røde/svarte informasjon også gjøres tilgjengelig for eksterne under samme kontrollerte tilgangsrettigheter. Informasjon kan sendes via intern e-post. Eksternt så må det benyttes kryptert løsning om det sendes via epost. Papirkopier: • Utskrift skal skje mens man er til stede ved skriver • Makuleres eller legges i beholder for makulering • Papirer oppbevares i låst skap • Sendes i lukket konvolutt til navngitt

Svart data	Informasjon som kan medføre meget betydelig skade for Fagskolen Diakonovas formål, omdømme, samarbeidspartnere, enkeltindivider og/eller offentlige interesser og samfunnet om den kommer på avveie og uautoriserte i hende. Slik informasjon skal være tydelig merket på hver side av dokumentet.	• Særlige kategorier av sensitive personopplysninger, f.eks. fagforeningsmedlemskap, helseopplysninger, religion etc • Særlige forretningsmessige og/eller strategiske sensitive/hemmelige opplysninger Feil i informasjonen kan gi betydelig erstatningsansvar, tap av kontrakter og omdømme.	Informasjon skal kun være tilgjengelig for medarbeidere med kontrollerte rettigheter og som har behov for denne informasjonen for å utføre en pålagt oppgave. I spesielle tilfeller kan strengt fortrolig informasjon også gjøres tilgjengelig for eksterne. Overføring, overføringstiltak og sikkerhetsvurdering må godkjennes av lokal databehandlingsansvarlig, personvernombudet eller informasjonssikkerhetsansvarlig. Papirkopier: • Utskrift skal skje mens man er til stede ved pålogget skriver • Makuleres eller legges i beholder for makulering • Papirer oppbevares i låst skap • Sendes i dobbel konvolutt, innerste konvolutt merkes strengt konfidensielt, ytterste konvolutt adressers autorisert mottaker • Papirkopier bør ikke tas ut av Fagskolen Diakonovas lokaler

4. Guide for lagring av informasjon

Generelle råd:
• Lagringsområdet må være tilgangsstyrt for å lagre røde/svarte informasjon der. • Ikke lagre på C:-området på din PC («Mine dokumenter»), med mindre det er midlertidig hvis du trenger tilgang til dokumenter uten nettilgang. Dokumentene skal slettes fra C:-området og flyttes til hjemmeområde/fellesområde på Fagskolens server så raskt som mulig når det ikke lenger er nødvendig å oppbevare dem på C:-området. • Opprett en rutine med jevnlig rydding og sletting av e-post og dokumenter som du ikke lenger trenger å oppbevare.

5. Retningslinjer for daglig informasjonssikkerhet

- Brukernavn og passord må ikke deles med andre. Alle brukere skal ha eget brukernavn og passord til alle systemer.
- Oppbevaring, bruk og sikring av passord/PIN-kode/sikkerhetskoder for elektronisk ID skal være iht. fastlagte prosedyrer. NB! Må aldri oppgis på telefon eller i e-post.
- Logge av/låse PC når du går i fra den. Når du forlater arbeidsplassen og ved arbeidsdagens slutt skal bruker logge ut av alle systemer
- Du skal ikke lagre røde/svarte personopplysninger *ukryptert* på bærbart utstyr som for eksempel minnepinne, eller sende det via åpen e-post. Ta ikke med bærbart utstyr med ukrypterte røde/svarte data utenfor kontoret/arbeidsplassen.
- Du skal ha kontroll på dokumentene dine
    - Hent utskrifter med en gang
    - Skriv ut kun det du må
    - Ikke legg igjen dokumenter på møterom
    - Ha gode makuleringsrutiner

- Det er forbudt å lese, søke eller på annen måte tilegne seg eller bruke røde/svarte opplysninger fra fagskolens datasystemer, om andre ansatte eller brukere, uten at det er begrunnet eller har særskilt hjemmel i lov eller forskrift
- Taushetsplikt gjelder også mellom personell, som inkluderer både ansatte og eksterne oppdragstakere/innleide konsulenter
- Pass på at ikke uvedkommende lytter når du snakker om røde/svart data med en kollega, i telefon eller på offentlig sted
- Pass på at uvedkommende ikke har innsyn
- Når du deler røde/svarte opplysninger med andre, må du forsikre deg om at vedkommende du kommuniserer med har rett til å få opplysningene. Mottar du f.eks. telefonsamtaler om studenter, og du er i tvil om identiteten til innringer, kan du be om å få ringe vedkommende tilbake.
- Dobbeltsjekk at e-post/SMS du sender ikke inneholder rød/svart informasjon
- Ikke bruk sosiale medier for å snakke eller skrive om jobbrelatert informasjon som regnes som intern eller røde/svarte data
- Følg avviksrutiner og bruk avvikssystemet
- E-post og vedlegg til e-post fra mistenkelig ukjent avsender skal ikke åpnes
- Vær kritisk til lenker og innhold i e-post (uærlige aktører med baktanker). Du kan få virus og spam på datamaskinen
- Installer kun programvare på din jobb-PC som er jobbrelevant og hent godkjennelse fra IT-seksjonen hvis du er usikker. Nedlastning for privat bruk vil som regel ikke godkjennes.
- Mobilen du har fått utdelt av jobben eller som du bruker i jobbsammenheng må være sikret med kodelås.
- Forsikre deg om at jobbrelevante programmer på din mobil (som e-post) er beskyttet med egen lås (kode, passord) for å hindre at røde/svart informasjon kommer på avveie hvis mobilen blir stjålet, hacket eller lignende.
- Utskrifter med personopplysninger skal oppbevares i låsbart skap og makuleres etter bruk.
- Elektronisk forsendelse av helse- og personopplysninger (e-post, meldingsutveksling mv.) skal krypteres.
- Det er ikke tillatt å laste ned uønsket innhold fra nettsider og sosiale medier.
- Det er ikke tillatt å bruke jobb-PC og jobbrelaterte programmer på mobilen for oppkobling i usikret internettnettverk (f.eks. i kafe, flyplass etc.)
- Rydd din e-postkasse hvert tertial og slett e-postene som ikke lenger er nødvendig å oppbevare eller arkivere.

6. Guide for sletting av informasjon

Personopplysninger skal ikke lagres lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen hvis ikke annet er bestemt i lov eller

f.eks. i forbindelse med finansiering av utvikling. Det vil si at når formålet er nådd, skal opplysningene slettes, selv om de som er registrert ikke har bedt om det. Formålet med behandlingen av de aktuelle opplysningene, samt hva som er det rettslige grunnlaget for innhentingen, er sentralt i vurderingen av når opplysninger skal slettes.

Virksomheten må også slette opplysningene av eget tiltak dersom behandlingen er basert på samtykke og enkeltpersoner trekker tilbake samtykket sitt, med mindre opplysningene samtidig behandles for andre formål basert på andre behandlingsgrunnlag.

Lokal behandlingsansvarlig har ansvar for å utarbeide rutiner for sletting som skal minimalisere sikkerhetsrisikoen i sin enhet. **Systemeier** har dette ansvaret for det systemet vedkommende er systemeier for og **lokal behandlingsansvarlig** har ansvar for gjennomgående administrative prosesser.

Hver enkelt medarbeider er ansvarlig for å slette personopplysninger som er lagret på vedkommende sitt personlige brukerområde. **Lokal behandlingsansvarlig** er ansvarlig for at personopplysninger blir slettet på fellesområder i sin enhet.

- Dersom personopplysninger som ikke skal oppbevares med hjemmel i arkivloven (5 år) eller annen lovgivning (eks. regnskapsloven 10 år), skal de slettes når det ikke er nødvendig lenger å oppbevare dem.
- Unødvendige personopplysninger etter at en ansatt slutter skal slettes innen 6 måneder.
- Personopplysninger som det er midlertidig nødvendig å lagre på passordbeskyttet fellesområde eller personlig område i forbindelse med utføring av en arbeidsoppgave, skal slettes når formålet ikke lenger er til stede.
- Medlemmer i styrer, nemnder og utvalg som får tilsendt saksdokumenter elektronisk som inneholder taushetsbelagte eller sensitive personopplysninger, skal slette tilsendt materiale når saken er behandlet.
- Arkivpliktige dokumenter, dvs. dokumenter som er gjenstand for saksbehandling og har verdi som dokumentasjon, skal arkiveres i institusjonens arkivsystem.

Se ellers Personalhåndboka for egne lagring- og slettingsrutiner for diverse prosesser innen HR, lønnskjøring, bilde- og videoopptak m.m. Referanse:

Datatilsynet https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/personalmappe/

7. Regler for oppbevaring på privat datamaskin

Du kan oppbevare intern informasjon på privat datamaskin hvis:

1. ... det er snakk om små mengder data

Man skal kun oppbevare de dataene man jobber med i øyeblikket, og ikke oppbevare og lagre store mengder data på lengre sikt.

2. ... du ikke synkroniserer mye interne data automatisk

Du har altså ikke lov til å jevnlig eller automatisk synkronisere over store mapper med data. Kun de dataene som det er behov for, skal befinne seg lokalt på din maskin. Dette er en vurdering den enkelte ansatte må gjøre. Fagskolen ønsker ikke at data kommer på avveie, og alle må bidra til å begrense omfanget dersom det skulle skje.

3. ... dataene bare er tilgjengelig for deg

Andre brukere av maskinen skal ikke ha tilgang til dataene. Familie og venner som låner maskinen skal ha egne kontoer.

4. ... datamaskinen din er tilstrekkelig sikret

- Automatisk sikkerhetsoppdateringer skal være skrudd på.
- Du skal bruke automatisk skjermlås, slik at ingen kan bruke maskinen hvis du forlater den mens du er logget inn.
- Passordene for deg selv og eventuelle administratorbrukere skal være gode, og byttes jevnlig.
- Vi anbefaler at harddisken er kryptert, og at maskinen skrus helt av under transport. Moderne maskiner har gode løsninger for dette.

5. ... din bruk av maskinen er tilstrekkelig sikret

- Du skal utvise forsiktighet og skepsis til lenker i e-post og på ukjente nettsider.
- Du skal være forsiktig med bruk av ukjente trådløsnett, spesielt på reise.
- Du skal kjenne maskinen og hvordan den oppfører seg. Vit hvilke programmer du har installert.
- Ikke installer flere programmer og apper enn du trenger.
- Vit hvilke programmer som kan tenkes å kopiere mapper og filer til ulike private backup- eller skyløsninger, og sørg for at mappene med Fagskolen-data ikke havner hos f.eks. Adobe, Google Music, Apple eller Get sin backupløsning.

Referanse: Lagring av gule data på private maskin, Universitetet i Oslo (UiO)

Beskrivelse lagringsområde	*Gule data*	*Røde data*	*Svarte data*
Lagring på PC			
Privateid PC	*Små mengder data (se siste side)*		
Fagskolen Diakonova stasjonær PC eller bærbar PC på internt nettverk	*√*	*√*	
Fagskolen Diakonova bærbar PC koblet opp med VPN løsning	*√*	*√*	
Fagskolen Diakonova bærbar PC som ikke er koblet opp med VPN	*√*		
Minnepinne/ekstern harddisk – ikke kryptert	*Små mengder data (se siste side)*		
Minnepinne/ekstern harddisk - kryptert	*√*	*√*	*√*
E-post			
Personlig e-post (gmail, hotmail og lignende)	*Ikke tillat*		
Fagskolen Diakonova e-post	*√*	*√*	
Fra Fagskolen Diakononva e-post til ekstern e-post	*√*		

Beskrivelse lagringsområde	*Gule data*	*Røde data*	*Svart data*

Lagringstjenester			
Privat skytjeneste (f.eks.: Outlook, gmail, iCloud, Dropbox)	***Ikke tillat***		
Fagskolen Diakonova fellesområde (felles mapper som er tilgangsstyrt)	***√***	***√***	
Fagskolen Diakonovas hjemmeområde (dokumenter som du lagrer i ditt H:området)	***√***	***√***	***√ (med to faktor tilgang styring, ikke sensitive personopplysninger)***
STUDD	***√***	***En del (kun fødselsnummer, karakterer)***	
Breeze	***√***	***√ (fødselsdato)***	
Admincontrol	***√***		
Onedrive (Office 365)	***√***	***√ (med tilgang styring, ikke stor mengde personopplysninger)***	
P360 arkiv	***√***	***√***	***√***
Teams	***√***		
Administrative tjeneste			
HR portal (Visma)	***√***	***√***	***√***
Publiseringsløsning			

Finn.no (med begrenset tilgang)	***√***	***√***	
Jobbnorge.no (med begrenset tilgang)	***√***	***√***	
Andre tjenester			
Nettskjemaer uten kryptering og sikre koblinger	***√***		
Nettskjemaer med kryptering og sikre koblinger	***√***	***√***	***√***
Instant Messaging uten begrenset tilgang og tilsvarende for Skype chattefunksjon	***√***		

Mobil:
Det skal som regel ikke lagres jobbrelatert informasjon lokalt på mobilen, men man kan åpne og lese e-post og vedlegg på tilgangskontrollerte programmer på mobilen.