



Notat om Privacy Impact Analyze, Persondata analyse eller blot PIA



Indhold



Notat om Privacy Impact Analyze, Persondata analyse eller blot PIA.	1	Fase 1	5
Tanken bag modellen	2	Generel it-sikkerhed i fase 1 ...	6
Fase 0	2	Kvalitetskontrol for fase 1	7
Tidsplan	3	Revision af fase 1	7
Kvalitetskontrol for fase 0	3	Ansvarsfraskrivelse.....	8
Revision af fase 0	4		



Notat om Privacy Impact Analyze, Persondata Analyse, eller blot PIA

EU's opdaterede persondataforordning stiller nye krav til fonde og foreninger. Derfor har vi udviklet et enkelt, brugbart værktøj, som en hjælp til at identificere de områder, der kan give udfordringer.

Vi har bestræbt os på at gøre værktøjet så let anvendeligt og tilgængeligt som muligt, og for at sikre, at alle vores kunder er godt med, har vi valgt at stille redskabet gratis til rådighed.

Vi kan ikke give garantier - hverken i forhold til de kommende regler eller i forhold til om de oplysninger, som I lægger ind i systemet, er korrekte, fuldstændige eller retvisende.

Det er dog vores opfattelse, at værktøjet vil støtte jer i bestræbelserne på at kortlægge de udfordringer, som persondataforordningen giver, og (næsten) uanset hvordan de kommende regler udformes, vil det arbejde, som er lagt i værktøjet, kunne danne grundlag for den videre regelopfyldelse, enten i den form det foreligger eller ved tilføjelse af supplerende oplysninger.

Vores hensigt med at stille værktøjet til rådighed for jer er at give jer mulighed for at opfylde lovkravene uden at blive tyngt af overdrevne omkostninger til systemer. Vi håber, at I vil tage godt imod det.

Fortsat god arbejdslyst!

A handwritten signature in black ink, appearing to be 'MS' or similar initials.

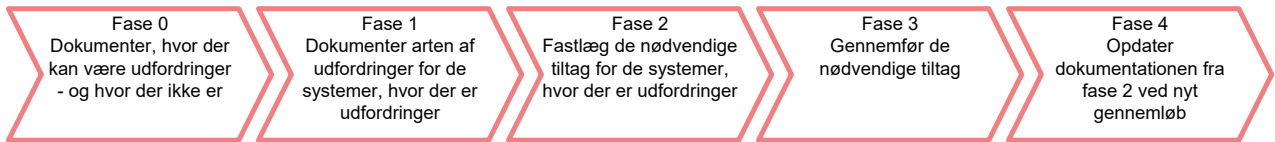
Martin Sørensen
statsautoriseret revisor



Tanken bag modellen

Der er to store udfordringer i forbindelse med opfyldelse af den kommende persondataforordning: At der endnu ikke er klarhed over reglernes fortolkning samt at der er forholdsvis kort tid til at implementere en løsning.

Derfor har vi fundet det nødvendigt med en faseopdelt tilgang, hvor udfordringerne hurtigt isoleres på overordnet niveau, således at problemløsningen kan iværksættes tidligst muligt. Vi opdeler processen i 5 faser, og vores værktøj er tænkt til faserne 0¹ og 1 samt til fase 4.



Figur 1 - Overordnet fasefordeling

Fase 0

Fase 0 omfatter dokumentation af, hvilke systemer, der eksisterer. Bemærk, at det er nødvendigt at vurdere alle systemer, og ikke blot systemer, som er i aktuel anvendelse. Regnearksmodellen "PIA-0, Systemoversigt" svarer til denne fase.

	A	B	C	D	E	F	G	H
1								
2	1 Kontorsystemer omfatter de standardprogrammer, som anvendes til generelt sekretærarbejde							
3	Kontorsystemer omfatter de standardprogrammer, som anvendes til generelt sekretærarbejde							
4								
5	Indeks	Systemets kaldenavn	Formål	Umiddelbar vurdering	Formelt navn	Leverandør	Driftes hos	Data lagres hos
6	1.1	Word	Tekstbehandling	Kan behandle persondata	MS Word	Microsoft	Internt	Data lagres c:/doku
7	5.2	Excel	kontaktoplysninger for medarbejdere	Kan behandle persondata	Side 1.1	Intern	Internt	Data lagres ikke
8	1.3	Power Point	Præsentationer	Behandler næppe persondata	MS PowerPoint	Microsoft	Os selv	Egne drev Bærbare medier Dokufix * One Drive
9	1.4	Word 365		Ikke vurderet				
10				Ikke vurderet				
11				Ikke vurderet				
12				Ikke vurderet				
13				Ikke vurderet				

Figur 2 Eksempel på fanen Kontorsystemer i arket "PIA-0, Systemoversigt"

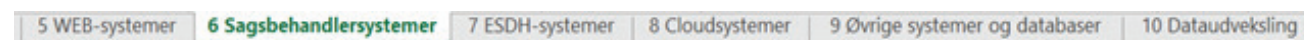
¹ Fase 0 er egentlig ikke en del af processen og vil ikke være nødvendig i alle forløb. Det er dog vores vurdering, at fasen vil være et nødvendigt forarbejde i mange organisationer. Derfor er Fasen betegnet 0.



Tanken bag modellen

I mange organisationer opretholdes udfasede systemer (fx udfasede medlemssystemer eller sikkerhedskopier af data herfra) der kan indeholde persondata. Også disse systemer er omfattet af forordningen.

For at hjælpe vores kunder til "at få det hele med", har vi valgt at prædefinere et antal faneblade, som vil være almindeligt forekommende, jf. nedenfor.



Figur 3 eksempel på faner i arket "PIA-0, Systemoversigt"

Faneinddelingen er ikke udtømmende, og nogle steder vil der være andre systemgrupper, som ikke er medtaget eller passer ind i eksisterende faner. Når dette forekommer, er der behov for at indsætte yderligere faner. Dette sker naturligvis blot ved de almindelige regnearksfunktioner ved at kopiere en eksisterende fane og tilrette navne mv.

Det skal endelig huskes, at EU's persondataforordning også gælder for manuelle arkiver. Hvis I har bevaret gamle fysiske kartoteker eller arkiver, så er de faktisk også omfattet af lovgivningen og skal indgå i vurderingen. Vi har ikke taget en fane med til disse arkiver, men modellen tilpasses i den konkrete situation ved indsættelse af en ekstra fane, som for eksempel kan betegnes "Fysiske arkiver", "Gamle Kartotekskort" eller en anden betegnelse, som måtte være relevant.

Tidsplan

Det er et naturligt led i fase 0 at etablere en tidsplan for opgaven. Tidsplanen vil afhænge af mange individuelle forhold, og vi stiller derfor ikke en generel tidsplan til rådighed. Vi deltager til gengæld gerne i arbejdet med udarbejdelse af en individuel tidsplan.

Kvalitetskontrol for fase 0

Vi anser det for naturligt, at ansvaret for at arket udfyldes tildeles en medarbejder med indsigt, men vi opfatter det lige så naturligt, at alle organisationens afdelinger modtager arkene og gennemgår samt supplerer med systemer, som måtte være glemt i første udfyldelse.



Tanken bag modellen

Revision af fase 0

Vi finder det naturligt, hvis bestyrelse eller daglig ledelse ønsker en objektiv tilbagemelding på arbejdets tilrettelæggelse og fremdrift. Blandt de emner som kunne være interessante, er

- Tilstedeværelse af en realistisk tidsplan
- Overholdelse af tidsplanens milepæle
- Kvaliteten i det foretagne arbejde herunder, hvorvidt de foretagne vurderinger er rimelige
- Omfanget af det udførte arbejde herunder, hvorvidt oversigter mv. forekommer at være tilstrækkeligt gennemarbejdede.

Omkostningen til en revisionsmæssig gennemgang vil variere i forhold til den anvendte tid, og vil blive gennemført ved gennemlæsning, interview, samt - i mindre omfang - ved selvstændige undersøgelser.

Tanken bag modellen

Fase 1

Fase 1 omfatter dokumentation af arten af udfordringer samt hvilke systemer, som berøres af disse udfordringer. Udgangspunktet er regnearket fra fase 0, og der oprettes et nyt ark for hver fane i arket "PIA-0, Systemoversigt", således at der er overensstemmelse imellem beskrivelserne i "PIA-0" og "PIA-1".

5 WEB-systemer	6 Sagsbehandlersystemer	7 ESDH-systemer	8 Cloudsystemer	9 Øvrige systemer og databaser	10 Dataudveksling
----------------	--------------------------------	-----------------	-----------------	--------------------------------	-------------------

Figur 4 Eksempel på faner i arket "PIA-0, Systemoversigt"

Hvor det var nødvendigt at inddrage alle systemer i fase 0, så omfatter fase 1 kun de systemer, hvor det er vurderet at der behandles persondata. Dette betyder, at der ikke bruges tid på systemer, hvor det i den indledende fase er fastslået, at systemgrupper, der ikke behandler persondata, udelades. Regnearksmodellen "PIA-1, xxxxxxxxxx" anvendes til denne fase.

	1.1 MS Word	
	Generelt	
	Hvem har udviklet systemet/hvem servicerer systemet?	Microsoft
	Har udvikler/leverandør udleveret compliance anvisninger?	Nej
	Anvendes databaser i forbindelse med systemet?	Nej, ikke direkte (fletning med databaser behandles under disse databaser)
	Hvor driftes systemet?	
	Hvor lagres data fra systemet?	
	Hvilke personoplysninger vil blive behandlet i systemet?	I princippet kan alle persondatatyper indgå
	Kan persondata uddrages af systemet med eksisterende funktioner?	
	Hvordan er personoplysninger indsamlet?	Systemet anvendes til videreformidling af allerede indsamlede oplysninger. Systemet har ikke nogen for for egen indsamling af persondata
		Systemets persondata vurderes i forbindelse med de systemer, som er kilde til systemerne
	Med hvilken hjemmel behandles personoplysningerne?	IRR
	Er det kontrolleret, at systemet kun opbevarer data, som er nødvendige for at opfylde formålet?	IRR
	Er det sikkert, at data ikke anvendes til andre formål?	IRR
	Oplysninger om dataindsamlingen?	
	Var datasubjektet orienteret før personoplysningerne blev indsamlet?	IRR
	Hvordan informeres datasubjekterne om databehandlingen?	IRR
	Anvises datasubjektet et kontaktpunkt for dataindsigt, klage, tilbagetrækning af samtykke mv?	IRR

Figur 5 Eksempel på systemfane i "PIA-1, Kontorsystemer"



Tanken bag modellen

I dette ark oprettes en fane for hvert system (se eksempel på en PIA-1, Kontorsystemer ovenfor). Arket indeholder en masterside med en række relevante spørgsmål, som skal besvares for hvert system. Omfanget af dette arbejde vil naturligvis svinge med omfanget af den konkrete it-anvendelse.

Det er vores opfattelse, at tidsforbruget for udfyldelse af de allerfleste systemer kan måles i minutter, men for nogle systemer vil tidsforbruget være større.

Generel it-sikkerhed i fase 1

Under udfyldelse af skemaerne i "PIA-1, xxxxxxxx" kan iagttages et afsnit om databeskyttelse. Dette afsnit indeholder spørgsmål om den individuelle sikring af persondata for det konkrete system, jf. figur 6.

Databeskyttelse	
Findes en sikkerhedsorganisation, som undersøger og sikrer systemets eventuelle persondata?	Nej
Foretages sikkerhedsvurderinger og anvendes en standard, som sikrer, at sikkerhedsvurderingerne omfatter al it i organisationen?	Nej
Er alle områder med systemets persondata sikret med en form for fysisk adgangskontrol?	Der er adgangskontrol til fysiske og logiske servere. Der er almindelig adgang til arbejdsstationer
Er brugeres rettigheder og adgang til systemets data opdelt efter behov, og bliver rettigheder styret og periodisk kontrolleret?	Adgang tildeles på baggrund af medarbejderens afdelingstilhør
Foretages der sikkerhedsopdateringer af det udstyr (servere, programmer, firewalls mv.), som systemet er afhængigt af?	Ja
Logges adgang til personoplysninger i systemet?	Nej
Er der adgang til systemets personoplysninger fra bærbart udstyr?	Ja
Kan data beskyttes ved at anonymisere personoplysninger?	Nej
Slettes systemets data, når de ikke længere er nødvendige i henhold til indsamlingsformålet eller som dokumentation for finansielle transaktioner?	Nej
Skal systemets databehandling anmeldes til myndighederne?	Sandsynligvis ikke - bør undersøges af advokat

Figur 6 Beskrivelse af databeskyttelse i "PIA-1, Kontorsystemer"



Tanken bag modellen

Nogle af disse oplysninger skal muligvis skaffes hos andre end organisationen selv, fx fra eksterne databehandlere, mens andre kræver inddragelse af egne generelle kontroller.

Spørgsmålene er udformet således, at de bør kunne besvares forholdsvis hurtigt, men det må være helt klart for alle, at der ikke er tale om en fyldestgørende gennemgang af generelle kontroller.

Kvalitetskontrol for fase 1

Ligesom i fase 0 anser vi det for naturligt, at ansvaret for at arket udfyldes tildeles en medarbejder med indsigt, ligesom vi opfatter det som naturligt, at alle organisationens afdelinger modtager arkene og gennemgår de anførte vurderinger.

Revision af fase 1

Organisationens ledelse kan også ønske en objektiv tilbagemelding om tilrettelæggelse og fremdrift af fase 1.

Blandt de emner, som kunne være interessante, er

- Overholdelse af tidsplanens milepæle
- Kvaliteten i det foretagne arbejde, herunder hvorvidt de foretagne vurderinger er rimelige
- Omfanget af det udførte arbejde, herunder hvorvidt oversigter mv. forekommer at være tilstrækkeligt gennemarbejdet
- Grundlaget for vurderinger af databehandlers kontroller i forbindelse med persondatahåndteringen

Vores rapportering for fase 1 vil ske på grundlag af gennemlæsning af dokumentation, interview samt i mindre omfang ved selvstændige undersøgelser.

Omkostningen til en revisionsmæssig gennemgang vil som altid variere med den anvendte tid.



Ansvarsfraskrivelse

Nærværende analyseværktøj er udarbejdet af Ri Statsautoriseret Revisionsaktieselskab (Ri), til brug for vurdering af behovet for de i EU's forordning om beskyttelse af persondata krævede Personal data Impact Assessment (PIA). Værktøjet er udarbejdet på baggrund af vores aktuelle analyser af regelsættet. Ri forbeholder sig ret til at ændre værktøjet som følge af blandt andet (men ikke indskrænket til) ændringer i reguleringen, indvundne erfaringer eller ændringer i generel konsensus på området.

Værktøjet stilles til rådighed "as is", og Ri forbeholder sig ret til på timebasis at fakturere kundebestemte forandringer, tilpasninger eller andet tidsforbrug.

Beslutning om anvendelse af værktøjet træffes efter anvenderens ledelses vurdering af egnethed og tilstrækkelighed, og Ri kan ikke gøres ansvarlig for modellens anvendelse eller tilstrækkelige udfyldelse i tilfælde, hvor vi ikke har forsynet analysen med vores erklæring. Ri kan heller ikke tage ansvar for eventuelle virkninger af modellens eventuelle senere ændringer eller tilpasninger eller for fremtidige ændringer i reguleringen, indvundne erfaringer eller ændringer i generel konsensus på området, herunder i danske særregler, i praksis for analyser af denne type.

Anvendelse af værktøjet sker på anvenderens eget ansvar.

København, den 21. april 2017

Ri Statsautoriseret Revisionsaktieselskab