

# Interviewskema

## Udgangspunkt

### Interviewskemaet tager udgangspunkt i publikation fra DI

Denne publikation har til formål at være en let tilgængelig vejledning i, hvordan virksomheder kortlægger konsekvenser for privatlivet ved digital behandling af personoplysninger og iværksætter tiltag til beskyttelse og kontrol af beskyttelse af privatlivets fred.

En sådan kortlægning kaldes en Privacy Impact Assessment (PIA)



# Interviewskema

## Hvorfor kortlægning af persondata

### Hvorfor bør man kortlægge sine persondatadata

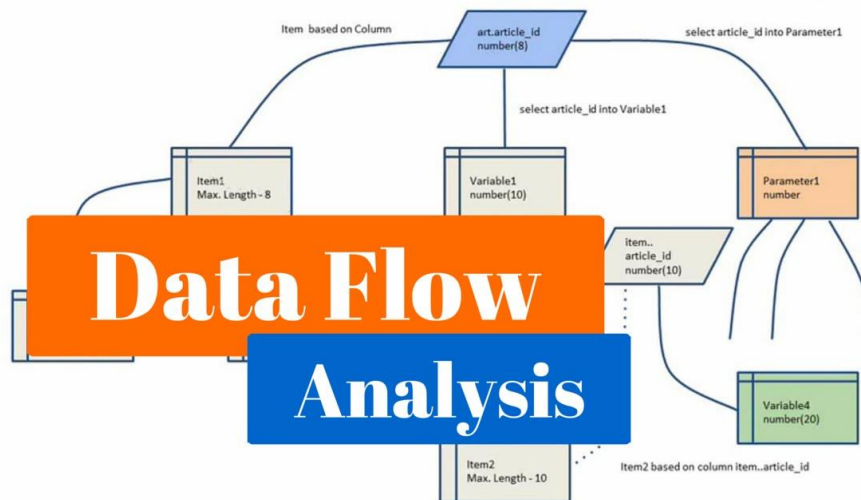
1. For det første vil signalet om at der samles så få personoplysninger ind som muligt, at de behandles så lidt som muligt af så få som muligt og sikres bedst muligt, skabe tillid hos individerne og dermed flere kunder.
2. For det andet skabes der med en PIA mulighed for at tekniske løsninger, der beskytter privacy, designes ind i it-systemerne, hvilket er langt billigere end at bygge dem på efterfølgende. Det er dermed omkostningsminimerende at lave en PIA.
3. For det tredje kan man bedre styre risici for problemer med behandling af personoplysninger, når man har en PIA.
4. For det fjerde mindskes sandsynligheden for databrud og dermed for tab af trust og omdømme.
5. For det femte er det lettere at sikre compliance med en given lovgivning.



# Interviewskema

## Dataflowanalyse

Det første, man skal give sig i kast med, er en dataflowanalyse. Dataflowanalyse er normalt en videnskabelig disciplin, der beskæftiger sig med, hvordan data flyder igennem og imellem funktioner i en applikation, med det formål at optimere applikationens performance. I denne sammenhæng har dataflowanalyse til formål at kortlægge, hvilke personoplysninger, som kommer ind i organisationen, hvordan, hvorfor, hvilken behandling der finder sted, og hvem der har adgang til personoplysningerne.





# Interviewskema

## Spørgeskema: Dataflow

Dataanalyse					
	Område:	System / Proces 1	System / Proces 2	System / Proces 3	System / Proces 4
	Dato:	Dato	Dato	Dato	Dato
	Interviewperson(er):	Navn	Navn	Navn	Navn
	Udfyldt af:	Navn	Navn	Navn	Navn
Dataflow					
1	Hvilke persondata bruges i dit område? (noter på liste)	se faneblad "Personoplysninger"	se faneblad "Personoplysninger"	se faneblad "Personoplysninger"	se faneblad "Personoplysninger"
2	Hvilke typer af teknologier anvendes?	(f.eks. databaser, webportaler, sociale medier, biometri, RFID eller TV-overvågning)	(f.eks. databaser, webportaler, sociale medier, biometri, RFID eller TV-overvågning)	(f.eks. databaser, webportaler, sociale medier, biometri, RFID eller TV-overvågning)	(f.eks. databaser, webportaler, sociale medier, biometri, RFID eller TV-overvågning)
3	Hvordan foregår indsamlingen af personoplysninger?	(f.eks. egne eksisterende data, data fra individ, tracking data eller data fra tredjepart)	(f.eks. egne eksisterende data, data fra individ, tracking data eller data fra tredjepart)	(f.eks. egne eksisterende data, data fra individ, tracking data eller data fra tredjepart)	(f.eks. egne eksisterende data, data fra individ, tracking data eller data fra tredjepart)
4	Til hvilket formål behandles personoplysningerne?	(f.eks. kreditering, udsendelse af nyhedsbrev, fremsendelse af varer eller profilering)	(f.eks. kreditering, udsendelse af nyhedsbrev, fremsendelse af varer eller profilering)	(f.eks. kreditering, udsendelse af nyhedsbrev, fremsendelse af varer eller profilering)	(f.eks. kreditering, udsendelse af nyhedsbrev, fremsendelse af varer eller profilering)
5	Sikres det at der ikke indsamles flere data end formålet tilsiger?	(begrundelse)	(begrundelse)	(begrundelse)	(begrundelse)
6	Sikres det at data ikke anvendes til andre formål?	(begrundelse)	(begrundelse)	(begrundelse)	(begrundelse)
7	Er det nødvendigt at indhente samtykke til databehandlingen?	(beskrivelse og begrundelse)	(beskrivelse og begrundelse)	(beskrivelse og begrundelse)	(beskrivelse og begrundelse)
8	Hvilken behandling finder sted?	(f.eks. indsamling, læsning, redigering, beregning, sammenstilling, videregivelse, opbevaring eller sletning)	(f.eks. indsamling, læsning, redigering, beregning, sammenstilling, videregivelse, opbevaring eller sletning)	(f.eks. indsamling, læsning, redigering, beregning, sammenstilling, videregivelse, opbevaring eller sletning)	(f.eks. indsamling, læsning, redigering, beregning, sammenstilling, videregivelse, opbevaring eller sletning)
9	Hvem har adgang til data?	(f.eks. hvilke personalegrupper, hvilke outsourcingpartnere eller indvilderne selv)	(f.eks. hvilke personalegrupper, hvilke outsourcingpartnere eller indvilderne selv)	(f.eks. hvilke personalegrupper, hvilke outsourcingpartnere eller indvilderne selv)	(f.eks. hvilke personalegrupper, hvilke outsourcingpartnere eller indvilderne selv)
10	Hvem har ansvaret for personoplysningernes sikkerhed?	(f.eks. data- og systemejer)	(f.eks. data- og systemejer)	(f.eks. data- og systemejer)	(f.eks. data- og systemejer)
11	Hvordan ser dataflowet ud efter personoplysninger er indsamlet?	(f.eks. kan man tegne et flowdiagram over, hvor personoplysninger lagres, hvem der kan tilgå personoplysningerne og hvordan, hvordan det sikres, at de ikke bruges til andre)	(f.eks. kan man tegne et flowdiagram over, hvor personoplysninger lagres, hvem der kan tilgå personoplysningerne og hvordan, hvordan det sikres, at de ikke bruges til andre)	(f.eks. kan man tegne et flowdiagram over, hvor personoplysninger lagres, hvem der kan tilgå personoplysningerne og hvordan, hvordan det sikres, at de ikke bruges til andre)	(f.eks. kan man tegne et flowdiagram over, hvor personoplysninger lagres, hvem der kan tilgå personoplysningerne og hvordan, hvordan det sikres, at de ikke bruges til andre)
12	Hvordan organiseres personoplysningerne? F.eks. Kundenr eller nummer relateret til et andet IT system (f.eks. CPR nr)	(f.eks. kundennummer eller nummer relateret til et andet it-system (f.eks. CPR-nummer))	(f.eks. kundennummer eller nummer relateret til et andet it-system (f.eks. CPR-nummer))	(f.eks. kundennummer eller nummer relateret til et andet it-system (f.eks. CPR-nummer))	(f.eks. kundennummer eller nummer relateret til et andet it-system (f.eks. CPR-nummer))
13	Videregives oplysningerne til andre?	(f.eks. andre interne systemer, eksterne it-leverandører, eksterne samarbejdspartnere eller offentliggørelse)	(f.eks. andre interne systemer, eksterne it-leverandører, eksterne samarbejdspartnere eller offentliggørelse)	(f.eks. andre interne systemer, eksterne it-leverandører, eksterne samarbejdspartnere eller offentliggørelse)	(f.eks. andre interne systemer, eksterne it-leverandører, eksterne samarbejdspartnere eller offentliggørelse)

# Interviewskema

## Spørgeskema: Risici

Behandlingen af personoplysninger kan ud fra datasubjekternes synspunkt være risikabel, fordi de kan få afsløret forhold, som de ikke ønsker at få afsløret. Man skal bemærke, at det er meget individuelt, hvilken risiko datasubjekterne tillægger behandling af personoplysninger. Køb af en roman kan være ok, men køb af koranen eller bibelen kan betragtes som risikabelt. Køb af en tv-serie kan være ok, men køb af en pornofilm kan være risikabelt. Afgivelse af personoplysninger kan være ok i en sammenhæng, men hvis de sammenstilles med personoplysninger fra en anden sammenhæng, kan det være risikabelt.





# Interviewskema

## Spørgeskema: Risici

Risici					
1	Vedrører den behandling af personoplysninger der sker forhold som datasubjektet vil betragte som følsomme?	<i>(f.eks. politik, religion, helbred, relationer, arbejdssituation, sex, økonomi, medlemskab eller lokation) (begrundelse)</i>	<i>(f.eks. politik, religion, helbred, relationer, arbejdssituation, sex, økonomi, medlemskab eller lokation) (begrundelse)</i>	<i>(f.eks. politik, religion, helbred, relationer, arbejdssituation, sex, økonomi, medlemskab eller lokation) (begrundelse)</i>	<i>(f.eks. politik, religion, helbred, relationer, arbejdssituation, sex, økonomi, medlemskab eller lokation) (begrundelse)</i>
2	Indgår der behandling af kreditkortoplysninger	<i>(beskrivelse og begrundelse)</i>	<i>(beskrivelse og begrundelse)</i>	<i>(beskrivelse og begrundelse)</i>	<i>(beskrivelse og begrundelse)</i>
3	Fremtræder behandlingen af personoplysninger troværdigt? F.eks. sikker transaktion, opbevaring af oplysningen	<i>(f.eks. virker transaktionen sikker, virker efterfølgende opbevaring af personoplysninger sikker) (beskrivelse og begrundelse)</i>	<i>(f.eks. virker transaktionen sikker, virker efterfølgende opbevaring af personoplysninger sikker) (beskrivelse og begrundelse)</i>	<i>(f.eks. virker transaktionen sikker, virker efterfølgende opbevaring af personoplysninger sikker) (beskrivelse og begrundelse)</i>	<i>(f.eks. virker transaktionen sikker, virker efterfølgende opbevaring af personoplysninger sikker) (beskrivelse og begrundelse)</i>
4	Kan datasubjektet få indsigt i informationer om behandling af personoplysninger?	<i>(f.eks. formål, ret til klage, ret til at tilbagetrække samtykke) (beskrivelse og begrundelse)</i>	<i>(f.eks. formål, ret til klage, ret til at tilbagetrække samtykke) (beskrivelse og begrundelse)</i>	<i>(f.eks. formål, ret til klage, ret til at tilbagetrække samtykke) (beskrivelse og begrundelse)</i>	<i>(f.eks. formål, ret til klage, ret til at tilbagetrække samtykke) (beskrivelse og begrundelse)</i>
5	Er der risiko for at personoplysninger spredes til en for datasubjektet kreds af uvedkommende?	<i>(f.eks. hacking eller tyveri fra ansatte med adgang til data) (begrundelse)</i>	<i>(f.eks. hacking eller tyveri fra ansatte med adgang til data) (begrundelse)</i>	<i>(f.eks. hacking eller tyveri fra ansatte med adgang til data) (begrundelse)</i>	<i>(f.eks. hacking eller tyveri fra ansatte med adgang til data) (begrundelse)</i>
6	Er der risiko for at data bruges til andre formål end dem de er indsamlet til?	<i>(begrundelse)</i>	<i>(begrundelse)</i>	<i>(begrundelse)</i>	<i>(begrundelse)</i>
7	Kobles der personoplysninger fra flere kanaler om datasubjektet uden datasubjektets viden?	<i>(f.eks. flere selskaber i samme koncern eller data købt fra tredjeparter) (beskrivelse og begrundelse)</i>	<i>(f.eks. flere selskaber i samme koncern eller data købt fra tredjeparter) (beskrivelse og begrundelse)</i>	<i>(f.eks. flere selskaber i samme koncern eller data købt fra tredjeparter) (beskrivelse og begrundelse)</i>	<i>(f.eks. flere selskaber i samme koncern eller data købt fra tredjeparter) (beskrivelse og begrundelse)</i>
8	Kan der ske nogen skade på eller for datasubjektet hvis oplysningen kommer til uvedkommende?	<i>(f.eks. økonomiske konsekvenser, forfølgelse, stigmatisering eller indskrænket handlefrihed) (beskrivelse)</i>	<i>(f.eks. økonomiske konsekvenser, forfølgelse, stigmatisering eller indskrænket handlefrihed) (beskrivelse)</i>	<i>(f.eks. økonomiske konsekvenser, forfølgelse, stigmatisering eller indskrænket handlefrihed) (beskrivelse)</i>	<i>(f.eks. økonomiske konsekvenser, forfølgelse, stigmatisering eller indskrænket handlefrihed) (beskrivelse)</i>
9	Kan der ske utilsigtet ændring eller tilintetgørelse af personoplysningerne?	<i>(begrundelse)</i>	<i>(begrundelse)</i>	<i>(begrundelse)</i>	<i>(begrundelse)</i>
10	Hvor stor en del af datasubjekterne kan blive berørt?	<i>(beskrivelse)</i>	<i>(beskrivelse)</i>	<i>(beskrivelse)</i>	<i>(beskrivelse)</i>

# Interviewskema

## Spørgeskema: Korrigerende foranstaltninger

Man kan iværksætte korrigerende foranstaltninger for at beskytte personoplysninger. For det første kan man forsøge at sikre, at informationer ikke kan henføres til en person og altså være personoplysninger. I de tilfælde, hvor det ikke er en mulighed, må man sørge for at sikre personoplysningerne bedst muligt. Som udgangspunkt anbefales det at beskytte personoplysninger under anvendelse af en sikkerhedsstandard.







# Interviewskema

## Spørgeskema: Korrigerende foranstaltninger

Korrigerende foranstaltninger					
1	Er der en sikkerhedsorganisation, som har til opgave at sikre personoplysningernes fortrolighed, integritet og tilgængelighed?	(kort beskrivelse)	(kort beskrivelse)	(kort beskrivelse)	(kort beskrivelse)
2	Følges en sikkerhedsstandard, som sikrer, at sikkerhedsvurderingerne kommer hele vejen rundt om organisationen?	(f.eks. ISO27000 eller ISF) (kort beskrivelse)	(f.eks. ISO27000 eller ISF) (kort beskrivelse)	(f.eks. ISO27000 eller ISF) (kort beskrivelse)	(f.eks. ISO27000 eller ISF) (kort beskrivelse)
3	Er der fysisk adgangskontrol?	(Beskrivelse)	(Beskrivelse)	(Beskrivelse)	(Beskrivelse)
4	Er der styring af brugeres rettigheder og adgang?	(Beskrivelse)	(Beskrivelse)	(Beskrivelse)	(Beskrivelse)
5	Foretages der sikkerhedsopdateringer af styresystemer, databaser, m.v.?	(Beskrivelse)	(Beskrivelse)	(Beskrivelse)	(Beskrivelse)
6	Logges adgang til personoplysninger?	(Beskrivelse)	(Beskrivelse)	(Beskrivelse)	(Beskrivelse)
7	Er der adgang til personoplysninger fra bærbart udstyr?	(Beskrivelse)	(Beskrivelse)	(Beskrivelse)	(Beskrivelse)
8	Kan der implementeres teknologier, som pseudonymiserer eller anonymiserer personoplysninger?	(beskrivelse og begrundelse)	(beskrivelse og begrundelse)	(beskrivelse og begrundelse)	(beskrivelse og begrundelse)
9	Slettes eller anonymiseres data, når der ikke længere er brug for dem i henhold til formålet?	(Beskrivelse)	(Beskrivelse)	(Beskrivelse)	(Beskrivelse)
10	Er der behov for at foretage anmeldelse af databehandlingen til myndighederne?	(begrundelse og evt. dokumentation)	(begrundelse og evt. dokumentation)	(begrundelse og evt. dokumentation)	(begrundelse og evt. dokumentation)





# Interviewskema

## Spørgeskema: Information

Det skal overvejes i hvilket omfang datasubjekterne skal gøres opmærksom på, at virksomheden behandler personoplysninger. Herunder skal det også overvejes at sikre, at datasubjekterne har adgang til at ændre data og trække deres samtykke tilbage.





# Interviewskema

## Spørgeskema: Information

Information					
1	Var datasubjektet orienteret før indsamlingen af personoplysningerne fandt sted?	(beskrivelse og begrundelse)	(beskrivelse og begrundelse)	(beskrivelse og begrundelse)	(beskrivelse og begrundelse)
2	Har datasubjektet mulighed for at samtykke til eller at afvise at data behandles?	(beskrivelse og begrundelse)	(beskrivelse og begrundelse)	(beskrivelse og begrundelse)	(beskrivelse og begrundelse)
3	Hvordan informeres datasubjekterne?	(f.eks. e-mail, hjemmeside eller EULA) (beskrivelse)	(f.eks. e-mail, hjemmeside eller EULA) (beskrivelse)	(f.eks. e-mail, hjemmeside eller EULA) (beskrivelse)	(f.eks. e-mail, hjemmeside eller EULA) (beskrivelse)
4	Har datasubjekterne nogen grad af direkte kontrol med personoplysningerne?	(f.eks. mulighed for at se og rette data via webadgang) (beskrivelse og begrundelse)	(f.eks. mulighed for at se og rette data via webadgang) (beskrivelse og begrundelse)	(f.eks. mulighed for at se og rette data via webadgang) (beskrivelse og begrundelse)	(f.eks. mulighed for at se og rette data via webadgang) (beskrivelse og begrundelse)
5	Har datasubjekterne et kontaktpunkt som de kan henvende sig til hvis de har spørgsmål til behandling af personoplysninger?	(beskrivelse)	(beskrivelse)	(beskrivelse)	(beskrivelse)
6	Er der en procedure for at datasubjekterne kan trække samtykke for behandlingen af personoplysningerne tilbage?	(beskrivelse)	(beskrivelse)	(beskrivelse)	(beskrivelse)
7	Er der en procedure for at vurdere om datasubjekterne skal orienteres hvis deres data fortabes?	(f.eks. hvis data stjæles af en hacker) (beskrivelse)	(f.eks. hvis data stjæles af en hacker) (beskrivelse)	(f.eks. hvis data stjæles af en hacker) (beskrivelse)	(f.eks. hvis data stjæles af en hacker) (beskrivelse)



# Interviewskema

## Spørgsmål

