conexus

Databehandleravtale

for Conexus Engage

mellom

Meland kommune
behandlingsansvarlig
og
Conexus AS
databehandler

1. Avtalens hensikt

Formålet med denne databehandleravtalen er å regulere Databehandlers behandling av personopplysninger på vegne av den Behandlingsansvarlige i tråd med kravene i personopplysningsloven og personvernforordningen.. Avtalen skal være et ledd i oppfyllelsen av art. 28 i personvernforordningen. I det følgende vil disse regelverkene bli betegnet som "Personvernreglene".

Avtalen regulerer også partenes rettigheter og plikter ved behandling av data og informasjon som er underlagt taushetsplikt i medhold av annet regelverk eller avtale.

Avtalen skal sikre at personopplysninger eller annen taushetsbelagt informasjon ikke brukes urettmessig eller kommer uvedkommende i hende.

Avtalen regulerer Databehandlers bruk av personopplysninger og annen taushetsbelagt informasjon på vegne av den Behandlingsansvarlige, herunder innsamling, registrering, sammenstilling, lagring, utlevering eller kombinasjoner av disse, m.m.

2. Definisjoner

Følgende definisjoner, som gjøres gjeldende i denne avtalen, fremgår av personvernforordningens art. 4.:

- Nr. 1: "personopplysninger" - enhver opplysning om en identifisert eller identifiserbar fysisk person ("den registrerte"); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f. eks et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en onlineidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet,

- Nr. 7: "behandlingsansvarlig" - en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med- og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett.

- Nr. 8: "databehandler" - en fysisk eller juridisk person, offentlig myndighet, institusjon, eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.

- Nr 12. "Brudd på personopplysningssikkerheten" - et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret, eller på annen måte behandlet.

3. Formål

Conexus Engage er et digitalt verktøy for kartlegging og oppfølging av elever. Det benyttes både av forskjellige brukergrupper som for eksempel lærere, skoleledere og skoleeier for å sikre kvalitet på undervisning på individnivå.

Innsamling og behandling av personopplysningene er nødvendig for å gi brukere et faktabasert grunnlag til å tilpasse undervisning til de enkelte elevers behov.

For å kunne identifisere og tilordne andre opplysninger på riktig individ, samt for å kunne utøve en korrekt tilgangsstyring, er det absolutt nødvendig å bruke personnummer som identifikator alle registrerte brukere og registrerte individer.

4. Databehandling

Behandlingen av personopplysninger som databehandleren gjør på vegne av den behandlingsansvarlige, består i å registrere brukere og elever.

Brukeropplysninger registreres og lagres og kan kobles til enkelte elementer, som kartlegginger, vurderinger og karakterer i løsningen.

Ved sletting av brukere blir disse koblingene fjernet og alle registrerte kartlegginger, vurderinger og karakterer anonymiseres.

Det produseres og arkiveres en rapport for avgangselever som oppbevares i løsningen i opp til 12 måneder. Brukere får innsynsprivilegier til rapporten iht. oppsett valgt av databehandleransvarlig.

Brukeradministratorer kan bare få innsyn i personlig identifiserbare data i sin egen organisasjon. Brukere får innsynsprivilegier iht. oppsett valgt av databehandleransvarlig.

Behandlingen er ikke tidsbegrenset og varer inntil avtalen sies opp av en av partene.

5. Partenes plikter

Databehandler skal følge de rutiner og instrukser for behandlingen som Behandlingsansvarlig til enhver tid har bestemt skal gjelde.

Dersom Databehandler mottar instruks som Databehandler mener bryter med Personvernreglene, skal Databehandler umiddelbart informere Behandlingsansvarlig.

Databehandlers ansatte/andre som opptrer på vegne av databehandler
Samtlige aktører som på vegne av Databehandler utfører oppdrag der bruk av / tilgang til Informasjon inngår, skal være kjent med Databehandlers avtalemessige og lovmessige forpliktelser overfor Behandlingsansvarlig og påta seg å etterleve disse.
(se vedlegg F)

6. Databehandlers taushetsplikt

Databehandler har taushetsplikt om Informasjonen og all annen relevant dokumentasjon som Databehandler får tilgang til iht. denne databehandleravtalen.
Taushetsplikten gjelder også etter opphør av Leveranseavtalen og denne databehandleravtalen.

Databehandler skal innhente taushetserklæring fra egne ansatte og andre som gis tilgang til Behandlingsansvarliges Informasjon og annen relevant dokumentasjon i anledning oppdrag disse utfører for Behandlingsansvarlig, før tilgang til informasjonen gis.

(se vedlegg F)

7. Overføring av data til utlandet

Informasjonen kan ikke uten skriftlig godkjenning fra Behandlingsansvarlig overføres til land utenfor EØS. Ved inngåelse av avtale om slik overføring skal Databehandler inngå "EUs Model Contract Clauses" med Behandlingsansvarlig som eksportør, og overføringene være i henhold til disse bestemmelsene.

8. Bistand til å svare på anmodninger som gjelder de registrertes rettigheter

Ved innsynskrav må databehandler bistå ved å samle opplysningene som er lagret om den registrerte. Databehandler må gjøre opplysningene tilgjengelig for den behandlingsansvarlige for at den behandlingsansvarlige kan vurdere innsynskravet.

(Se vedlegg D)

conexus

9. Bruk av underleverandør

Databehandleren har den behandlingsansvarliges generelle godkjennelse til å bruke andre databehandlere.
Dersom databehandler benytter seg av underleverandør eller andre som ikke normalt er ansatt hos databehandler skal dette avtales skriftlig med behandlingsansvarlige før behandlingen av personopplysninger starter.

Benytter databehandler underleverandører som behandler data på vegne av seg skal tilsvarende avtale tegnes med underleverandør.

Den enkelte Databehandler plikter fortløpende å føre å føre en oversikt over alle underleverandører/ tredjeparter/ samarbeidspartnere som benyttes i Leveranseavtalen og fremlegge denne for behandlingsansvarlig på forespørsel

Samtlige som på vegne av databehandler utfører oppdrag der bruk av de aktuelle personopplysningene inngår, skal være kjent med databehandlers avtalemessige og lovmessige forpliktelser og oppfylle vilkårene etter disse.

Hvis den andre databehandleren (underleverandøren) ikke oppfyller sine forpliktelser med hensyn til vern av personopplysninger, har databehandleren det fulle ansvaret overfor den behandlingsansvarlige.

(Se vedlegg G)

10. Sikkerhet

Databehandler skal oppfylle de krav til sikkerhetstiltak som stilles etter person opplysningsloven og personopplysningsforskriften, herunder særlig personopplysningslovens § 32. Databehandler skal dokumentere rutiner og andre tiltak for å oppfylle disse kravene. Dokumentasjonen skal være tilgjengelig på behandlingsansvarliges forespørsel.

Avviksmelding/melding om brudd på personopplysningssikkerheten skal skje ved at Databehandler melder avviket til Behandlingsansvarlig. Behandlingsansvarlig har ansvaret for at avviksmelding/melding om brudd på personopplysningssikkerheten sendes Datatilsynet.

Databehandler plikter å gi behandlingsansvarlig tilgang til sin sikkerhetsdokumentasjon, og bistå, slik at behandlingsansvarlig kan ivareta sitt eget ansvar etter lov og forskrift.

Behandlingsansvarlig har, med mindre annet er avtale eller følger av lov, rett til tilgang til og innsyn i personopplysningene som behandles og systemene som benyttes til dette formål. Databehandler plikter å gi nødvendig bistand til dette.
(se vedlegg C, D, E og F)

11. Sikkerhetsrevisjoner

Den behandlingsansvarlige eller en representant for den behandlingsansvarlige, gjennomfører et fysisk tilsyn hos databehandler for å sikre at databehandleravtalen overholdes. Hyppighet og tidspunkt avtales mellom behandlingsansvarlig og databehandler.

conexus

12. Avtalens varighet

Avtalen gjelder så lenge databehandler behandler personopplysninger på vegne av behandlingsansvarlig.
Ved brudd på denne avtale eller personopplysningsloven kan behandlingsansvarlig pålegge databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

13. Ved opphør

Databehandleren er forpliktet til å tilbakelevere alle personopplysninger som er behandlet på den behandlingsansvarliges vegne til den behandlingsansvarlige ved opphør av avtaleforholdet, og deretter slette egne kopier.
Databehandler skal skriftlig dokumentere at sletting og eller destruksjon er foretatt i henhold til avtalen innen rimelig tid etter avtalens opphør.

14. Personopplysninger som samles inn

Se vedlegg A

15. Slette- og anonymiserings regler

Se vedlegg B

16. Operasjonell kommunikasjon / meddelelser

Forespørsler om innsyn, sletting, bistand, meddelelser, samt avviksmeldinger etter denne avtalen skal sendes skriftlig mellom partene:

Forespørsler om innsyn, sletting, bistand, meddelelser	
Til / fra Conexus	Til / fra Meland kommune
E-post: support@conexus.no	E-post: reidun.elin.johannessen@meland.kommune.no
Post: Conexus AS Grønland 67 3045 Drammen	Post: Postboks 79 5906 FREKHAUG
Avviksmeldinger	
Til / fra Conexus	Til / fra Meland kommune
E-post: support@conexus.no	E-post: reidun.elin.johannessen@meland.kommune.no ev. www.iktnh.no
Post: Conexus AS Grønland 67 3045 Drammen	Post: Postboks 79 5906 FREKHAUG

17. Lovvalg og verneting

Avtalen er underlagt norsk rett og partene vedtar Drammen tingrett som verneting. Dette gjelder også etter opphør av avtalen.

Denne avtale er i 2 – to eksemplarer, hvorav partene har hvert sitt.

Vedlegg:
Vedlegg A – Conexus Engage Databehandleravtale – Personopplysninger
Vedlegg B – Conexus Engage Databehandleravtale – Slette regler
Vedlegg C – Conexus Sikkerhets Policy
Vedlegg D – Conexus Sikkerhets Organisasjon
Vedlegg E – Forespørsel om innsyn, informasjon og sletting
Vedlegg F – Prosedyrer for behandling av personopplysninger og sensitive personopplysninger
Vedlegg G – Underleverandører, data lagring og tilgang til produksjonsdata

For Meland kommune – behandlingsansvarlig	For Conexus AS - databehandler
Frekhaug 13.07.2018	Drammen 02.07.2018
Sted og dato	Sted og dato
Reidunn Jobs	
Signatur	Signatur

conexus

Vedlegg B – Conexus Engage Databehandleravtale – Sletteregler

	Utløsende faktor	Tiltak	Data i produksjon	Tilgang til data for brukerne	Data i backup
1	Avtalen utløper	Alle data er gjøres utilgjengelige for brukerne. Sletting av data iverksettes	Fjernes iht. tekniske sletterutiner	Ingen tilgang	Oppbevares i maksimalt 12 måneder
2	Databehandlings-ansvarlig ber om sletting	Data gjøres utilgjengelig for de forespurte brukerne. Sletting av data iverksettes. Det er kun databehandlingsansvarlig som kan be Conexus om sletting.	Fjernes iht. tekniske sletterutiner	Ingen tilgang	Oppbevares i maksimalt 12 måneder
3	Et individ ber om at data skal slettes	Informer databehandlingsansvarlig. Dersom databehandlingsansvarlig har integrasjon mellom SAS (skoleadministrativt system) og Conexus Engage, må databehandlingsansvarlig slette individet i SASet. Når slettingen er utført i SAS vil data automatisk slettes i Engage. Dersom databehandlingsansvarlig ikke har integrasjon, kan brukeradministrator slette individet i Conexus Engage.	Fjernes iht. tekniske sletterutiner	Full tilgang	Oppbevares i maksimalt 12 måneder
4	Dataintegriteten har blitt brutt.	Ved indikasjoner på eller oppdagelse av brudd på integriteten, skal det etableres kommunikasjon mellom behandlingsansvarlig og	Løsningen er frakoblet inntil integriteten er gjenopprettet	Ingen	Backup kan brukes i forbindelse med tilbakerulling .

conexus

	Utløsende faktor	Tiltak	Data i produksjon	Tilgang til data for brukerne	Data i backup
		databehandler i den hensikt å identifisere omfanget og årsaken til integritetsbruddet. Dersom integritetsbruddet skyldes eksterne årsaker (f.eks. datainntrenging), skal tjenesten umiddelbart tas ned og en beredskapsgruppe opprettes. Denne skal først: - sikre eksisterende data - rette informasjonselementer med feil og/eller fjerne skadede data - gjenopprette integriteten i løsningen			

conexus

Vedlegg C – Conexus Sikkerhets Policy

Conexus Sikkerhets Policy

Sikkerhetsmål og sikkerhetsstrategi for behandling av personopplysninger ved Conexus AS.

Innledning

Dette dokumentet gjelder elektronisk og manuell behandling av personopplysninger som ledd i tjenester levert av Conexus AS. Dokumentet definerer overordnede krav og retningslinjer som gjelder behandling av personopplysninger.

Conexus Security Policy er en støttende policy til de enkelte databehandleravtaler.

Målgruppe er alle ansatte, partnere, kunder og underleverandører og andre som behandler personopplysninger som ledd i tjenester levert av Conexus AS.

Mål for arbeidet med behandling av personopplysninger

Conexus AS har et løpende mål om trygg behandling av personopplysninger gjennom å sikre konfidensialitet, integritet, tilgjengelighet, samt å kunne gjenskape data og å gjennomføre revisjoner. Dette skal oppfylle de til enhver tid gjeldende krav i lov (personopplysningsloven), forskrift og interne retningslinjer.

Ansvarsforhold og roller

Behandling av personopplysninger i Conexus er et linjeansvar.

I samsvar med personopplysningsloven er administrerende direktør i Conexus AS ansvarlig for bruk og behandling av personopplysninger ved Conexus AS.

Sikkerhetsansvarlig

Operative behandlingsoppgaver

Administrerende direktør har delegert operative behandlingsoppgaver for personopplysninger til informasjonssikkerhetssjef i Conexus.

Operative behandlingsoppgaver er blant annet etablering og oppfølgning av rutiner, sikringstiltak, avviksbehandling og opplæring av medarbeiderne innenfor sin organisatoriske enhet.

conexus

Strategi for arbeidet med personopplysninger

Kvalitetssystem

For å nå målet beskrevet ovenfor har Conexus AS et eget kvalitetssystem som sikrer konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Det er etablert system for internkontroll som skal sikre at sikkerhetsmålene ivaretas.

Prioriteringer

Ved behandling av personopplysninger i virksomhetssammenheng skal hensynet til konfidensialitet prioriteres fremfor krav til tilgjengelighet. Dette skal presiseres klart for alle med operativt behandlingsansvar. Conexus AS skal likevel etterstrebe løsninger som sikrer at tjenestene er tilgjengelig ved behov.

Hensyn til konfidensialitet skal tillegges avgjørende vekt ved valg av teknologiske løsninger. Dersom det skal behandles sensitive personopplysninger i datanettverk/over internettet skal det etableres nødvendig sikkerhets tiltak (blant annet kryptering/anonymisering).

Personopplysninger som oppbevares og dokumenteres i fysisk arkiv eller på den enkeltes arbeidsplass skal sikres mot innsyn.

Risikovurdering

Conexus AS skal til enhver tid ivareta oppdatert oversikt over hvilke personopplysninger som behandles.

Sikringstiltak skal vurderes opp mot personopplysningenes karakter og dokumenteres i en konsekvensanalyse.

Den behandlingsansvarlige skal sørge for at det blir gjort en risikovurdering med sikte på å kartlegge mulige farer for brudd på sikkerheten, og fastsette nivå for akseptabel risiko for

- Konfidensialitet
- Integritet
- Tilgjengelighet

Conexus AS har fastsatt følgende generelt nivå for akseptabel risiko:

- Det aksepteres ikke at uvedkommende får innsyn i person- og helseopplysninger
- Det aksepteres ikke at registrerte personopplysninger går tapt
- Det aksepteres ikke at registrerte personopplysninger endres uten at gjeldende interne prosedyrer er fulgt
- Det aksepteres ikke at personopplysninger er ufullstendige eller gir et misvisende inntrykk i forhold til behandlingen av opplysningene
- Tilgjengelighet skal normalt prioriteres etter hensyn til konfidensialitet og integritet.

Gjennomføring

Fastlagt nivå for akseptabel risiko skal benyttes til å avgjøre om avdekket risiko er innenfor et akseptabelt nivå.
Dersom det skjer endringer som kan påvirke risikoen, skal det gjennomføres ny risikovurdering.

Sikkerhetsrevisjon

Kontroll med bruk av sikkerhetssystemet skal gjennomføres jevnlig. Resultatet av revisjonen skal dokumenteres.

Sikringstiltak

Det skal gjennomføres tiltak mot innbrudd, strømbrudd, svikt i maskinvare/programvare og ødeleggende programvare slik at uautorisert adgang til utstyr og data hindres.

Det skal også gjennomføres tiltak som hindrer uautorisert innsyn, for eksempel i form av kryptering, og tiltak som sikrer tilgang til personopplysninger der tilgjengelighet er nødvendig, for eksempel i form av reservekopi.

Avvik

Med avvik menes ethvert brudd på Conexus AS' policy og rutiner for behandling av personopplysning og informasjonssikkerhet.

Den enkelte ansatte som oppdager avvik fra sikkerhetsrutinene er pliktig å melde fra til nærmeste overordnede/operativt behandlingsansvarlige som skal behandle avviket.

Ved avvik fra fastsatt nivå for akseptabel risiko skal behandlingsansvarlig sørge for at det iverksettes tiltak for å bringe sikkerheten innenfor akseptabelt nivå.

Personvernombud

Conexus AS skal ha personvernombud.

Forholdet til andre parter

Samarbeidspartnere, underleverandører etc.

Der Conexus samarbeider med andre parter, skal virksomheten avklare ansvarsforhold rundt behandling av personopplysninger og sikre tilfredsstillende informasjonssikkerhet.

conexus

Vedlegg D – Conexus Sikkerhets Organisasjon

Sikkerhetsorganisasjon i Conexus

Innledning

Conexus sin sikkerhetsorganisasjon består av forskjellig roller beskrevet nedenfor. Sikkerhetsorganisasjonen skal sikre at Conexus ivaretar sikkerheten til informasjon, personopplysninger eller sensitive personopplysninger i all administrasjon av, behandling av og tilgang til slike opplysninger.

Oppdraget til rollene baserer seg på norsk lovgivning, og Conexus sin egen interesse i å ivareta Conexus sin virksomhet, våre verdier, vårt omdømme og våre forpliktelser i samsvar med personvernlovgivning, kontrakter og lignende.

Begrepet «sikkerhetsansvarlig» kan brukes om følgende roller/enkeltpersoner.

«To-person-konseptet» henviser til at ingen enkel person kan få tilgang eller innsyn til data på egenhånd og at bare en kombinasjon av minst to av følgende roller/enkeltpersoner sammen har tilgang eller innsyn.

Rolle	Rollebeskrivelse/ansvarsområder	Enkeltperson
Informasjonssikkerhetssjef (CISO)	Er en av tre sikkerhetsansvarlige hos Conexus. Identifisere, utvikle, implementere og vedlikeholde sikkerhetsrelaterte prosesser som reduserer organisasjonens driftsrisiko. Utarbeide og implementere sikkerhetsrelaterte retningslinjer. Kontrollere overholdelse av regelverk. Ivareta personvern. Lede bedriftens responsteam ved datasikkerhetsrelaterte hendelser. Tilsynsansvarlig, og tilgangsstyring. Utarbeide og kontrollere organisasjonens sikkerhetsarkitektur. Gjennomføre elektroniske oppdagelser og digital etterforskning.	Thomas Haslestad

conexus

Rolle	Rollebeskrivelse/ansvarsområder	Enkeltperson
	Utarbeide katastrofegjenoppretting (DR) og kontinuitetsplaner for virksomheten. Være sikkerhetsansvarlig for driften ved behov.	
Arkitekt for informasjonssikkerhet (ISA)	Arkitekt for informasjonssikkerhet har følgende hovedansvar: • Arkitekt for sikkerhetsstrategi for applikasjoner • Arkitekt for sikkerhetsstrategi for skybasert nettplattform • Arbeider sammen med utviklings- og driftsgrupper for å implementere sikkerhetsstrategier • Arbeider sammen med utviklings- og driftsgrupper i forbindelse med taktiske sikkerhetsløsninger ved behov • Gir veiledning som sikkerhetskonsulent ved implementering av ny teknologi • Har ansvaret for sikkerhetskontroller som utføres av tredjepart • Gjennomfører risikoanalyser for å avdekke potensielle sikkerhetsproblemer • Sporer sikkerhetsresultater og fremdrift ved feilretting • Skal holde seg oppdatert på den nyeste utviklingen innen både sikkerhet og hacking Bestemmer sikkerhetskrav ved å evaluere forretningsstrategier og krav, kontrollerer standarder for informasjonssikkerhet, gjennomfører analyser og risikovurderinger av systemsikkerhet og sårbarhet, studerer arkitektur/plattform, identifiserer integrasjonsproblemer og utarbeider kostnadsoverslag. Planlegger sikkerhetssystemer ved å evaluere nettverk og sikkerhetsteknologier, utvikler krav for lokalnett (LAN), WAN, virtuelle private nettverk (VPN), rutere, brannmurer og relaterte sikkerhets- og nettverksenheter,	Morten Udnæs

Rolle	Rollebeskrivelse/ansvarsområder	Enkeltperson
	designer offentlige nøkkelinfrastrukturer (PKI), inkludert bruk av sertifiseringsinstanser (CA) og digitale signaturer, samt maskinvare og programvare samt sikre at bransjestandarder følges. Implementerer sikkerhetssystemer ved å spesifisere metodologi og utstyr for deteksjon av innbrudd, bestemmer installasjon og kalibrering av utstyr og programvare, utarbeider preventive og reaktive tiltak, lager, overfører og vedlikeholder nøkler, gir teknisk brukerstøtte og kompletterer dokumentasjon. Kontrollerer sikkerhetssystemer ved å utvikle og implementere testskript. Opprettholder sikkerheten ved å overvåke og sikre at standarder, retningslinjer og prosedyrer følges, gjennomfører analyser ved hendelsesrespons, og utvikler og gjennomfører treningsprogrammer. Oppgraderer sikkerhetssystemer ved å overvåke sikkerhetsmiljø, identifisere sikkerhetshull og evaluere og implementere forbedringer. Utarbeider rapporter for systemsikkerhet ved å samle inn, analysere og oppsummere data og trender. Oppdaterer arbeidskunnskap ved å spore og forstå nye praksiser og standarder for sikkerhet, deltar på kurs, leser bransjelitteratur, vedlikeholder personlige nettverk og deltar i profesjonelle organisasjoner. Forbedrer avdelingens og organisasjonens omdømme ved å ta eierskap til nye og forskjellige forespørsler, og utforsker muligheter for å tilføre verdi til arbeidsprestasjoner.	

Rolle	Rollebeskrivelse/ansvarsområder	Enkeltperson
	Være sikkerhetsansvarlig for driften ved behov.	
Informasjonssikkerhetsansvarlig	<u>Vurdering</u> Informasjonssikkerhetsansvarlige vurderer organisasjonens sikkerhetstiltak, for eksempel brannmurer, antivirusprogramvare og passord, for å identifisere svake punkter som kan føre til at informasjonssystemer blir sårbare for angrep. De kan utføre simulerte angrep for å teste sikkerhetstiltakenes effektivitet. De prioriterer også sikkerhetsdekningen for å sikre at strategisk viktige data, som kommersiell informasjon eller personopplysninger, har best mulig sikkerhetsnivå. <u>Retningslinjer</u> For å minimere risikoer utarbeider disse lederne retningslinjer som skal oppmuntre til sikre arbeidsrutiner og beskytte data. De gir medarbeidere og ledere ulik tilgang til bedriftens data basert på ansiennitet og arbeidsoppgaver. De gir også de ansatte opplæring, forklarer sikkerhetsrisikoer og demonstrerer mønsterpraksis, for eksempel bruk av sterke passord og å beskytte data når de bruker mobile enheter utenfor kontoret. <u>Overvåking</u> Ledere utarbeider prosedyrer og automatiserte prosesser for å overvåke status for datamaskiner og nettverk. Hvis overvåkingssystemet avdekker unormale adferdsmønstre, skal lederne raskt respondere for å finne årsaken og eliminere eventuelle trusler.	

Rolle	Rollebeskrivelse/ansvarsområder	Enkeltperson
	De analyserer også rapporter som genereres av overvåkingssystemet for å identifisere trender som kan indikere en fremtidig risiko. De leder utvikling, dokumentasjon og vedlikehold av retningslinjene for informasjonssikkerhet, prosedyrer og standarder på tvers av avdelinger. Oppfyller målene for drift av systemsikkerheten ved å bidra med informasjon og anbefalinger til strategiske planer og evalueringer, utarbeider og fullfører handlingsplaner, implementerer standarder for produksjon, produktivitet, kvalitet og kundeservice, gjennomfører ettersyn, identifiserer trender, bestemmer forbedringer av systemer og implementerer endringer. Oppfyller de økonomiske kravene til systemsikkerhet ved hjelp av prognoser, utarbeider et årlig budsjett, planlegger utgifter, analyserer avvik og tar initiativ til korrigerende tiltak. Beskytter datamaskinaktiva ved å utarbeide sikkerhetsstrategier, leder utvikling av systemkontroll og tilgangsadministrasjon, overvåking, kontroll og evaluering. Utarbeider systembeskyttelse ved å lede utvikling av katastrofeberedskap, gjennomfører beredskapstester. Utvikler bevissthet for sikkerhet ved å lede utvikling av orienteringer og opplæringsprogrammer, rådgir klienter. Rådgir seniorledelse ved å identifisere kritiske sikkerhetsproblemer, anbefaler løsninger for å redusere risikoer. Tar initiativ til, tilrettelegger for og fremmer aktiviteter for å skape bevissthet	

Rolle	Rollebeskrivelse/ansvarsområder	Enkeltperson
	om sikkerhet i organisasjonen. Overvåker og evaluerer rutinemessig alle prosedyrer og retningslinjer for informasjonssikkerhet, og sikrer enhetlig interne kontroller på tvers av avdelinger. Leder utarbeidelse og vedlikehold av planer for katastrofegjenoppretting av informasjonssystemer og kontinuitet for virksomheten. Skal inkludere utrulling og vedlikehold av systemer for sikkerhetskopiering av arbeidsstasjoner og server. Følger med på endringer i lokale, regionale og nasjonale forskrifter, samt akkrediteringsstandarder som påvirker informasjonssikkerhet, og gir anbefalinger til CIO og andre ledere om behov for endringer av retningslinjer. Gir oversikt og tar eierskap til innbruddsdeteksjon og respons. Utarbeider og vedlikeholder alle sikkerhetssertifiseringstiltak for informasjonssystem og programvare. Skal inkludere oversikt over etterlevelse av PCI. Bistår i system- og programvarearkitektur og -design for å sikre tilstrekkelig sikkerhetsnivå for verdiene.	

Vedlegg E – Forespørsel om innsyn, informasjon og sletting

Prosessbeskrivelse for forespørsel om innsyn, sletting eller uthenting av informasjon

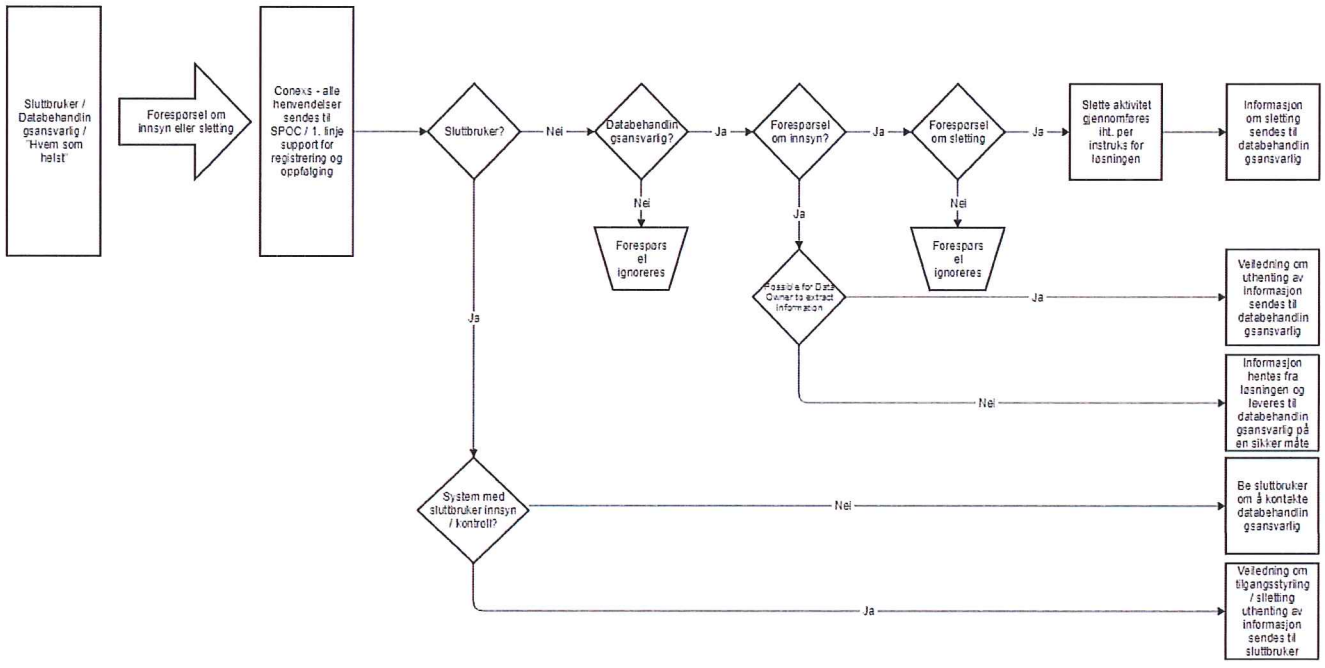
Innledning

Som databehandler for både databehandlingsansvarlige og sluttbrukere kan Conexus motta forespørsler om innsyn, sletting og uthenting av informasjon som har blitt lagret om et individ.

Conexus har for tiden 2 typer løsninger hvor personlig identifiserbar data lagres. Den ene type løsning tilbyr sluttbrukeren fult innsyn og kontroll over hvilke data som er lagret og delt med hvem. I den andre type løsning administrerer kundens brukeradministratorer dette.

Når Conexus mottar forespørsler om innsyn, sletting eller uthenting av informasjon følger Conexus prosessen beskrevet nedenfor.

Flytdiagramm



conexus

Vedlegg F – Prosedyrer for behandling av personopplysninger og sensitive personopplysninger

Prosedyrer og rutiner for behandling (administrasjon) av personopplysninger og sensitive personopplysninger

Innledning

Å ivareta personopplysninger eller sensitive personopplysninger er en hjørnestein i all administrasjon av, behandling av og tilgang til slike opplysninger. Man må vær ekstremt oppmerksom i slike situasjoner.

Det er pålagt av norsk lovgivning, og det er også i Conexus' interesse å ivareta vår virksomhet, våre verdier, vårt omdømme og våre forpliktelser i samsvar med personvernlovgivning, kontrakter og lignende. Instruksjonene nedenfor skal følges for å unngå datalekkasje og datatap. Datalekkasje eller tap skal håndteres i samsvar med disse instruksjonene og norsk lovgivning.

Systemene våre inneholder vanligvis tre typer informasjon, som beskrevet i sikkerhetsklassifiseringen nedenfor.

Sikkerhetsklassifiseringer

Informasjonskategorier er basert på tiltenkt bruk og forventede konsekvenser hvis de offentliggjøres. Dataklassifiseringer er definert av lovverket, men behandlingsansvarlig kan bruke høyere klassifisering enn det lovverket krever. Klassifiseringen av data kan endres ved at de kombineres med andre data, slik at hele datasettet enders til enten *personopplysninger* eller *sensitive personopplysninger.* Hvis du ikke kan finne ut hvilken sikkerhetsklassifisering som er riktig for dataene du behandler, skal du alltid anta at de hører hjemme i kategorien *sensitive personopplysninger.*

- Offentlig
  Informasjon som er tiltenkt offentlig bruk. Når den brukes slik den er tiltenkt, vil den ha få eller ingen konsekvenser for den registrerte, for Conexus' virksomhet, verdier og omdømme og for våre forpliktelser i samsvar med personvernlovgivning, kontrakter og lignende. Informasjon som vanligvis kan finnes på internett.

- Personopplysninger
  Personopplysninger defineres som alle opplysninger som kan brukes til å identifisere enkeltpersoner, for eksempel navn, personnummer, dato og fødested, morens pikenavn og biometriske opplysninger som er koblet til, eller som kan kobles til en enkeltperson, for eksempel opplysninger om helsetilstand, utdanning, økonomi og arbeidsforhold.

- Sensitive personopplysninger
  Sensitive personopplysninger defineres som informasjon som kan brukes til å identifisere enkeltpersoner, for eksempel navn, personnummer, dato og fødested, morens pikenavn eller biometriske opplysninger, samt all annen informasjon som er knyttet, eller som kan knyttes til en enkeltperson og som inneholder informasjon om personens rase eller etnisitet, politiske

meninger, filosofisk eller religiøs overbevisning, om personen har vært mistenkt for, siktet for eller dømt for kriminalitet, personens helse, seksualliv eller fagforeningsmedlemskap.

Behandle og administrere sensitive opplysninger

Opprettelse og vedlikehold

Det opprettes registre i forbindelse med levering av systemer og tjenester til kundene våre. Disse registrene dokumenterer kundenes beslutninger og aktiviteter, samt deres prosesser. Det er viktig at de kun opprettes og vedlikeholdes på riktig måte gjennom hele livssyklusen. Datamanipulering for andre formål eller på andre måter enn med de forhåndsdefinerte verktøyene og mekanismene, er strengt forbudt.

Sensitiv informasjon i systemene våre er et kritisk område. Hvis registre brukes på feil måte, uvedkommende får tilgang til informasjonen eller hvis informasjonen blir utlevert, utgjør det en stor risiko for kundene våre og for Conexus' juridiske forpliktelser, drift, verdier og omdømme. Derfor skal registre med sensitiv informasjon kun finnes når det finnes et berettiget behov for det i virksomheten.

Levetiden for sensitive personopplysninger skal styres med rutiner for lagringstid (som utarbeides i samarbeid med kunder) og i samsvar med norsk lovgivning. Rutiner for lagringstid skal dokumentere at slike opplysninger finnes, begrunnelsen for at vi har lagret dem og de skal bidra til å sikre at de er tilgjengelige i den perioden de er viktige enten i forbindelse med administrasjon eller som historiske registre. Rutiner for lagringstid skal også sikre riktig sletting av ikke-permanente og inaktive opplysninger. På den måten reduseres risikoen for utlevering av informasjon som ikke lenger har en administrativ eller historisk funksjon.

Tilgang

Både personopplysninger og sensitive personopplysninger krever streng kontroll og veldig begrenset tilgang og utlevering. De kan også være underlagt lovmessige begrensninger. I enkelte tilfeller er opplysningene sensitive fordi de har blitt samlet i ett register eller dokument.

Tilgang til sensitive opplysninger gis kun til Conexus-medarbeidere eller medarbeidere hos databehandler som har fått godkjenning fra behandlingsansvarlig og som har signert en taushetserklæring.

All annen utlevering av sensitive opplysninger krever skriftlig godkjenning fra behandlingsansvarlig og sikkerhetsansvarlig hos Conexus, som innhenter tillatelse fra juridisk direktør ved behov.

- Medarbeidere skal ikke hente sensitive opplysninger fra systemer, databaser eller lignende med mindre det er nødvendig for at de skal kunne utføre arbeidsoppgavene sine.
- Når det gis tilgang til sensitive personopplysninger, skal bruken av slike opplysninger begrenses til formålet som er nødvendig for å kunne utføre de definerte arbeidsoppgavene.
- Personer som har tilgang til personopplysninger / sensitive personopplysninger, skal respektere den registrertes konfidensialitet og personvern, følge etiske retningslinjer som gjelder for opplysningene de får tilgang til, samt følge gjeldende lovverk og retningslinjer for tilgang, bruk og utlevering av informasjon.
- Ledelsen hos Conexus eller relevant databehandler skal umiddelbart varsles om terminering av bruker eller fjerning av tilgang til sensitive opplysninger.

- Det skal finnes en oppdatert oversikt over alle som har tilgang til sensitive personopplysninger, databaser og systemer.

Bruk og sletting

Følgende kontroller er **påkrevd** når man bruker eller sletter sensitive opplysninger:

- Ikke diskuter eller vis sensitive personopplysninger i et miljø hvor uvedkommende kan se eller overhøre dem.
- Sørg for at tilgangsnøkler, brukernavn og passord ikke havner hos uvedkommende.
- Du må ikke lagre brukernavn, passord eller kopier av opplysninger på steder, i systemer eller som filer som uvedkommende kan få tilgang til.
- Du må ikke skrive dem ut, ta bilde av dem, kopiere dem eller sende dem med telefaks.
- Sørg for at alle fysiske kopier (utskrifter, skjermdumper og lignende) ikke er tilgjengelige for uvedkommende.
- Du må ikke oppbevare fysiske eller digitale kopier (utskrifter, skjermdumper eller filer) på fysiske eller logiske steder som ikke er trygge og som ikke har blitt godkjent av sikkerhetsansvarlig hos Conexus.
- Slik informasjon skal merkes som sensitiv slik at alle som har tilgang til den, er klar over det. Merk den med «Sensitiv», og sørg for at alle medarbeidere som får tilgang til, eller som behandler opplysningene, har fått opplæring. Det skal finnes tydelige instruksjoner og rutiner for hvordan opplysningene skal behandles.
- Alle sensitive opplysninger som lagres i elektroniske systemer, skal krypteres til det nivået som er definert av behandlingsansvarlig eller sikkerhetsansvarlig hos Conexus.
- Alle krypteringsnøkler skal lagres og brukes basert på «to-person»-konseptet.
- Bruk en kjent og dokumentert livssyklus for programvareutvikling når det skal lages programvare som har tilgang til sensitive opplysninger.
- Alle ledere har ansvar for at medarbeidere får opplæring i formålet for disse retningslinjene og hvordan de skal bruke og slette personopplysninger.
- Sletting av fysiske eller elektroniske registre (databaser, inkludert sikkerhetskopier, fysiske kopier, datasystemer og lagringsenheter) skal automatisk registreres eller bevitnes basert på «to-person»-konseptet.
- Fysisk destruksjon av elektroniske personopplysninger eller ved hjelp av metoder for sletting som er godkjent av Nasjonal sikkerhetsmyndighet. Formatering av en harddisk er ikke tilstrekkelig for å fjerne alle data på en sikker måte.
- Sensitiv informasjon i papirform skal makuleres (vi anbefaler krysskutting) eller omdannes til cellulose. Dette inkluderer alle midlertidige arbeidsverktøy (for eksempel ubrukte kopier, utkast og notater).
- Sørg for at gamle datamaskiner og elektroniske medier (alt som kan lagre data, for eksempel CD-er, DVD-er, USB-minnepinner, disketter, iPoder og lignende) avhendes på riktig måte slik at de ikke inneholder opplysninger. Dette kan innebære fysisk ødeleggelse av datamaskinens harddisk (eller elektroniske medier). Det kan også innebære elektroniske tiltak som sletting av harddisken ved hjelp av en metode som er godkjent av Nasjonal sikkerhetsmyndighet.

Overføring og transport

Følgende kontroller **kreves** når du skal overføre eller transportere sensitive personopplysninger:

- Når du sender sensitive personopplysninger i posten (inkludert via postvesen i inn- og utland, DHL, UPS, FedEx og lignende), skal avsenderen bruke sikre og sertifiserte tjenester med sporing og signatur. Det skal også brukes forseglet emballasje som ikke kan åpnes uten at det

etterlater spor.
Behovet for, eller kravet til kryptering av de sensitive opplysningene gjelder fortsatt.

- Personopplysninger skal ikke lagres på flyttbare medier (for eksempel bærbare PC-er, PDA-er og smarttelefoner). Slike opplysninger skal heller ikke overføres elektronisk med mindre sikkerhetsansvarlig hos Conexus har godkjent det.

- Hvis personopplysninger skal overføres digitalt mellom det opprinnelige og sikre lagringsstedet og andre elektroniske systemer, skal overføringen gjøres via trygge og krypterte (minimum standard AES256) kanaler.
- Det er forbudt å bruke e-post (også internt i Conexus), direktemeldinger, chat og usikret filoverføring (for eksempel FTP) med mindre opplysningene minimum er kryptert til AES256.

- Sensitive opplysninger skal ikke fjernes fra et godkjent og sikkert lagringssted med mindre det foreligger tillatelse fra behandlingsansvarlig eller sikkerhetsansvarlig hos Conexus.
- Hvis en medarbeider eller en stilling krever at sensitive opplysninger fjernes fra det sikre lagringsstedet, skal opplysningene (uansett om de er i elektronisk eller fysisk form) beskyttes mot utilsiktet utlevering. Det skal finnes rutiner for å beskytte personopplysningene når de ikke er lagret på sitt opprinnelige og sikre sted. Når det ikke lenger er behov for å ha opplysningene utenfor det opprinnelige og sikre stedet, skal de destrueres i samsvar med instruksjonene som ble beskrevet tidligere.

- Eventuelle sikkerhetskopier av personopplysningene (på bånd, disketter, nettbasert sikkerhetskopi og lignende) skal krypteres på godkjent måte før de overføres. Når det er mulig, skal man bruke andre former for overføring enn post, for eksempel sikret og kryptert nettbasert overføring.
  Slike overføringer som bruker passord for å kryptere eller dekryptere data, skal ha sin egen unike identifikator eller et unikt passord.

Brudd på sikkerheten og datalekkasje

Hvis det oppstår brudd på noen av disse rutinene, skal prosessen for styring av sikkerhetshendelser aktiveres, og vi må anta at det har oppstått en lekkasje av sensitive personopplysninger. (Datalekkasje: Uautorisert overføring av gradert informasjon fra et datasystem eller et datasenter til uvedkommende. Datalekkasje kan oppstå ved at man husker ting man har sett, ved at man fysisk fjerner bånd, disketter og rapporter eller på mer subtile måter, ved for eksempel å skjule data).

Vurderinger/analyser

Hvis det oppstår mistanke om en mulig datalekkasje, må man først vurdere om lekkasjen er reell, hvor store konsekvenser det kan få, hvilke brukere som er involvert, finne tidslinjen (dato og klokkeslett for bruddet, og dato og klokkeslett for når det ble avdekket), samt hvilke systemer og applikasjoner som er involvert.

Det gjennomføres en analyse for å avdekke de tekniske detaljene, den grunnleggende årsaken, systemiske problemer og potensielle konsekvenser som følge av en sikkerhetshendelse.

All relevant informasjon skal samles (for eksempel tidligere innhentede data, hendelseslogger, revisjonsspor og informasjon fra alle kilder).

Koordiner med andre organisasjoner for å samle inn ytterligere informasjon.

Gjennomfør analyser for å finne ut om hendelsen har skjedd, identifiser leveringsvektorer og svakheter i system, og finn rotårsaken og potensielle konsekvenser.

Rapportering

Den mistenkte hendelsen skal umiddelbart rapporteres til behandlingsansvarlig (sikkerhetsansvarlig hos Conexus). Den nevnte informasjonen skal inkluderes i rapporten.

Rapporten skal inneholde en detaljert beskrivelse av problemets natur, hvilken informasjon som (potensielt) har gått tapt og hva som gjøres for å løse problemene og minimere skadeomfanget. I tillegg skal det henvises til en kontaktperson, og det skal informeres om hvilke tiltak de involverte partene kan iverksette for å begrense tapet.

Bruk et system for å registrere sikkerhetshendelser og for å sikre informasjon om hendelsen.

Gi oppdateringer hvis statusen for hendelsen endres.

Isolere

Isoler og begrens for å minimere skadeomfanget og sikre bevis som kan være nødvendige for å vurdere skadeomfang og risiko, for rettshåndhevelse eller i forbindelse med kontraspionasje. Identifiser all maskinvare, alle programvaresystemer og alle applikasjoner som ble påvirket, og følg godkjente rutiner for å sikre at lekket data ikke kan spres videre. Berørte medier/enheter blir klassifisert som kompromitterte til responsteamet har vurdert situasjonen og iverksatt nødvendige tiltak. Hvis klassifisert informasjon havner i pressen, skal det ikke gis noen uttalelse som bekrefter informasjonens nøyaktighet eller status. Du skal heller ikke diskutere saken med noen med mindre de har tilstrekkelig sikkerhetsklarering og har behov for informasjon om hendelsen. Hvis bruddet og skadeomfanget bekreftes, kan det føre til en nedgradering av klassifiseringen for alle eller deler av dataene.

Begrens

Undersøk og identifiser tiltak som skal iverksettes som følge av hendelsen.

conexus

Vedlegg G – Underleverandører, data lagring og tilgang til produksjonsdata

Underleverandører, lagringslokasjoner og tilgang til produksjonsdata

Innledning

Conexus bruker for tiden underleverandørene som er beskrevet under iht. personvernlovgivning og databehandleravtalen dette vedlegget er del av.

Informasjonen som behandles lagres i de fysiske lokasjonene beskrevet under og vil ikke overføres til land utenfor EØS uten skriftlig godkjenning fra Behandlingsansvarlig.

Ved inngåelse av avtale om slik overføring skal Databehandler inngå "EUs Model Contract Clauses" med Behandlingsansvarlig som eksportør, og overføringene være i henhold til disse bestemmelsene.

Definisjoner:

«Produksjonsdata» er data/informasjon som er produsert eller samlet inn gjennom registrering / innsamling av reelle data til eksisterende individer / personer.

Leverandører / Underleverandører

Navn	Org. nr.	Adresse	Rolle	Kontakt informasjon
Conexus AS	995 807 564	Grønland 67, 3045 Drammen Norge	Kundestøtte, Produkt management, Produktutvikling	support@conexus.no
Basefarm AS	982 211 743	Nydalen Allé 37A 0484 Oslo Norway	Fysisk hosting, basis drift av servere og infrastruktur for produksjons- og kvalitetssikringsmiljøer	post@basefarm.no
SSC Networks Norge AS	985 549 567	Hofgaards gate 22 3011 DRAMMEN	Fysisk hosting, basis drift av servere og infrastruktur for produksjons- og kvalitetssikringsmiljøer	salg@ssc.no

Navn	Org. nr.	Adresse	Rolle	Kontakt informasjon
BAIP	301318539	Gynėjų st. 14, 01109 Vilnius Lithuania	24/7 monitorering, drift og avvikshåndtering	info@baip.lt

Fysiske lagringssteder som brukes for produksjonsdata

Land / sted	Hensikt	Miljø
Norway - Basefarm	Produksjon, kvalitetssikring og sikkerhetskopi	Produksjonsmiljø, Kvalitetssikringsmiljø og sikkerhetskopi
Norway - Conexus	Funksjonell verifikasjon	Kvalitetssikringsmiljø

Tilgang til produksjonsdata

Tilgang til produksjonsdata er til enhver tid begrenset til autoriserte roller og personale hos Conexus og / eller underleverandører.

Dokumentasjon om roller og autorisert personale vedlikeholdes fortløpende av Conexus og kan fremlegges på forespørsel.