Maj 2017

Eksempel fra KOMBIT: Udkast til krav om compliance med persondatalovgivning og sikkerhedsstandarder

KOMBIT gør opmærksom på, at kravene i dette dokument foreligger i udkastform *og indgår i et overordnet arbejde med at implementere Databeskyttelsesforordningen i KOMBIT. Der pågår således stadig en proces om formuleringen af kravene.*

Det skal understreges, at dette udkast er et internt KOMBIT-dokument udarbejdet til brug i KOMBITs organisation og projekter. Der er således tale om et eksempel på KOMBITs tilgang, som udelukkende deles til inspiration. Dokumentet deles i sin oprindelige form og indholdet i dokumentet afspejler derfor udelukkende den viden om Databeskyttelsesforordningens indhold, som var kendt på det tidspunkt, hvor KOMBIT udarbejdede udkastet. Vi gør opmærksom på, at dette dokument derfor ikke vil være tilpasset eventuelle senere anbefalinger fra f.eks. Justitsministeriet, KL eller Datatilsynet vedr. fortolkning og national implementering af Databeskyttelsesforordningen. For at undgå en overimplementering af forordningens krav, anbefaler vi, at kommuner løbende orienterer sig om KL's og Justitsministeriets arbejde med at kortlægge, hvordan forordningen skal implementeres – vi henviser i den forbindelse til KL's hjemmeside, hvor man kan finde KL's anbefalinger til implementering af forordningen. Enhver brug af dette dokument i original eller tilpasset form sker på eget ansvar.

Vejledning

Kravene om compliance med lovgivning og sikkerhedsstandard er en del af et generelt sikkerhedsbilag, der kan danne udgangspunkt for KOMBITs udbud af it-systemer. Kravene er generiske og skal opfattes som en brutto-liste af sikkerhedskrav. Der bør derfor altid ske en tilpasning i forhold til behovene for det konkrete System. Der kan f.eks. være krav, som ikke er relevante for en bestemt løsning og som derfor bør slettes, eller der kan være behov for at tilpasse ambitionsniveauet i andre krav på baggrund af en konkret risikovurdering. Her forsøger vejledningsbokse som denne at guide, hvornår det enkelte krav er relevant.

Som udgangspunkt er ambitionsniveauet i dette bilag sat højt for at understøtte behandling af følsomme personoplysninger, da dette er et behov i mange af KOMBITs udbud. For systemer, der ikke behandler personoplysninger eller forretningsfølsomme data, kan sikkerhedskravene derfor godt være for høje.

Inden tilpasning af sikkerhedskravene er det essentielt at have gennemført en kortlægning af hvilke data, der findes i systemet, samt deres følsomhedskategorier. Endvidere er det relevant at have gennemført en sikkerhedsmæssig risikovurdering samt en privatlivsimplikationsanalyse (PIA) for systemer med mange og følsomme personoplysninger. Dette sikrer, at valget af kontroller (og dermed tilhørende omkostninger) er afstemt med identificerede risici.

Krav om ledelsessystem for informationssikkerhed

Krav 01-01.	**ISO 27001**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Leverandøren skal med henblik på løbende sikring af sikkerhedskravene i tilknytning til levering af Kontraktens ydelser opretholde et ledelsessystem for informationssikkerhedsstyring (ISMS) efter den til enhver tid gældende version af ISO/IEC 27001 eller tilsvarende (national eller international) anerkendt standard baseret på en risikostyringsproces. Leverandøren skal herunder løbende tilpasse sit ISMS, såfremt Leverandørens opdatering af sin risikovurdering medfører et behov herfor.		

Krav om compliance med persondatalovgivning og praksis

Krav 01-02.	**Persondataregulering**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Leverandøren skal sikre, at Systemet behandler persondata i overensstemmelse med persondataloven: • Lov om behandling af personoplysninger (Persondataloven) Lov nr. 429 af 31.5.2000 med senere ændringer, herunder ved lov nr. 280 af 25.4.2001 (Justitsministeriet/Datatilsynet), og Lov nr. 639 af 12.6.2013 (Justitsministeriet). • Bekendtgørelse nr. 528 af 15. juni 2000 som ændret ved Bekendtgørelse nr. 201 af 22. marts 2001 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsbekendtgørelsen). • EU General Data Protection Regulation 679/2016 (GDPR). Bemærk, at denne træder i kraft 25. maj 2018. Datatilsynets praksis omkring behandling af personoplysninger skal følges, og data skal behandles i overensstemmelse med god databehandlingsskik.		

Krav 01-03.	**Kun nødvendige data eksisterer i systemet**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Systemet skal, blandt andet ved integration af data fra eksterne systemer, understøtte, at der kun indhentes og gemmes oplysninger, som er nødvendige og relevante.		

Persondataloven (lov nr. 429 af 31. maj 2000 med senere ændringer) erstattes pr. 25. maj 2018 af Databeskyttelsesforordningen (EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse)) og herefter følger reglerne for, hvornår og hvordan personoplysninger kan behandles direkte af Databeskyttelsesforordningen (i det følgende også benævnt GDPR).

Forordningen stiller krav til dataansvarlige og databehandlere, når de behandler personoplysninger, f.eks. i forbindelse med indsamling og videregivelse af personoplysninger, hvor man – alt afhængig af, hvilket følsomhedsniveau personoplysningerne har – skal overholde en række betingelser i forbindelse med behandlingen af disse oplysninger.

Forordningen giver herudover den registrerede en række rettigheder om f.eks. ret til indsigt i de oplysninger, der behandles i Systemet om den registrerede, ret til at få information om, at der indsamles oplysninger om den registrerede, og ret til at få slettet eller rettet urigtige oplysninger.

Forordningen opdeler personoplysninger i forskellige typer med hver deres følsomhedsniveau, fordi der gælder forskellige betingelser og procedurer for behandling af personoplysninger afhængig af oplysningernes følsomhed.

Databeskyttelsesforordningen indeholder en række regler om håndtering af persondata og registreredes rettigheder og træder i kraft 25. maj 2018. Der er med dette udgangspunkt behov for, at Systemet understøtter funktionalitet, der gør det muligt for anvenderne at overholde Databeskyttelsesforordningens regler om håndtering af persondata og registreredes rettigheder. For at understøtte dette behov, skal Systemet understøtte retten til indsigt samt retten til at blive glemt.

Ret til indsigt og ret til at blive glemt

I forhold til retten til indsigt, har den registrerede ret til at få den dataansvarliges bekræftelse på, om der behandles oplysninger og i så fald hvilke.

Retten til at blive glemt omhandler den registreredes ret til at blive glemt, hvilket kræver funktioner til udsøgning og sletning af data.

Vejledning

Nedenstående krav følger af de almene rettigheder for datasubjekter i GDPR. Hvis det vurderes, at der eksisterer en lovhjemmel der gør, at disse rettigheder ikke bliver relevante (f.eks. retten til at blive glemt), kan kravene fjernes eller opblødes.

Krav 01-04.	**Håndter ønske om indsigt og at blive glemt – Fremsøgning af data**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Det skal være muligt i Systemet at fremsøge alle data om en person i forbindelse med en indsigtsbegæring samt i forbindelse med retten til at blive glemt. I forbindelse med fremsøgningen skal Systemet understøtte, at der kan søges i samtlige datakilder inkl. databaser, filer, logs mv. om en given Person. I fremsøgningen skal der kunne angives en person, en tidsperiode, typer af data (f.eks. dokumenter eller billeder) etc.		

Krav 01-05.	**Håndter ønske om indsigt og at blive glemt - Bruttoliste**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Systemet skal understøtte, at der i forbindelse med en søgning vises en bruttoliste over data, der matcher søgekriterier, og som kan omhandle den valgte Person, herunder hvor Personen fremgår i forbindelse med opmærkninger, eller hvor det på anden måde kan udledes, at data sandsynligvis er relateret til Personen.		

Krav 01-06.	**Håndter ønske om indsigt og at blive glemt – eksport af bruttoliste**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Systemet skal understøtte, at bruttolisten, jf. krav [01-05], kan eksporteres til videre behandling.		

Efter eksport af bruttolisten vil Brugeren kunne gennemgå listen manuelt for at afgøre, om de enkelte dataobjekter er omfattet af indsigtsbegæringen, og om der eventuelt skal slettes dele af indholdet, inden det deles. På den måde kan der anlægges en menneskelig/juridisk fortolkning af, hvilke data, der er omfattet. Efter endt manuel gennemgang og filtrering kan Brugeren dele dataobjekterne med den Person, der har fremsat indsigtsbegæringen.

Krav 01-07.	**Håndter ønske om indsigt og at blive glemt – sletning af data**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Systemet skal understøtte, at data i kan slettes som led i retten til at blive glemt.		

Brugeren forventes, efter data er slettet, at informere Personen om, at dennes anmodning om at få slettet data er imødekommet.

Systemet må ikke opbevare data, som med sikkerhed ikke skal anvendes senere af Systemet. Desuden har alle data en maksimal tid, som de må gemmes, og derfor er det vigtigt, at Systemet sørger for daglig oprydning af data.

Krav 01-08.	**Sletning af data sikres**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Systemet skal sikre, at data i Systemet, som ikke senere skal anvendes af Systemet, bliver slettet. Systemet skal indeholde oprydningskørsler, som gennemfører disse sletninger i alle Systemets datakilder (inkl. databaser, filer og logninger). Disse oprydningskørsler skal også sikre sletning af data, som skal fjernes fra Systemet på baggrund af retten til at blive glemt. Leverandøren skal i samarbejde med KOMBIT i afklaringsfasen fastlægge regler for sletning af data.		

Som anført skal Systemet understøtte retten til at blive glemt. Af praktiske årsager medfører retten til at blive glemt ikke sletning af backup-kopier af data. Her gælder i stedet det princip, at data, som er slettet på baggrund af reglerne om retten til at blive glemt, ikke må restores. Hvis der er behov for en stor restore-operation, hvor disse slettede data ikke kan undtages fra restore, f.eks. ved fuld restore af database, skal data slettes igen umiddelbart efter restore.

Krav 01-09.	**Retten til at blive glemt skal registreres**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Systemet skal sikre, at data i Systemet, som bliver slettet på baggrund af retten til at blive glemt, bliver registreret, så det kan sikres, at disse data ikke senere bliver restored fra backup. Inden restore af fuld backup skal Systemet undersøge, om der i backuppen findes data, som er slettet på baggrund af retten til at blive glemt, og slette disse, inden de bliver tilgængelige i Systemet. Når en fuld backup-cyklus er overstået, og der derfor er sikkerhed for, at data, som er slettet på baggrund af retten til at blive glemt, ikke længere er at finde på backup, skal registreringen af den gennemførte sletning også fjernes.		

Vejledning

Nedenstående krav handler eksplicit om personer, der i CPR har navne- og adressebeskyttelse. Hvis sådanne personer ikke behandles i systemet, kan kravet fjernes.

Navne og adressebeskyttelse

Krav 01-10.	**Navne- og adressebeskyttelse**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Systemet skal sikre, at navne- og adressebeskyttelse i CPR altid registreres sammen med de berørte oplysninger, og Systemet skal vise en meddelelse til Brugeren om, at navn og adresse er omfattet af navne- og adressebeskyttelse.		

Samtykke (GDPR artikel 7 og 8)

Vejledning

Nedenstående krav handler om håndtering af samtykker i relation til behandling af personoplysninger. Hvis der vurderes at være lovhjemmel til alle systemets behandlinger af personoplysninger, er samtykkekravene umiddelbart ikke relevante.

Krav 01-11.	**Indhentning af samtykke**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Systemet skal understøtte, at der kan indhentes samtykke fra de registrerede til følgende formål: • Formål X (*Definer hvad samtykket indebærer*) • Formål Y (*Definer hvad samtykket indebærer*) • Formål Z (*Definer hvad samtykket indebærer*) Samtykket til behandling af personoplysninger skal være frit, specifikt, informeret og utvetydigt.		

Jf. GDPR, skal samtykket være utvetydigt, og hvis der behandles følsomme personoplysninger, skal samtykket være eksplicit.

Samtykket er utvetydigt, når de registrerede foretager en bekræftende handling, som tilkendegiver, at de registrerede accepterer den konkrete behandling af personoplysningerne til det konkrete formål. Eksempler på et sådant samtykke inkluderer, at de registrerede klikker i en boks, vælger indstillinger, afgiver en erklæring eller på anden måde udviser en adfærd, der tilkendegiver samtykket.

Den dataansvarlige er forpligtet til at kunne dokumentere, at samtykket er givet.

Krav 01-12.	**Dokumentation af samtykke**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Systemet skal kunne dokumentere, at samtykket er specifikt, informeret og utvetydigt i forhold til formålet.		

De registrerede har dog altid mulighed for at trække deres samtykke tilbage, hvis de har behov for dette. Derfor er det også vigtigt, at et system der anvender samtykker også understøtter de registrerede i at trække et samtykke tilbage.

Krav 01-13.	**Tilbagetrækning af samtykke**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Systemet skal understøtte registreredes ret til at trække sine samtykker tilbage.		

Ret til indsigelse og automatiske individuelle afgørelser (profilering)

> ***Vejledning***
>
> *Nedenstående krav handler om håndtering af profilering. Hvis det vurderes, at systemet ikke foretager profilering som defineret i Databeskyttelsesforordningen (afgørelser baseret på automatisk behandling), kan det overvejes, om kravene bør fjernes.*

Der introduceres i Databeskyttelsesforordningen en helt ny rettighed til de registrerede, som skal sikre, at de ikke kan profileres. Profilering er afgørelser, der alene er baseret på automatiserede behandlinger, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende.

Krav 01-14.	**Fritagelse for Profilering**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Hvis den registrerede har ret til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, så skal systemet understøtte den registreredes ret til at kunne fritages for profilering		

Krav 01-15.	**Indsigelse til Profilering**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Hvis den registrerede har været genstand for en afgørelse, der alene er baseret på automatisk behandling, som har været fejlbehæftet, så skal man i systemet kunne gå tilbage og rette i den gældende profilering.		

Privacy by default & Privacy by design

GDPR's artikel 25 fastsætter principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger vedrører helt overordnet, hvordan den dataansvarlige skal indrette sig teknisk og organisatorisk for at opnå effektiv implementering af databeskyttelsesprincipper og integrering af de fornødne garantier i behandlingen for at opfylde kravene i GDPR og beskytte de registreredes rettigheder.

Vejledning

Nedenstående krav handler om princippet "privacy by default and design" (også kendt som databeskyttelse gennem design og standardindstillinger, jævnfør GDPR's artikel 25). Hvis brugeren har indstillingsmuligheder i systemet (f.eks. under en brugerprofil), vil delen om standardindstillinger være særlig relevant.

Bestemmelsens nærmere rækkevidde giver – navnlig grundet dens forholdsvis abstrakte indhold – anledning til en vis usikkerhed i forhold til, hvornår en dataansvarlig med sikkerhed kan siges at have henholdsvis overtrådt og efterlevet bestemmelsens krav.

Det er derfor relevant, at projektet i KOMBIT nærmere overvejer implikationerne for det konkrete system, og dermed ikke efterlader for stor usikkerhed hos Leverandøren.

Muligheden for at anvende godkendte certificeringsmekanismer til at dokumentere overholdelse af kravene om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger er et af de tiltag, som man overvejer i forhold til at konkretisere indholdet og rækkevidden af kravene.

Krav 01-16.	**Databeskyttelse gennem design og standardindstillinger**		
Kategori:	(K)	Type:	Ikke funktionelt
Beskrivelse:	Systemet skal understøtte databeskyttelse gennem design og standardindstillinger (jævnfør GDPR's artikel 25), hvilket betyder, at alle standardindstillinger som udgangspunkt skal give den stærkest mulige privatlivsbeskyttelse, samt at sikkerhed og privatlivsbeskyttelse skal være designet ind i systemet fra begyndelsen. Hvis man vil afvige fra disse indstillinger, skal datasubjektet træffe et eksplicit valg. Mængden af informationer der vises om den registrerede skal stadig være nok til at brugeren/systemet kan gennemføre behandlingen.		