Alinea

ENISA sikkerhedsforanstaltninger

Lindhardt og Ringhof (L&R) har et mål om organisatoriske og tekniske foranstaltninger der svarer til den samlede risikovurdering på *Medium* i forhold til ENISA metoden.

Følgende sikkerhedsforanstaltninger afviger fra målet, og der er iværksat nedenstående handlinger og specielle procedurer.

Målkategori	ID	ENISA Målbeskrivelse	Status og mitigerende handling
Logning og overvågning	L.1	Logfiler skal aktiveres for hvert system / applikation, der bruges til behandling af personoplysninger. De bør omfatte alle typer adgang til data (visning, ændring, sletning).	Dette er kun delvist på plads i L&Rs ældre læremidler med persondata. Dette omfatter Stavevejen og Mitformat. Begge produkter har planlagt EOL (End-of-live) i 2024.

	Logning og overvågning	L.2	Logfiler skal være tidsstemplet og tilstrækkeligt beskyttet mod manipulation og uautoriseret adgang. Ure skal synkroniseres med en simpel referencetid

Dette er ikke på plads i L&Rs ældre læremidler med persondata. Dette omfatter Stavevejen og Mitformat. Begge produkter har planlagt EOL (End-of-live) i 2024.

Data og retention perioder i læremidler

Følgende læremidler er omfattet af databehandleraftalen med tilhørende data og retention perioder.

Digitale læremidler	Persondata	Data retention
Licenssystem og Single-Sign-On Håndtering af brugere og adgange.	STILs lille datapakke: Navn, Klasse, Institution, Email, Type (Lærer, Elev)...	Data slettes efter max 6 mdr. når bruger ikke længere kommer fra STIL
Alinea Portaler Alle Alineas portaler til alle klassetrin/fag med en række forskellige undervisningsforløb.	Data er pseudonymiseret. Kun et internt brugerID gemmes i databasen. Elev input data: Validerbare og ikke-validerbare opgave-besvarelser.	Når bruger ikke længere sendes fra STIL slettes brugerID og data anonymiseres.
Onlineprøver Alle Alineas onlineprøver til at teste elevernes færdigheder i lytning, læsning, sprog og sprogbrug og skriftlig fremstilling.	Data er pseudonymiseret. Kun et internt brugerID gemmes i databasen. Elev input data: Validerbare opgavebesvarelser.	Når bruger ikke længere sendes fra STIL slettes brugerID og data anonymiseres.

Alinea

Camp-produkter Alineas træningsprodukter til dansk, matematik og sprog. Herunder CampMat, CampEngelsk og CampStavning.	Data er pseudonymiseret. Kun et internt brugerID gemmes i databasen. Elev input data: Validerbare opgavebesvarelser.	Når bruger ikke længere sendes fra STIL slettes brugerID og data anonymiseres.
Træning: "Den første læsning" App med simple spil for indskoling.	Trin 0: Data er pseudonymiseret. Kun et bruger ID gemmes i databasen. Trin 1+2: Navn, Klasse, Institution	Trin 0: Som ved "Portaler" Trin 1+2: Data på inaktive elever slettes årligt.
Træning: Matematikfessor Matematiktræning til alle klassetrin	STILs lille datapakke: Unilogin ID, Navn, Klasse, Institution, Email, Type (Lærer, Elev). Elev input data: Validerbare og ikke-validerbare opgavebesvarelser.	Data anonymiseres én gang årligt på de brugere som ikke længere har adgang.
Træning: Diverse med EOL (end-of-life) planlagt Stavevejen og Mitformat.dk	STILs lille datapakke: Unilogin ID, Navn, klasse og institution. Elev input data: Validerbare og ikke-validerbare opgavebesvarelser.	Data slettes efter max 6 mdr. når bruger ikke har adgang længere.
Ressource sites til grundsystemer Diverse websites til grundsystemer ("Har du bog, har du web!") med diverse digitale ressourcer, fx format.alinea.dk, PraktiskSprog m.fl.	Data er pseudonymiseret. Kun et internt brugerID gemmes i databasen. Elev input data: Validerbare og ikke-validerbare opgavebesvarelser.	Når bruger ikke længere sendes fra STIL slettes brugerID og data anonymiseres.
Clio.me portaler Alle Clio portaler til alle klassetrin/fag med en række forskellige undervisningsforløb.	STILs lille pakke, som består af følgende: Fornavn, efternavn, elevrolle (barn, elev, studerende), studienummer, elevens niveau (for grundskoleelever), elevens hovedgruppe (klasse),	Når bruger ikke længere sendes fra STIL slettes brugerID og data anonymiseres.

Alinea

yderligere grupper eleven/læreren (herunder pædagoger og andre, der har en undervisningsfunktion samt administrativt personale) er tilknyttet, afdeling, bygning eller værelsesnummer på efterskole, elevens ID i det lokale studieadministrative system, ansættelsesroller (fx lærer, pædagog, leder,...), Medarbejderens initialer og stilling, UNI-login brugernavn (bruger-ID) gruppeID, gruppenavn, gruppetype, niveau, spor, startdato og slutdato.

Ved brugen af de digitale læremidler behandles desuden følgende personoplysninger af databehandleren: Clio login, Clio bruger ID, IP-adresse, forbrugsdata, brugernes anvendel-se af databehandlerens digitale læremidler, herunder besvarelse af opgaver, bedømmelse af opgaver og egen-evaluering af opgaveløsning.

Underdatabehandlere

Følgende underdatabehandlere er omfattet af databehandleraftalen med tilhørende risikovurdering og databeskyttelse.

Underdatabehandler	Databehandling og persondata	Datalokation og beskyttelse
Sentia A/S CVR: 10008123 Lyskær 3A, DK-2730 Herlev, Danmark	Hosting af digitale læremidler, herunder vedligehold af servere, backup, sikkerhed mv. Hosting sker i deres hostingcenter i Danmark.	Sentia hostingcenter i Danmark.

	Persondata: Elever og lærere: Navn, Unilogin brugernavn, email (ved servicepermission), klasse og institution.	
Microsoft (Azure West Europe Region) CVR: 13612870 Microsoft Datacenter Holland, Agriport 601, Middenmeer Netherlands	Hosting af digitale læremidler, herunder vedligehold af servere, backup, sikkerhed mv. Persondata: Elever og lærere: Navn, Unilogin brugernavn, email (ved servicepermission), klasse og institution.	Azure datacenter i EU (Amsterdam, Holland) Data er krypterede fra det øjeblik de bliver afleveret til L&R, når de transmitteres, og når de lagres i L&Rs læremidler/brugerstyring og helt frem til brugerens browser eller app. Nøglerne til krypteringen er, hvor muligt, egne nøgler og kan dermed ikke tilgås af uvedkommende. L&R benytter kun Core Online Services ifbm. persondata, hvilke kontraktuelt forpligter til at data forbliver i EU. Data at rest er placeret i EU og er krypteret med "FIPS 140-2 validated cryptographic module". Data in transit er krypteret ved brug af TLS. Customer Lockbox er aktiveret for at sikre kontrol med hvilke lokationer der kan tilgå data i forbindelse med supportsager. I relation til myndighedsanmodniner er der udarbejdet en risikovurdering som kan udleveres ved forespørgsel.

Egmont IT CVR: 11456111 Vognmagergade 11, 1148 København K	Drift af Lindhardt og Ringhofs løsninger på Microsoft Azure, herunder administration af miljøer, overvågning, brugeradministration mv. Persondata: Elever og lærere: Navn, Unilogin brugernavn, email (ved servicepermission), klasse og institution.	Azure datacenter i EU (Amsterdam, Holland) *Se beskrivelse ved "Microsoft Denmark ApS".*
Dixa ApS CVR: 36561009 Vimmelskaftet 41A, 1 Sal., 1161 Copenhagen S	Sagsstyringssystem til håndtering af kundehenvendelser. Persondata: Brugerens kontaktinformationer ved henvendelse til kundeservice - typisk mail, navn og telefonnummer.	AWS datacenter i EU (Frankfurt, Tyskland) Data er beskyttet med AWS Key Management Service (KMS) og krypteringsnøglen ligger hos Dixa. AWS KMS er designet, så ingen, inklusive AWS-medarbejdere, kan hente nøgler fra tjenesten. Nøgler transmitteres aldrig uden for den AWS-region, hvor de blev oprettet, og kan kun bruges i den region, hvor de blev oprettet.
Sii Sp. z o.o CVR: 140381516 al. Niepodległości 69, 02-626 Warszawa, 3rd floor, Metron building	Udvikling og support af licenssystem. Persondata: Leverandører får i perioder adgang til produktionsdata i forbindelse med vedligehold og fejlsøgning.	Azure datacenter i EU (Amsterdam, Holland) *Se beskrivelse ved "Microsoft Denmark ApS".*

Alinea

Amazon Web Services Inc. CVR: B18628438 Avenue John F. Kennedy L-1855, Luxembourg	Hosting af digitale læremidler på clio.me, herunder vedligehold af servere, backup, sikkerhed mv. Persondata: STILs lille pakke.	Amazon AWS datacenter i Irland. Data er krypterede fra det øjeblik de bliver afleveret i systemet, når de transmitteres, når de lagres i læremidler/brugerstyring og helt frem til brugerens browser eller app. Nøglerne til krypteringen er, hvor muligt, egne nøgler og kan dermed ikke tilgås af uvedkommende. De personoplysninger, der behandles som led i brugernes anvendelse af systemer er ikke krypteret under hostingen hos AWS i det valgte datacenter. Den overførte data bliver placeret i databehandlerens datamiljø, der er sikret og adgangs-kontrolleret via AWS. Databehandleren bruger ligeledes Amazon Virtual Private Cloud (VPS), som sikrer både et offentligt og privat subnet. Dette indebærer, at databehandlerens læringsmoduler opbevares i et isoleret miljø (privat subnet), hvortil brugerne alene kan få adgang via såkaldte gateways. Selve adgangen til produktionsmiljøet er styret via en særlig beskyttet og isoleret proxy server, som er fuldt kontrolleret af databehandleren. Adgang til denne proxy server er beskyttet med symmetrisk kryptering, hvor de private krypteringsnøgler, der er nødvendige for at opnå adgang, opbevares af

Alinea

databehandleren i en yderligere krypteret datafil, udenfor AWS. I relation til myndighedsanmodninger er der udarbejdet en risikovurdering som kan udleveres ved forespørgsel.

Microsoft Azure EU data boundary og håndtering af support-sager

Databehandleren benytter udelukkende Microsoft Azure services, som er indenfor EU data boundary og hvor Microsoft forpligter sig til at opbevare og behandle data indenfor EU.

Databehandleren har, i tilfælde af support, sikret et teknisk set-up, der indebærer, at en medarbejder hos databehandleren aktivt skal give adgang til databehandlerens data, hvis en tekniker fra Microsoft skal have adgang. Dette tekniske system er sikret ved et såkaldt "Customer Lock Box" system. Systemet består i, at hvis Microsofts teknikere ikke kan løse en support-sag uden adgang til databehandlerens indhold, herunder databaser med personoplysninger, kan den pågældende tekniker via Customer Lock Box anmode databehandleren om adgang. Dette giver den eller de personer hos databehandleren, der er tildelt administratorrollen til Customer Lock Box, mulighed for at godkende eller afvise anmodningen og give direkte adgangskontrol til databehandlerens indhold. Hvis den pågældende medarbejder med administratorrettigheder til Customer Lock Box systemet godkender anmodningen, modtager teknikeren fra Microsoft godkendelsesmeddelelsen, logger på databehandlerens database, og løser support-sagen. Microsofts teknikere har den af databehandleren ønskede/valgte varighed til at løse problemet, hvorefter adgangen tilbagekaldes automatisk.

Alle handlinger, der udføres af en Microsoft tekniker i forbindelse med en support[1]sag via Customer Lock Box systemet, logføres i en overvågningslog. Databehandleren kan således til enhver tid søge efter og gennemse disse overvågningsposter, og vil således altid kunne monitorere hvilke adgange der er givet og til hvem i forbindelse med support-sager.

Databehandleren har med implementering af ovennævnte system sikret et system, hvorefter det er databehandleren som egenhændigt styrer, om Microsofts teknikere skal gives adgang til databehandlerens personoplysninger i forbindelse med en supportsag. På denne måde kan databehandleren ligeledes styre, at en given support altid ydes fra en tekniker, der befinder sig indenfor EU.

Det skal nævnes, at det hos databehandleren alene er få medarbejdere, der er tildelt administratorrollen i forbindelse med håndtering af Customer Lock Box systemet, og at der er indført procedurer, der sikrer, at de pågældende medarbejdere er instrueret i korrekt håndtering af systemet. Endvidere fremgår det af procedurerne, at der aldrig må gives adgang til Microsoft teknikere, der befinder sig udenfor for EU. Derudover kan det oplyses, at Microsoft heller ikke til dato af egen drift via Customer Lock Box systemet har anmodet databehandleren om adgang til databaser, der indeholder personoplysninger.

Derudover har databehandleren etableret tekniske foranstaltninger som krypterer databasernes data-at-rest med egen krypteringsnøgle (customer-managed-key) så Microsoft under ingen

omstændigheder vil kunne tilgå data-at-rest i fx databaser.

På baggrund af ovenstående sker der således ikke overførsler af personoplysninger til tredjelande i forbindelse med Microsofts udførelse af cloud service, herunder i forbindelse med supportsager.

Behandlingssikkerhed for digitale læremidler på clio.me

Overførsel af data mellem databehandleren og AWS

Databehandleren krypterer alle personoplysninger, der sendes mellem databehandlerens platform, brugeren og AWS "in transit" for at sikre efterlevelse af de tekniske krav i databeskyttelsesforordningen. Ved transmissionen gøres brug af kryptering TLS, version 1.2.

Hostede data

De personoplysninger, der behandles som led i brugernes anvendelse af www.clio.me er ikke krypteret under hostingen hos AWS i det valgte datacenter i Irland.

Den overførte data bliver placeret i databehandlerens datamiljø, der er sikret og adgangs-kontrolleret via AWS. Databehandleren bruger ligeledes Amazon Virtual Private Cloud (VPS), som sikrer både et offentligt og privat subnet. Dette indebærer, at databehandlerens læringsmoduler opbevares i et isoleret miljø (privat subnet), hvortil brugerne alene kan få adgang via såkaldte gateways. Sidstnævnte sikrer, at det korrekte indhold af læringsmodulerne bliver vist på databehandlerens platform (offentligt subnet), ud fra hvad den pågældende bruger har adgang til.

AWS er kendt for at have et af cloud-markedets højeste sikkerhedsniveauer for databehandling, som uddybes her:

https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

https://aws.amazon.com/compliance/

AWS er ISO 27001-certificeret for informationssikkerhed, og aflægger årligt SOC2-erklæringer, som i lighed med ISAE 3000 erklæringer dokumenterer it-sikkerhed, tilgængelighed, fortrolighed, ægthed og beskyttelse af de registreredes rettigheder.

AWS' support af services og infrastruktur

Ved kritiske driftsfejl og nedbrud kan det i sjældne tilfælde være nødvendigt at undersøge brugerdata direkte i databaserne. Denne adgang er kun mulig for enkelte medarbejdere hos AWS' datacenter i Irland, og kun efter aftale med databehandleren, som tildeler adgangen. Adgangen er altid tidsbegrænset.

Databehandleren har i tilfælde af behov for support sikret et teknisk set-up, der indebærer, at enhver adgang til personoplysninger (også inden for EU/EØS) kræver databehandlerens forudgående godkendelse og tildeling af ad gang. Dette er sikret ved, at adgang er konfigureret via en proxy server som beskrevet ovenfor. Adgang til denne proxy server er beskyttet med symmetrisk kryptering, hvor de private krypteringsnøgler, der er nødvendige for at opnå adgang,

opbevares af databehandleren i en yderligere krypteret datafil, udenfor AWS. Databehandleren har således indført procedurer, der skal sikre, at databehandleren har kontrol med, hvem, der får adgang til personoplysningerne.

Ovenstående indebærer, at der ikke sker overførsler af personoplysninger til tredjelande i forbindelse med AWS' udførelse af cloud service, herunder i forbindelse med supportsager.

For at undgå at en support-henvendelse behandles udenfor EU har databehandleren instrueret AWS om, at support-sager kun må løses af teknikere hos AWS, der befinder sig indenfor EU, uagtet at dette i værste fald kan betyde en længere behandlingstid, idet databehandleren hermed har fravalgt "follow the sun" princippet, hvor support og vedligeholdelse i løbet af et døgn leveres fra forskellige lokationer alt efter, hvor "solen skinner" via en fjernopkobling.

Version 7: 01-09-2023, LRIKTI
Version 6: 13-06-2023, LRIKTI (se tidligere version)
Version 5: 31-10-2022, LRIKTI (se tidligere version)
Version 4: 20-09-2022, LRIKTI (se tidligere version)
Version 3: 14-02-2022, LRITOL (se tidligere version)
Version 2: 16-12-2021, LRITOL (se tidligere version)
Version 1: 01-03-2021, LRITOL (se tidligere version)