Vejledning til kortlægningsværktøj 4.0

Processer, systemer, services, dataklassificering og behovsvurdering for konsekvensanalyse.

December 2019

pwc

Revision. Skat. Rådgivning.

Indholdsfortegnelse

Introduktion til kortlægningsværktøjet

Formålet med kortlægningsværktøjet er at danne et dokumenteret og detaljeret overblik over de(t) udvalgte forretningsområde(r), herunder de tilknyttede

processer, systemer, services og behandlede personoplysninger.

Templaten er overordnet inddelt i otte faneblade, som bør udfyldes i nedenstående rækkefølge:

1. Processer
2a. Systemer
2b. Systemdeling
2c. Dataklassifikation
3a. Services og ydelser (ikke systemer)
3b. Dataklassifikation (services og ydelser)

Flere af fanerne er yderligere farveopdelt i hovedområder, der kræver input fra forskellige afdelinger/personer i organisationen, som angivet nedenfor:

- Ansvarlig for forretningsområdet
- It
- Juridisk afdeling

Generelt er værktøjet opbygget med forklaringer og eksempler på, hvordan det anvendes og udfyldes korrekt. Bemærk, at **det kun er hvide felter, der skal udfyldes.**

I denne vejledning følger en kort introduktion til hvert faneblad, herunder formålet og guidelines til, hvordan de udfyldes korrekt. Mange af forklaringerne findes også i selve kortlægningsværktøjet.

1. Processer (og dataflow)

Overordnet er fanen opdelt i tre hovedområder – beskrevet nedenfor – som hver kræver input fra forskellige afdelinger:

Daglige arbejdsgange – Forretningsansvarlig
Først og fremmest skal alle forretningsområdets processer og dataflows beskrives. For at skabe bedre overblik er det muligt

at kategorisere processerne med underprocesser. Et eksempel på en proceskategorisering i HR kunne fx være som illustreret til højre herfor:

Ud fra hver underproces skal dataflowet beskrives, herunder bl.a. hvorfra personoplysninger indsamles fra, hvem de(n) deles med, og hvor den lagres. Derudover skal det angives, hvorvidt processen er dokumenteret og beskrevet i eksempelvis politikker eller lignende.

Periodiske arbejdsgange – It
Som en del af dataflowet skal det angives, om – og i så fald – hvor personoplysninger logges og arkiveres, samt hvornår og hvordan personoplysninger slettes. Dette kræver muligvis en større teknisk indsigt og derfor involvering af en it- eller systemansvarlig.

Juridiske grundlag – Juridisk afdeling
Sidste del af procesbeskrivelsen omhandler det juridiske grundlag, herunder formål, behandlingsgrundlag, hvordan et eventuelt samtykke indhentes, og hvorvidt oplysningspligten er iagttaget. Vi anbefaler, at jeres juridiske afdeling inddrages til beskrivelsen af disse punkter.

Bemærk, at det anbefales at der laves én Excel-fil pr. hovedproces, så der fx laves én fil for alle HR-processer, én for alle marketingprocesser mv..

Proces	Underproces
Ansættelse	Jobopslag Modtagelse af ansøgninger Afslag på ansøgning Indkaldelse til jobsamtale Personlighedstests Anbefalinger Straffeattest
Kontrakt	Oprettelse af kontrakt Ændring af kontrakt
Kontrakt	Medarbejder opsiger Medarbejderen opsiges

2a. Systemer (og applikationer)

Overordnet er fanen opdelt i tre hovedområder beskrevet nedenfor, som hver kræver input fra forskellige afdelinger:

Systemer – Forretningsansvarlig

Først og fremmest skal alle de systemer og applikationer, der anvendes inden for forretningsområdet, angives under systemnavn. Der skal ligeledes angives henholdsvis en dataejer og en systemejer.

Dataejeren bør være den enhed eller ansvarlige for enheden, der har sin daglige gang i systemet og behandler personoplysninger, og som for den enhed er den overordnede ansvarlige for de personoplysninger, der registreres i systemerne. Systemejeren er den person eller afdeling, der har ansvaret for driften og vedligeholdelsen af systemet, fx intern it eller ansvarlig herfor.

Da et systemnavn ikke nødvendigvis angiver, hvilken type system der er tale om, skal der i feltet beskrivelse angives en beskrivelse af systemet og ligeledes bør de processer, systemet anvendes i, også angives.

Leverandør – It

Dernæst skal leverandøren af systemet angives, samt om løsningen er outsourcet og lokation for datalagring. Denne information er vigtig, da der gælder forskellige regler ifølge databeskyttelsesforordningen, alt efter hvor og hvordan personoplysninger lagres. Da denne information muligvis kræver større teknisk indsigt og baggrundsviden, anbefales det, at it eller den systemansvarlige inddrages til beskrivelsen heraf.

Juridisk grundlag – Juridisk afdeling

Til sidst skal det juridiske grundlag for systemet beskrives. Først og fremmest skal ansvaret for personoplysninger, der behandles, angives, dvs. om jeres rolle er dataansvarlig, databehandler, eller om ansvaret er delt. Dernæst skal det angives, om der er indgået en databehandleraftale med leverandøren. Såfremt personoplysningerne overføres til et tredjeland (lande uden for EU/EØS), skal det juridiske grundlag herfor angives.

Det er vores klare anbefaling, at der her inddrages juridisk bistand til fastlæggelse af det juridiske grundlag, da disse oplysninger er essentielle i forhold til opfyldelse af kravene i databeskyttelsesforordningen. Nedenfor er angivet en kort beskrivelse af ansvarsrollerne og en databehandleraftale. Beskrivelserne findes også i templaten ved at holde musen over felterne.

Ansvarsroller:
Dataansvarlig: Er den som afgør, til hvilket formål og med hvilke hjælpemidler personoplysningerne må behandles.
Databehandler: Er den der behandler personoplysningerne på vegne af den dataansvarlige og under instruks fra den dataansvarlige.

Delt ansvar eller fælles dataansvar: finder sted i de tilfælde hvor to eller flere parter i fællesskab bestemmer formålet med behandlingen af personoplysninger og hvilke hjælpemidler.

Databehandleraftale: En databehandleraftale er en aftale (en kontrakt eller anden retligt dokument), som den dataansvarlige indgår med databehandleren, i de tilfælde hvor der benyttes en databehandler. I aftalen fremgår der bl.a., at databehandleren alene handler under instruks fra den dataansvarlige, og at databehandleren skal træffe forskellige tekniske og organisatoriske sikkerhedsforanstaltninger.

2a. Systemer (og applikationer)

Overførsel til tredjelande (lande uden for EU/EØS):

Følgende er eksempler på, hvornår personoplysninger overføres til et tredjeland:

- Et system hvor personoplysningerne registreres og behandles i, ligger på en server i et tredjeland,
- It-udviklingsafdelingen og/eller supportafdelingen befinder sig i et tredjeland, og disse får adgang til, herunder kigge-adgang til personoplysningerne i forbindelse med deres a rbejde;
- Personoplysningerne tilgås i tredjeland via fjernadgang til systemet (selv hvis systemet hostes indenfor EU/EØS);
- Personoplysningerne overføres/sendes til en leverandør, samarbejdspartner, kunde eller lign. i et tredjeland.

Bemærk at listen ikke er udtømmende og I derfor altid bør undersøge dybdegående, om der sker overførsel af personoplysninger til tredjelande.

Såfremt personoplysningerne overføres til et tredjeland, skal I sikre jer, at I har et juridisk grundlag herfor. Se herunder for eksempler[1] på muligheder for at overføre personoplysninger til et tredjeland:

1. Sikre tredjelande[2] er lande uden for EU/EØS, som EU-Kommissionen har vurderet som sikre lande i forhold til overførsel af personoplysninger, og som derfor ikke kræver yderligere tiltag, før man må overføre personoplysninger til de pågældende lande.Bemærk, at for nogle sikre lande, er det kun visse personoplysninger der må overføres.
2. Privacy Shield (USA)[3] – er en selvcertificeringsordning, hvor amerikanske selskaber kan søge om at få et certifikat, der giver dem lov til at behandle visse typer personoplysninger.
3. Standardbestemmelser om databeskyttelse vedtaget af EU-kommissionen: Eu-kommissionen har vedtaget tre sæt standardbestemmelser om databeskyttelse. Standardkontraktenskal indgås med den leverandør, samarbejdspartner, kunde eller lign. som I overfører personoplysningerne til.
4. Bindende virksomhedsregler – også kaldet Binding Corporate Rules (BCR), er interne virksomhedsregler i en koncern, der stiller krav til virksomhedens behandling af personoplysninger. De bindende virksomhedsregler skal godkendes af det lokale datatilsyn i det EU/EØS land, hvor koncernens hovedkontor ligger. Inden de kan godkende, skal der forelægges et udkast til godkendelse hos Det Europæiske Databeskyttelsesråd, som kommer med en udtalelse. Hvis det pågældende datatilsyn følger udtalelsen, kan de godkende de bindende virksomhedsregler, og så må koncernen frit overføre og behandle personoplysninger indenfor koncernen uagtet om det sker indenfor eller udenfor EU/EØS. Bemærk at denne ordning kun gælder for koncernen.

Mindst én af de ovenstående muligheder skal benyttes, før man må overføre personoplysningerne til tredjelandet.

1 Se nærmere i datatilsynets vejledning om overførsel af personoplysninger til tredjelande, juni 2019

2 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

3 https://www.privacyshield.gov/list

2b. Systemdeling (med andre selvstændige selskaber)

Fanen systemdeling er ikke relevant for alle organisationer. Såfremt jeres organisation ikke deler systemer med andre selvstændige selskaber og/eller jeres organisation ikke er en del af en koncern eller er franchisegiver eller -tager, skal dette faneblad ikke udfyldes.

Overordnet er fanen opdelt i tre hovedområder, beskrevet nedenfor, som hver kræver input fra forskellige afdelinger:

Systemanvendelse – Forretningsansvarlig

Såfremt et system anvendes af andre selvstændige selskaber end jeres eget, skal disse selskaber angives under anvendelse. Andre selvstændige selskaber kan fx være andre selskaber inden for koncernen, men som har deres eget CVR-nummer. Det kan eksempelvis også være franchisebutikker, der bruger systemer, stillet til rådighed af franchisegiveren. I dette tilfælde deler franchisegiveren systemer med franchisetagerne.

Herudover skal det angives, om ansatte i jeres organisation har adgang til de oplysninger, som de selvstændige selskaber registrerer og behandler i systemet. Kan ansatte i jeres organisation fx læse, rette, slette eller på anden vis behandle oplysningerne.

Data – It

Hvis et system anvendes af andre selvstændige selskaber, skal det angives under dataadskillelse, hvorvidt personoplysningerne kan adskilles teknisk og logisk. Dvs. om de selvstændige selskabers personoplysninger kan adskilles og flyttes til et andet system, såfremt det selvstændige selskab ønsker dette.

Juridisk grundlag – Juridisk afdeling

Til sidst skal det angives, hvorvidt der er indgået en leverandørkontrakt med det selvstændige selskab om brugen af systemet; eller såfremt der er tale om koncernforbundne selskaber, om der er indgået en koncernintern aftale om brugen af systemet. Dernæst skal ansvaret for personoplysningerne beskrives, dvs. om rollen er dataansvarlig, databehandler eller om ansvaret er delt, om der er indgået en databehandleraftale, og om personoplysningerne overføres til tredjelande.

2c. Data(klassifikation)

Under fanen ”2c. Dataklassifikation” skal alle de forskellige kategorier af personoplysninger, der behandles i systemerne og applikationerne, angives og klassificeres. Der er foruddefineret en række personoplysninger, men såfremt der behandles andre typer, skal disse angives i kolonnen “Persondata/Kategori” – enten ved at vælge dem ud fra den foruddefinerede liste eller ved at indtaste dem manuelt. Vælges personoplysningerne fra den foruddefinerede liste, klassificeres oplysningerne automatisk ud fra dataklassifikationsmodellen (se separat dokument), men indtastes de manuelt, skal klassifikationen også tilføjes manuelt ved at klikke på dropdown-boksen. Få hjælp til klassifikationen i klassifikationsmodellen.

Ud fra hvert system, der automatisk er udfyldt i række tre, skal der blot sættes x ud for de oplysninger, som behandles i systemet.

Nedenfor er vist en lang række af eksempler på kategorier af personoplysninger og deres klassificering:

Kategori af personoplysninger	Klassifikation	Kategori af personoplysninger	Klassifikation	Kategori af personoplysninger	Klassifikation
Adfærdsdata fra hjemmeside	Almindelig, fortrolig	Filosofisk overbevisning	Følsom	Mobilbilleder	Almindelig, fortrolige
Adresse – arbejde	Almindelig	Forbrugsvaner	Almindelig, fortrolig	Mobilkontakter	Almindelig
Adresse – privat	Almindelig	Fordelskort-nr.	Almindelig	Navn	Almindelig
Betalingskortoplysninger	Almindelig	Fødselsdato	Almindelig	Onlineidentifikation (fx IP- og MACadresse)	Almindelig
Biometriske data	Følsom	Genetiske data	Følsom	Oplysninger om forbrug	Almindelig, fortrolig
Booking-nr.	Almindelig	Google-login	Almindelig	Politisk overbevisning	Følsom
CPR-nr.	Almindelig, fortrolig	Helbredsoplysninger	Følsom	Foto	Almindelig, fortrolig, følsom
Data fra sociale medier (Fx Facebook)	Almindelig	Interesser	Almindelig	Reg.- og konto-nr.	Almindelig
		Ja til nyhedsmail	Almindelig	Religiøs overbevisning	Følsom
Data fra søgemaskiner (fx Google)	Almindelig	Ja til SMS	Almindelig	Seksuelle forhold/orientering	Følsom
		Kunde-nr.	Almindelig		
E-mail – arbejde	Almindelig	Køn	Almindelig	Sociale forhold	Almindelig, fortrolig
E-mail – privat	Almindelig	Lokationsdata	Almindelig	Strafbare forhold	Almindelig, fortrolig
Etnicitet/Race	Følsom	Medarbejder	Almindelig	Telefonnr.	Almindelig
Facebook-login	Almindelig	Medlems-nr.	Almindelig	Titel (hr., frk. el fru)	Almindelig
Fagforening	Følsom			Økonomiske forhold	Almindelig, fortrolig
Favoritbutik	Almindelig				

Bemærk, at I kan have en anden dataklassifikationsmodel end den generiske, der følger med kortlægningsværktøjet. I bør derfor altid forholde jer kritisk til den prædefinerede liste med eksempler på kategorier af personoplysninger og deres klassificering i kortlægningsværktøjet og tilrette så den stemmer overens med den dataklassifikationsmodel, I har besluttet at benytte internt i jeres organisation.

2d. Personrisikovurdering og grundlag for vurdering

Fanen systemdeling er ikke relevant for alle organisationer. Formålet med risikovurderingen er at identificere, analysere og vurdere nuværende og fremtidige risici for de registrerede, der er knyttet til de systemer som indgår i behandlingsprocesserne.

Selve risikovurderingen består af en vurdering af, hvad sandsynligheden er, for at en given hændelse (der kan resultere i et sikkerhedsbrud) rammer et system og en behandling, samt hvilke konsekvenser det vil kunne give for den registrerede.

En hændelse er den forekomst eller ændring af en bestemt række omstændigheder, der kan forårsage et sikkerhedsbrud. Derfor kaldes en hændelse ofte for et brud eller et uheld. Hændelser kan resultere i enten tab af fortrolighed, integritet og/eller tilgængelighed:

Tab af fortrolighed: Processens fortrolighed er truet pga. hændelsen; uautoriserede kan få viden om data i processen, som de ikke har ret til.

Tab af integritet: Processens integritet er kompromitteret pga. hændelsen og der kan ske uautoriserede ændringer af data, der betyder, at oplysningerne ikke er præcise/korrekte og fuldstændige.

Tab af tilgængelighed: Tilgængeligheden til processen for autoriserede brugere er truet pga. hændelsen og oplysningerne kan ikke tilgås af de autoriserede brugere på de tidspunkter hvor der ønskes adgang til data.

Vurdering af konskvens:

Til vurdering af konsekvensensen (altså hvad det ville betyde for den registrerede hvis der fx sker et tab af fortrolighed) kan skemaerne "Personoplysningernes karakter" og "Konsekvenser for registrerede" under fanen "2d. Grundlag for vurdering" anvendes. Personoplysningernes karakter (altså om der er tale om fx fortrolige eller følsomme personoplysninger) har umiddelbart størst betydning når fortroligheden vurderes, da det antages det vil have større konsekvenser for den registrerede hvis fx kreditkort oplysninger og/eller helbredsoplysninger blev lækket end hvis navn og email adresse blev lækket. Dog er skal der altid tages en konkret vurdering, da der altid er undtagelser til reglen.

Når konsekvensen skal vurderes, skal der altid tages udgangspunkt i "worst case scenario". Altså hvad er den værst tænkelige konsekvens for den registrerede ved tab af fortrolighed. I kolonnen "Konsekvenstype" vælges den konsekvens som anses som værende størst herunder om det er privatlivrettigheder, frihedsrettigheder, fysisk sikkerhed eller børn.

Vurdering af sandsynlighed:

Til vurdering af sandsynligheden kan skemaet "Hændelser der kan udløse risici for registrerede" under fanen "2d. Grundlag for vurdering" anvendes. Her findes der en række eksempler på forskellige hændelser som kan påvirke hhv. fortrolighed, integritet og tilgængelighed. Disse eksempler kan anvendes når sandsynligheden skal vurderes. De hændelser som vurderes værende mest sandsynlige skrives ind i kommentarfeltet "årsagsforklaring til sandsynlighed" under fanen "2c. Personrisikovurdering" og der sættes et "x" ud fra 1-4 alt efter hvor sandsynlig hændelsen vurderes. Skemaet "Sandsynlighed" under fanen 2d. Grundlag for vurdering", kan anvendes som inspiration til vurdering af sandsynligheden.

Se eksempel på vurdering på næste side:

Vurdering af sandsynlighed

			Fortrolighed Registreredes fortrolighed er truet; personoplysninger er ikke korrekt beskyttet mod uautoriseret udbredelse og anvendelse.									Integritet Registreredes integritet er kompromitteret; der kan ske uautoriserede ændringer der betyder, at oplysningerne ikke er præcisere/korrekte og fuldstændige.									Tilgængelighed Tilgængeligheden til registreredes oplysninger for autoriserede brugere er truet; oplysningerne kan ikke tilgås af de autoriserede brugere på ønskede tidspunkter.								
Systemer	**Klassifikation af personoplysninger**	**Evt. note**	**Konsekvens**				**Konsekvenstype**	**Sandsynlighed**				**Årsagsforklaring til sandsynlighed**	**Konsekvens**				**Konsekvenstype**	**Sandsynlighed**				**Årsagsforklaring til sandsynlighed**	**Konsekvens**				**Konsekvenstype**	**Sandsynlighed**				**Årsagsforklaring til sandsynlighed**
			1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4		1	2	3	4	
Mail system	Følsom					X	Privatlivs-rettigheder				X	Uvedkommende og uretmæssig adgang til personoplysningerne pga. manglende kryptering	X				Privatlivs-rettigheder		X			Utilsigtet ændring af oplysninger. Vil altid blive opdaget hurtigt og rettet.		X			Frihedsrettigheder	X				Utilsigtet sletning. Vil dog altid kunne genskabes hurtigt fra back up.
Økonomi system	Alm., fortrolig				X		Privatlivs-rettigheder			X		Uvedkommende og uretmæssig adgang til personoplysningerne pga. manglende adgangsbegrænsning		X			Frihedsrettigheder			X		Utilsigtet ændring af fx lønoplysninger pga. manglende adgangsbegrænsning.			X		Frihedsrettigheder	X				Utilsigtet sletning. Vil dog altid kunne genskabes hurtigt fra back up.

2e. Risikomatrix

Under fanen ”2e. Risikomatrix” kan den samlede risikovurdering aflæses. Såfremt der er vurderinger på 9 eller derover er der vurderet en høj risiko ved behandlingen i systemet og der skal derfor foretages en vurdering af, om der bør udarbejdes en konsekvensanalyse (DPIA).

Systemer & Applikationers samlet risiko			
System	**Fortrolighed**	**Intigritet**	**Tilgængelighed**
Mail system	16	2	2
Økonomi system	9	6	6

3a. Services og ydelser

Formålet med denne fane er at få registreret de leverandører/samarbejdspartnere, som ikke er system- eller applikationsleverandører. Overordnet er fanen opdelt i to hovedområder, som er beskrevet nedenfor:

Services og ydelser – Forretningsansvarlig

Først og fremmest skal alle services og ydelser, der anvendes inden for forretningsområdet, samt leverandøren eller samarbejdspartneren, angives. Dernæst skal der angives en dataejer, samt de processer servicen eller ydelsen er en del af – på samme måde som under fanen ”2a. Systemer” (se evt. afsnittet herfor i vejledningen).

Juridisk grundlag – Juridisk afdeling

Under det juridiske grundlag skal det juridiske ansvar for de behandlede personoplysninger angives, dvs. om jeres rolle er dataansvarlig, databehandler, eller om ansvaret er delt, samt om der er indgået en databehandleraftale – på samme måde som under fanen ”2a. Systemer” (se eventuelt afsnittet herfor i vejledningen, for uddybning og forklaring af begreberne).

3b. Data(klassifikation) (services og ydelser)

Under fanen “Dataklassifikation af services og ydelser” skal alle de forskellige kategorier af personoplysninger, der behandles i forbindelse med servicen eller ydelsen, angives og klassificeres. På samme måde som under fanen til dataklassifikation af data i systemerne (2c) er der foruddefineret en række personoplysninger samt mulighed for at tilføje kategorier af personoplysninger manuelt. Se evt. afsnit ”2c. Dataklassifikation” for nærmere vejledning.

Succes skaber vi sammen ...