Formål

Formålet med at lave en revision af GDPR-compliance

- Beskytte persondata mod tilsigtet eller utilsigtet tilintetgørelse, tab, ændring eller uretmæssig videregivelse
- Dette gøres ved at implementere passende tekniske og organisatoriske foranstaltninger
- For at realisere dette er det nødvendigt med et overblik over hvor og hvordan persondata behandles.

Generelt

Alle kendte arbejdsprocesser er beskrevet og lagt i GDPR portalen, der kan være arbejdsprocesser, der ikke er detaljerede nok. Hjemmel er angivet på de fleste arbejdsprocesser.

I arbejdsprocessen Administration af elever og kursister er hjemlen for behandling af personoplysninger Myndighedsudøvelse og ikke en retslig forpligtelse. Dette bør ændres. Det samme gælder arbejdsprocessen Ansøgninger fra elever og kursister.

I arbejdsprocessen Administration af medarbejdere er brugt hjemlen legitim interesse, den må offentlige myndigheder ikke bruge, der skal i stedet anvendes opfyldelse af en kontrakt.

Fortegnelsen bør gennemgås for at kontrollere om de rigtige hjemler er angivet, og måske en gennemgang af beskrivelserne samt hvor på skolen, der håndteres persondata, kan være en god ide, idet det f.eks. er svært at gennemskue, hvor arbejdsprocesser omkring eksamen er beskrevet.

Der mangler risikovurderinger på enkelte IT-systemer og Datamodtagere.

I alle arbejdsprocesser er angivet hvem data videregives til, og hvor data befinder sig. Der er overensstemmelse mellem arbejdsprocesser og oplysningspligten, den nye oplysningspligt er under opdatering, og der mangler ændringer i forhold til IT-sikkerhed.

Der er ingen arbejdsprocesser, hvor der indgår fælles dataansvars aftaler.

Cookies på hjemmesiden er ændret, så de overholder de nye retningslinjer.

Opdatering af oplysningspligterne og fortegnelsen bør afsluttes snarest.

Oplysningspligt/privatlivspolitik/persondatapolitik

Oplysningspligten er under opdatering, der mangler kun en finpudsning, så er den klar til at blive udgivet.

Oplysningspligten er udformet så den følger de nye retningslinjer, hvor der for hvert formål er angivet hjemmel, samt hvilke data der behandles om de enkelte kategorier af registrerede.

Informationssikkerhed (udpluk fra Datatilsynets tilsynsskema)

Skolen behandler oplysninger om ca. 1.000 aktive registrerede.

Den internt ansvarlige for informationssikkerhed er skolens Økonomi- og administrationschef.

IT-sikkerhedspolitikken er en del af årshjulet, og den revideres en gang om året.

Skolen har ikke udarbejdet en forretningsmæssig risikovurdering.

Adgangskoder skal indeholde store og små bogstaver samt tal, og de skal være på min. 8 karakterer.

To faktor godkendelse indføres inden sommerferien.

Skolen har indført Admin by Request, så medarbejderne skal argumentere for, at de installerer programmer der ikke er godkendt af skolen. Der er også indført Geofencing og tvungen TLS.

Default browser er Edge.

Awarenes

Cyberpilot bruges til awarenes, og det har været brugt siden 2018, der udsendes nye moduler hver 2. måned. Der følges op på, hvorvidt modulerne gennemføres, og efter to rykkere notificeres nærmeste leder.

Nye medarbejdere modtager en start pakke, og de introduceres til Cyberpilot og GDPR under deres introforløb.

På intra er der et GDPR-område, hvor der bl.a. ligger en FAQ. Der hænger plakater i personalestuen som skiftes med jævne mellemrum.

Der er udsendt et spørgeskema, som er fordelt til 5 undervisere og 5 administrative medarbejdere. Spørgeskemaet omhandler emner som indgår/bør indgå i awarenes kampagnerne.

Resultatet af spørgeskemaet ses herunder svar procent 100.

Spørgsmål	Rigtige svar	Kommentar
Du modtager en phising sms, hvad gør du? a) Kontakter ITCN b) Genkender nr. og trykker på link c) Sletter sms d) Gør intet da du ikke mener password skal skiftes	a) 9 c) 2 Forkert 0	9 havde kun et svar
Hvad er det bedste password? a) d0k4U66 b) J3gElskerEnGodBøf c) kaffe123	b) 7 Forkert 4	1 havde afkrydset tre muligheder, det rigtige og et forkert. 1 har ikke svaret

d) Foråret2017!		
Hvad kan man gøre for yderligere at sikre pc og systemer? a) Noterer alle password ned b) To faktor godkendelse c) Har billede af alle koder d) Benytter kun password få gange om dagen	b) 10 Forkert 0	
Hvad er en sikker mail? a) Ingen fortrolige og følsomme oplysninger b) Mail fra computer med antivirus c) Krypteret mail e) Sikrer at uvedkommende ikke får adgang	c) 10 Forkert 0	
Hvad er fordelen ved at anvende sikkermail? a) Man sikrer, at mailen kommer frem b) Mail kan ikke videresendes c) Indhold af mail kan ikke lækkes d) Uvedkommende har ikke adgang til mail	d) 6 Forkert 4	
Hvad er personoplysninger? a) Email b) Trafikdata c) Politisk overbevisning. d) Tatovering e) Biltypen man kører i f) Regnskab for en virksomhed g) Betalingsoplysninger	a) 3 c) 7 d) 7 g) 4 Forkert 4	2 mangler to svar 1 mangler tre svar 3 mangler et svar 1 har tre rigtige og et forkert svar 1 har tre rigtige og to forkerte svar 1 har ikke svaret 1 har et rigtigt og et forkert svar
Hvad kan indeholde personoplysninger? a) En video b) En lydoptagelse c) Et billede d) Et telefonopkald e) En avisartikel	a) 8 b) 7 c) 8 d) 6 e) 3 Alle rigtige 2	4 mangler et svar 1 mangler tre svar 1 mangler fire svar 1 mangler to svar 1 har ikke svaret
Hvor skal du henvende dig ved et sikkerhedsbrud? a) Digitaliseringsstyrelsen b) Datatilsynet c) Ingen da du er tvivl om, hvorvidt det er et databrud d) DPO, IT ansvarlig eller nærmeste leder	d) 10 Forkert 1	1 har to svar
Hvad er et sikkerhedsbrud? a) En klasseliste i et vindue i stueplan b) En vejledning om opsætning af en telefon c) En stjålet computer d) En åben computer e) Dokumenter med personoplysninger på et fællesdrev f) En mail med et nyhedsbrev	a) 10 c) 9 d) 9 e) 10 Forkert	2 har kun tre svar

Hvorfor er det vigtigt at installere alle opdateringer til computeren? a) Det er ikke vigtigt b) Computeren holder op med at virke c) For at få nyeste version af software d) Opdateringer lukker huller i software	d) 10 Forkert 1	1 har to svar
Hvad er udbyttet af awarenes programmet? a) Kan genkende persondata, ved hvordan de håndteres b) Kan genkende et brud på persondatasikkerheden c) Ved hvordan et stærkt password laves d) Genkender en phising mail e) Ved hvordan man arbejder sikkert hjemmefra f) Intet udbytte	a) 10 b) 10 c) 10 d) 10 e) 9 f)	

Der er generelt godt styr på, hvordan persondata skal behandles, og hvad man skal gøre, hvis man opdager et sikkerhedsbrud. Der er dog nogen tvivl om, hvad der er persondata, og hvilke medier der kan indeholde persondata. Måske en awarenes kampagne om disse emner er en god ide.

Alle ved, hvor de skal henvende sig, når der sker et sikkerhedsbrud, samt hvad der kan kendetegne et sikkerhedsbrud.

En awarenes kampagne om, hvordan man laver de stærkeste password, kan være en god ide.

Alle mener de har fået noget ud af awarenes træningen, det motiverer til at få modulerne gennemført.

Sikkerhedsbrud

Hvor mange sikkerhedsbrud har I haft i 2020 og 2021 til dato?

Type	2020	2021
Meldt til Datatilsynet	2	3
Mail sendt forkert	2	2
Eboks	0	0
Berører mange brugere	1	4
Fysiske dokumenter	1	1
Stjålet/bortkommet hardware	1	1
Andre sikkerhedshændelser	2	4
Sikkerhedsbrister i alt	8	10

For at vurdere om der er tale om et brud på persondatasikkerheden bruges følgende kriterier: Er der persondata involveret, og hvilken konsekvens har det for de registrerede.

GDPR-teamet vurderer, evt. i samarbejde med DPO, om sikkerhedsbruddet skal meldes til Datatilsynet. Kriteriet for om DPO involveres er, hvorvidt der er tale om en kendt problemstilling, eller om det er et nyt scenarie.

Hver gang et sikkerhedsbrud opdages, vurderes det, hvorvidt dette giver anledning til ændringer i processer og/eller risikovurderingen, samt om der er behov for øget awarenes.

Den medarbejder der forårsager/opdager et sikkerhedsbrud indberetter dette til GDPR-teamet, evt. via skema på intra, hvorefter GDPR-teamet varetager det videre forløb. Skaden forsøges begrænset som det første, herefter gennemgås sikkerhedsbruddet for at vurdere om, der skal ske anmeldelse til Datatilsynet. Den fulde dokumentation udarbejdes, og forløbet evalueres.

Beredskabsplan gennemgået den er fin.

De registreredes rettigheder

Har I en log over henvendelser vedr. de registreredes rettigheder?

Hvor mange henvendelser vedr. registreredes rettigheder, har i haft? fordelt på kategori

Type	2020	2021
Indsigtsbegæringer		
Berigtigelse		
Sletteanmodninger		
Begrænsning af behandling		
Dataportabilitet		
Afslag		

Der har ikke været henvendelse fra registrerede som ønskede at udøve deres rettigheder.

Stikprøve på behandling

Stikprøve for en behandling i Økonomi:

Afregning af kørsel: For medarbejdere foretages afregningen via Navision, og der indberettes via MinLøn Appen, dermed angives cpr. nr. ikke, og der er heller ingen følsomme oplysninger.

For elever foregik det tidligere via Navision, men pt. udbetales via banken, da det så ikke er nødvendigt at opbevare cpr. nr., dermed gemmes kun navn, adresse og konto oplysninger.

Eleven afleverer et fysisk dokument som dokumentation for kørsel f.eks. ved flytning fra Grenå til Randers. Dokument skannes og bogføres, hvorefter dokumentet makuleres.

Arbejdsprocessen er beskrevet meget kort i GDPR portalen, den kan med fordel uddybes.

Udlæg medarbejdere: Tidligere afleverede medarbejderne et fysisk dokument, pt. bruges Min Løn app, der kun indeholder alm. personoplysninger, lederen godkender udlægget.

Stikprøve for en behandling i forbindelse med ansøgning om SU:

Elever ansøger selv om SU og skolen involveres sjældent, da denne proces er automatisk, kun hvis eleven ikke er indskrevet korrekt, skal skolen gøre noget.

Skolen involveres, når der skal søges dispensation f.eks. i forbindelse med udeboende SU, elever uden uddannelsesaftaler, barsel m.m., eller når der går noget galt, så dukker ansøgningen op på en kontrolliste i US2000. Kontrollisten tjekkes en gang om dagen, når der er skolestart, ellers en gang om ugen.

Afsluttes uddannelsen før tid, skal datoen ændres i US2000

Dokumentation for ovenstående gemmes i Visma Case på den enkelte elev. Fysiske dokumenter makuleres.

Alle beskeder til eleverne sendes til elevernes eboks.

Ingen yderligere kommentarer.

Samtykker

Samtykker fra elever indhentes via studie +, de indhentes til brug af billeder og virksomhedsforlagt undervisning. Også til markedsføring indhentes samtykker.

Skolen bruger en standard skabelon til udarbejdelse af samtykker.

En stikprøvekontrol af hvorvidt samtykker stadig er gældende indføres i årshjulet.

Når der kommer en tilbagekaldelse af et samtykket, fjerner Kommunikation billederne. Modtagne tilbagekaldelse af samtykke har kun vedrørt billeder.

Sletning

I forhold til sletning af persondata, når elever/kursister afslutter uddannelsen, så følges anbefalingerne fra STIL.

Oplysninger der skal gemmes i en længere periode (f.eks. eksamensbeviser), gemmes i Visma Case, her opsættes kassationsregler, så der sker automatisk sletning.

Alt andet end beviser er opbevaret elektronisk, her er der opsat kassations/slette regler, så sletning sker automatisk.

Beviser opbevares fysisk, og her sker en årlig oprydning.

Der bør indføres en stikprøvekontrol i årshjulet, hvor der kontrolleres, at både automatisk sletning og oprydning i fysiske arkiver er sket i overensstemmelse med de angivne regler.

TV-overvågning

Der er ingen tv-overvågning.

Opfølgning fra 2020

Der er handlet på alle punkter fra rapporten i 2020.

Konklusion

Fortegnelsen bør opdateres med korrekte hjemler og udarbejdelse af de resterende risikovurderinger.

Cookies på hjemmesiden er opdateret efter de nyeste retningslinjer.

Generelt er der godt styr på, hvordan persondata skal behandles. Ligeledes er der ingen tvivl om, hvad der kendetegner et sikkerhedsbrud, samt hvad man skal gøre, hvis man opdager et sikkerhedsbrud.

Der er tvivl om, hvad der kendetegner persondata og et stærkt password, så en awarenes kampagne om disse emner er en god ide.

Oplysningspligterne er under opdatering, dette bør afsluttes snarest.

Anbefaling

Oplysningspligterne bør færdiggøres snarest.

Fortegnelsen bør gennemgås for at afdække om de rigtige hjemler er brugt, og de manglende risikovurderinger bør udarbejdes. Det bør gennemgås hvorvidt alle arbejdsprocesser, hvor der behandles persondata er fundet.

Awarenes kampagner, vedr. definitionen på persondata, hvad er et stærkt password og hvilke medier kan indeholde persondata, bør udføres.

Årshjulet bør færdiggøres.

Aalborg den 10.8.2022

Anne Lene Pugholm