BRUKERVEILEDNING TIL TRINN 1 - Datakartlegging

Klarlegging av overordnet ansvar

Før kartleggingen av data går i gang, bør det avklares hvem – hvilken posisjon - som har det overordnete ansvaret i virksomheten for at personopplysninger blir håndtert i henhold til lovgivningen.

Det er et krav at en bestemt posisjon i virksomheten har ansvaret for håndteringen av personopplysninger. Normalt er dette øverste administrative leder, men det kan gjerne være fagpersoner eller mellomledere som i praksis er mer involvert i håndteringen av personopplysninger. Virksomheten står fritt til selv å bestemme hvilken posisjon som skal ha rollen.

Tips!

Den som har det overordnete ansvaret for personvern i virksomheten bør være aktivt involvert i arbeidet med dette personvernverktøyet. Ofte er det også hensiktsmessig at eventuelle andre personer som jobber med HR, IT og markedsføring i virksomheten er med i prosessen.

Kommentarer til utfylling av skjema for datakartlegging

Virksomheten må ha oversikt over hvilke personopplysninger virksomheten håndterer, på hvilken måte opplysningene brukes og til hvilke formål. Skjemaet i trinn 1 skal kartlegge dette. Spørsmålene er utarbeidet for at virksomheten skal få nødvendig oversikt. De gir også grunnlag for å avgjøre om virksomheten overholder de lovpålagte kravene for håndtering av personopplysninger. Dette vil bli nærmere vurdert i forbindelse med trinn 2 avviksanalyse.

Det fylles ut ett datakartleggingsskjema for hvert enkelt system der personopplysninger håndteres. For eksempel fylles det ut ett skjema for personalregisteret, ett for lønnssystemet, ett for epostsystemet, ett for filbehandlingssystem, ett for virksomhetens kundedatabase, ett for hvert av virksomhetens ulike manuelle arkiver etc. Har virksomheten tre ulike systemer, er skjemaet lagt opp slik at det totalt skal fylles ut tre skjemaer.

Dersom virksomheten ikke har noe svar på ett eller flere av spørsmålene i skjemaet, kan utfyllingsfeltet stå tomt. Da blir dette et oppfølgingspunkt i forbindelse med trinn 2) avviksanalyse.

Nedenfor er det tatt inn kommentarer fortløpende til de ulike spørsmålene i skjema for datakartlegging.

Dette skjemaet gjelder: [Fylles inn]	**Kommentarer til utfyllingen:**
Hvem i organisasjonen "eier"/har ansvar for systemet?	Fylles ut, hvis aktuelt.
Hvem gjelder opplysningene som er registrert i systemet? *For eksempel: Ansatte, tidligere ansatte, familie/nærstående, kunder, potensielle kunder, forretningskontakter eller andre.*	Fyll inn hovedkategorier, som vist i eksempelet.
Hva slags personopplysninger finnes i systemet? *Inneholder systemet sensitive eller konfidensielle opplysninger?*	De ulike personopplysningene som finnes beskrives overordnet. Spesielt sensitive/konfidensielle opplysninger beskrives mer detaljert.
Hvor er opplysningene hentet fra/hvordan er de samlet inn?	Angi om ansatte/andre legger inn de ulike opplysningene selv eller om opplysningene hentes fra tredjeparter, og i tilfelle hvem/hvor.
Hva er formålet med bruken av personopplysningene?	Beskriv overordnet. Formålet med personalregisteret er for eksempel personaladministrasjon.
Er personene som opplysningene gjelder informert om bruken av personopplysningene?	Fyll ut med ja eller nei. Hvis nei, blir dette et punkt for oppfølging i forbindelse med trinn 2) avviksanalyse.
Finnes rutiner for retting av opplysninger der det er behov for det? *Hvem er ansvarlig for at opplysningene er riktige og oppdaterte?*	Beskriv kort eventuelle eksisterende rutiner.
Utleveres personopplysningene til tredjeparter (utenfor virksomheten)? *Hvis ja: Hva er formålet med utleveringen?*	Beskriv kort eventuell utlevering, samt formål.

Dette skjemaet gjelder: [Fylles inn]	**Kommentarer til utfyllingen:**
Gis andre virksomheter tilgang til personopplysninger virksomheten har i forbindelse med oppgaver som skal utføres? *Hvis ja: Er det inngått avtale/finnes rutiner for inngåelse av avtale om dette (databehandleravtale)?*	Beskriv kort tilfeller der andre virksomheter gis tilgang til personopplysninger. Dette kan for eksempel være, hvis virksomheten har satt ut drifting av lønnssystemet til en tredjepart. Tredjeparter som håndterer personopplysninger på vegne av virksomheten, for eksempel leverandør av lønnssystem, er såkalt *databehandler*. Det er et krav at skriftlig databehandleravtale inngås mellom virksomheten og databehandleren. Fyll ut om slik avtale er inngått. Hvis slik avtale ikke er inngått, blir dette et punkt for oppfølging i forbindelse med trinn 2) avviksanalyse.
Sendes opplysninger ut av EU/EØS?	Fyll ut ja eller nei. Hvis ja, blir dette et punkt for oppfølging i forbindelse med trinn 2) avviksanalyse.
Er det gjort vurderinger av risiko knyttet til håndtering og bruk av personopplysningene (risikovurdering)?	Fyll ut ja eller nei. Hvis nei, blir dette et punkt for oppfølging i forbindelse med trinn 2) avviksanalyse.
Hvilke tiltak er etablert for å sikre personopplysningene? Er tiltakene dokumentert?	Beskriv eventuelle tiltak kort. Hvis ikke noen tiltak er etablert og/eller dokumentert, blir dette et punkt for oppfølging i forbindelse med trinn 2) avviksanalyse.
Finnes rutiner for håndtering av avvik, dvs. tilfeller der personopplysninger kommer på avveie, misbrukes eller lignende? Hvilke rutiner er etablert?	Beskriv eventuelle rutiner kort. Hvis ikke noen rutiner er etablert og/eller dokumentert, blir dette et punkt for oppfølging i forbindelse med trinn 2) avviksanalyse.

Dette skjemaet gjelder: [Fylles inn]	**Kommentarer til utfyllingen:**
Hvor lenge lagres opplysningene? *Hva er kriteriene for å slette opplysninger?* *Hvem bestemmer om/når opplysninger skal slettes?* *Hvordan foregår sletting?*	Beskriv kort. Hvis ikke sletterutiner finnes, blir dette et punkt for oppfølging i forbindelse med trinn 2) avviksanalyse.
Er det sendt melding til Datatilsynet om bruken av personopplysninger? *Alternativt: er det søkt om/gitt konsesjon?* - *Hvis nei: Er dette vurdert og hvorfor er melding/konsesjon evt ikke nødvendig?* - *Hvis ja: Er meldingen/konsesjonen oppdatert? Hvem er ansvarlig for at meldinger/konsesjoner holdes oppdatert, og hvordan gjøres dette?*	Beskriv kort. - Hvis dette ikke er vurdert, blir dette et punkt for oppfølging i forbindelse med trinn 2) avviksanalyse. - Hvis dette er gjort, men ikke er oppdatert, blir dette et punkt for oppfølging i forbindelse med trinn 2) avviksanalyse.
Er det etablert rutiner for å håndtere henvendelser fra personer som Virksomheten har opplysninger om? *Hva er rutinene for håndtering av slike henvendelser, inkludert ved:* - *Krav om tilgang til opplysninger* - *Krav om informasjon om bruk og håndtering av opplysninger* - *Krav om retting og/eller sletting av opplysninger*	Beskriv eventuelle rutiner kort. Hvis ingen rutiner er etablert og/eller dokumentert, blir dette et punkt for oppfølging i forbindelse med trinn 2) avviksanalyse.