24. maj 2018

Kommunernes it-fællesskab

Kære bibliotekschefer og kontaktpersoner

Som bekendt træder EU's nye databeskyttelsesforordning (GDPR) i kraft d. 25. maj 2018.

I den forbindelse gør KOMBITs projekter/løsninger status på deres GDPR-arbejde. Du modtager derfor denne status for Fælles Biblioteksbibliotek (FBS).

Generelt om KOMBITs arbejde med GDPR

Siden starten af 2017 har et internt projekt i KOMBIT arbejdet på at sikre, at alle løsninger, indkøbt på vegne af kommuner, indfrier GDPR, når den træder i kraft 25. maj 2018.

I den forbindelse har samtlige projekter/løsninger fra KOMBIT, der har nogen som helst berøring med personoplysninger, fået udstukket fire opgaver.

Projekterne har først kortlagt de datatyper og datastrømme, som den enkelte løsning behandler og understøtter. Dette blandt andet for at opfylde GDPR's fortegnelseskrav.

Med denne forudsætning på plads, har hver enkelt projekt/løsning skulle forholde sig til, hvordan registreredes rettigheder understøttes og håndteres i løsningen. Vi gør nærmere rede for dette længere nede i dette brev.

Den tredje opgave har været at gennemføre en risikovurdering for løsningen, hvor der er taget afsæt i de såkaldte ISO-standarder – som også er fundamentet for KL's drejebog for det kommunale arbejde med informationssikkerhed. Risikovurderingen for de enkelte løsninger udgør jeres kommunes fundament for den it-tekniske risikovurdering af jeres arbejde med løsningen.

Som den fjerde opgave, har alle projekter med væsentlige risici skulle forholde sig til disse i en såkaldt "Risikohåndtering". Dette har for nogle løsningers vedkommende givet anledning til ekstra udvikling, og kan også betyde enkelte opgaver til jer i kommunen.

Nedenfor gør vi status på arbejdet for FBS, og det arbejde vi har gjort, for at blive klar til GDPR den 25. maj 2018.

Du kan læse mere om KOMBITs arbejde med GDPR her.

Status på FBS' arbejde med GDPR

Vi har i FBS-projektet været igennem ovenstående opgaver, for at kortlægge, hvor FBS står i forhold til den nye forordning. Dette arbejde har vist, at FBS er rigtig godt med, hvorfor der ikke kræves de store tiltag for at indfri kravene fra GDPR.

Risikovurderingen har vist, at FBS systemmæssigt er konfigureret på en måde, der sikrer et passende sikkerhedsniveau. De implementerede sikkerhedsforanstaltninger i FBS er nærmere beskrevet i databehandleraftalens bilag 1.

Risikovurderingen tager udgangspunkt i selve FBS, og CMS- og selvbetjeningsløsninger ligger derfor udenfor rammerne af vurderingen.

Projektet har udsendt nye databehandleraftaler. Aftalerne er opdateret i forhold til de eksisterende med henvisning til Databeskyttelsesforordningen og er tilpasset Databeskyttelsesforordningens krav til databehandleraftaler. Aftalen er herudover udformet efter en fælleskommunal standardskabelon, som er godkendt af KOMBITs juridiske referencegruppe, og den ligger tæt op ad den nye databehandleraftale mellem leverandør og kommune.

Parterne i aftalen er KOMBIT (databehandler) og kommunen (dataansvarlig). KOMBIT er formelt databehandler på de løsninger, som KOMBIT på kommunernes vegne får udviklet, testet og idriftsat. Leverandøren (Systematic) til Biblioteksystemet FBS Cicero, er underdatabehandler til KOMBIT.

Databehandleraftalen er en forudsætning for, at kommunens behandling af personoplysninger i Biblioteksystemet FBS/Cicero kan finde sted. Da der skal indgås databehandleraftaler med alle kommuner tilsluttet Biblioteksystemet FBS/Cicero (én for hver kommune) er det nødvendigt, at aftalerne er identiske, så it-leverandøren (Systematic) kan leve op til ét sæt sikkerhedskrav.

Ændringer i FBS

KOMBITs arbejde med ovenstående har vist, at det ikke er påkrævet at foretage ændringer i FBS som følge af GDPR på nuværende tidspunkt.

Kommunens opgaver

Det er KOMBITs vurdering, at FBS løsningen ikke i sig selv afføder opgaver til kommunen ud over indgåelse af en ny databehandleraftale.

Kommunen bør dog generelt forholde sig til kommunens håndtering af registreredes rettigheder i forordningens art.12-22 på biblioteksområdet.

Konkret har KOMBIT herudover identificeret eventuel håndtering af oplysningspligten i artikel 14 og indsigtsretten i artikel 15.

Vedrørende artikel 14 bør i forhold til lærere og elever, hvor kommunen bør vurdere i forhold til lærere og elever, om disse skal gives særskilt. Oplysning om indhentning af oplysninger fra STIL ved oprettelse på skolebibliotekerne, eller dette ikke er omfattet af artikel 14.

Vedrørende artikel 15 bør kommunen vurdere, om indsigtsretten kan håndteres i kommunens selvbetjeningsløsninger eller dette skal håndteres manuelt.

KOMBIT vil løbende vurdere, om der viser sig processer, der med fordel kan understøttes digitalt i FBS.

24. maj 2018

KOMBIT
Kommunernes it-fællesskab

Registreredes rettigheder

Kommunerne har som dataansvarlige ansvaret for, at de registrerede sikres en række rettigheder i forhold til de personoplysninger, kommunen behandler og lader databehandlerer som fx KOMBIT og KOMBITs leverandører behandle i KOMBITs løsninger.

FBS-projektet i KOMBIT har analyseret FBS og vurderet, på hvilke områder FBS direkte understøtter håndteringen af de registreredes rettigheder, og hvor håndteringen sker udenfor FBS enten ved manuelle arbejdsgange eller it-understøttelse i andre systemer.

Analysen for FBS har vist, at:

1. FBS understøtter håndteringen af visse af de rettigheder, som den registrerede har
2. mange af rettighederne / oplysningspligterne hører hjemme i de grænseflader, som den registrerede benytter.

Det er begrænset, i hvilket omfang de registrerede selv kan tilgå FBS. FBS indeholder ikke en brugergrænseflade for selvbetjening på folkebibliotekerne. For folkebibliotekerne benytter lånere enten selvbetjeningsudstyr i filialen, personlig betjening af ansatte og forskellige webløsninger som bibliotekets CMS-system og bibliotek.dk For PLC'erne kan FBS-klienten sættes i et special mode, hvor den fungerer som selvbetjeningsklient. Endvidere er det muligt at benytte skoleportalen, som er en del af FBS.

Nedenfor får du et overblik over de artikler fra Databeskyttelsesforordningen der omhandler den registreredes rettigheder. Ud for hver enkelt artikel angives, i hvilket omfang KOMBIT og FBS kan bistå kommunerne med at håndtere de registreredes rettigheder.

Artikel 12 Håndteringen af udøvelsen af den registreredes rettigheder	Forordningens artikel 12 indeholder en række generelle betingelser for, hvordan den dataansvarlige (kommunen) skal kommunikere, når oplysningspligter, der følger af artikel 13 og 14, skal opfyldes. Det handler meget om principper og kommunikation. Da der ikke kommunikeres med borgere gennem FBS, men fx via mailserver i kommunen, skal kommunen håndtere dette udenfor FBS.
Artikel 13 Oplysningspligt ved indsamling af personoplysninger hos den registrerede	FBS indsamler ikke personoplysninger direkte hos den registrerede. I forbindelse med låneoprettelse sker indsamlingen enten via kommunens CMS-løsning eller ved personlig henvendelse til en bibliotekar. FBS understøtter derfor ikke oplysningspligten i artikel 13, og skal heller ikke gøre det fremover.
Artikel 14 Oplysningspligt, hvis personoplysninger	Artikel 14 handler om oplysningspligten, hvis den dataansvarlige indsamler personoplysninger hos andre end den registrerede, hvor den dataansvarlige også er forpligtet til at give den registrerede en række oplysninger herom.

ikke er indsamlet hos den registrerede	For lånere i PLC så oprettes lærer og elever automatisk som lånere ved at informationen hentes fra STIL's Infotjeneste eller manuelt ved at bibliotekaren opretter lånere i FBS-klienten. Artikel 14 indebærer derfor potentielt, at kommunen i forbindelse med oprettelse af lærere og elever kan have en oplysningspligt overfor lærere og elever om, at der indsamles oplysninger fra STIL Infotjeneste. Se nærmere herom under "kommunens opgaver":
Artikel 15 Ret til indsigt	I forhold til indsigtsret, så har den registrerede ret til at få den dataansvarliges bekræftelse på, om og hvilke personoplysninger om den registrerede, den dataansvarlige behandler. Der fremgår af artikel 15 a-ah en række konkrete oplysninger som den registrerede har ret til at få oplysninger om. Da ikke alle brugere har adgang til FBS, kan FBS ikke understøtte denne indsigtsret for den registrerede. Kommunen må derfor vurdere om opgaven kan løses i de lånervendte brugergrænseflader i fx CMS herunder den aktuelle registrerede information, eller om opgaven skal løftes manuelt, hvis en bruger henvender sig.
Artikel 16 Ret til berigtigelse	Databeskyttelsesforordningens artikel 16 fastsætter, at den registrerede har ret til at få urigtige personoplysninger om sig selv berigtiget af den dataansvarlige uden unødig forsinkelse. FBS stiller funktionalitet til rådighed, hvor den registrerede kan ændre visse personoplysninger gennem andre brugergrænseflader (fx CMS) eller ved henvendelse til en bibliotekar. Visse personoplysninger skal rettes i kildesystemerne som fx CPR-registeret eller STIL's Infotjeneste. Herudover understøtter FBS ikke kommunens håndtering af berigtigelsesanmodninger.
Artikel 17 Ret til sletning	Forordningens artikel 17 omhandler den registreredes ret til at få personoplysninger om sig selv slettet. Denne ret understøttes af muligheden for at blive slettet som låner i FBS. Der er dog visse situationer, hvor dette ikke kan ske. Fx ved fjernlånsbestillinger, skyldige beløb mm. Når en bruger slettes i FBS vil alle personoplysninger blive slettet fra FBS' database. Lånerne, der ikke har være aktive i en periode skal pt. slettes manuelt. FBS arbejder på at få implementeret en løsning, hvor lånere automatisk kan blive slettet, når de har været inaktive i en bestemt periode.

	Visse personoplysninger bliver automatisk slettet, eller når der ikke længere er erstatninger og mellemværende. Fx slettes lånehistorik efter 30 dage, dog ikke for Biblioteket Kommer-lånere.
Artikel 18 Ret til begrænsning af behandling	Forordningens artikel 18 fastsætter nærmere regler for, hvornår den registrerede har ret til at få begrænset behandlingen af personoplysninger, herunder nærmere regler for, hvad begrænsning af behandling indebærer. FBS indeholder ikke på nuværende tidspunkt funktionalitet til at begrænse behandlingen, da den registrerede i de fleste tilfælde blot vil kunne lad sig slette som låner. Er der tale om behandlingen af mellemværender med biblioteket, vil en begrænsning/standsning af behandlingen som udgangspunkt ske i debitorsystemet. Skulle der vise sig behov for funktionalitet til at begrænse behandling direkte i FBS, vil dette naturligvis indgå i videreudviklingen af FBS - løsningen.
Artikel 19 Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling	Det fremgår af forordningens artikel 19, at den dataansvarlige skal underrette hver modtager, som personoplysningerne er videregivet til, om enhver berigtigelse eller sletning af personoplysningerne eller begrænsning af behandling (der er udført i henhold til artikel 16, artikel 17, stk. 1, og artikel 18), medmindre dette viser sig umuligt eller er uforholdsmæssigt vanskeligt. Den dataansvarlige oplyser den registrerede om disse modtagere, hvis den registrerede anmoder herom. FBS videregiver ikke oplysninger om sletning, berigtigelse mv. til andre. Sker dette på anden vis i kommunen, f.eks. manuelt, bør kommunen ligeledes sikre, at der tages højde for artikel 19.
Artikel 20 Ret til dataportabilitet	Det vurderes ikke, at FBS er omfattet af artikel 20.
Artikel 21 Ret til indsigelse	Det fremgår af forordningens artikel 21, at den registrerede af forskellige grunde kan have ret til at gøre indsigelse mod behandling af sine personoplysninger. Artikel 21 er ikke relevant i relation til FBS-løsningen, da behandling i FBS er baseret på samtykke, og lånere kan lade sig slette, hvis de ikke længere ønsker deres oplysninger behandlet.
Artikel 22	I FBS træffes der ingen automatiske individuelle afgørelser, herunder afgørelser baseret på profilering, så artikel 22 er derfor ikke relevant.

24. maj 2018

KOMBIT
Kommunernes it-fællesskab

Automatiske
individuelle
afgørelser, herunder
profilering

Håndtering af evt. brud på persondatasikkerheden *(Databeskyttelsesforordningen art. 33-34)*

En afgørende faktor i forbindelse med brud på persondatasikkerhed er reglen om, at en hændelse skal håndteres uden unødig forsinkelse og senest indenfor 72 timer.

KOMBIT har i længere tid arbejdet med et fast sikkerhedsberedskab, som historisk set såvel som fremadrettet altid vil reagere og rette eventuelle sikkerhedsbrist indenfor mindre end 72 timer.

For at sikre hurtig reaktion og rettelse, er det imidlertid vigtigt, at kommunerne hurtigt bringer eventuelle henvendelser om sikkerhedsbrud videre til leverandørerne af den berørte løsning, som vil orientere KOMBIT, der straks vil sætte sit sikkerhedsberedskab i værk.

KOMBITs Videncenter arbejder derfor også på at nedfælde og dele faste processer for sikkerhed i relationen mellem kommunerne og KOMBIT.

Efter opdaget sikkerhedsbrud køres alle processer imellem KOMBIT og berørte kommuner via sikker mail. Leverandørerne er forpligtet til at levere en redegørelse, så berørte kommuner kan få et fuldt overblik over hændelsens årsag, omfang og berørte parter indenfor 24 timer.

I KOMBITs proces for håndtering af brud på persondatasikkerhed er det kommunen, der vurderer, om hændelsen anmeldes til Datatilsynet, og kommunen selv, der har ansvaret for at sende anmeldelsen til Datatilsynet.

Kommunerne er også selv ansvarlige for at vurdere, om registrerede skal underrettes (i henhold til artikel 34), ligesom det er kommunen der varetager selve underretningen.

KOMBITs opgave ligger således i at indsamle informationer om sikkerhedsbruddet til kommunen, mens kommunen er ansvarlig for at foretage det videre fornødne for at opfylde kravene i artikel 33 (anmeldelse til Datatilsynet) og artikel 34 (underretning af registrerede).

Det er vigtigt, at kommunen er opmærksom på at have et beredskab klar, til at modtage redegørelser fra KOMBIT i forbindelse med sikkerhedsbrud.

Spørgsmål

Kan altid rettes til projektpostkassen bibsys@kombit.dk