Bliv klar til whistleblowerordningen for SME'er

GDPR-krav ved whistleblower-ordningen

28. februar 2024

pwc

Hvem er vi?

Catrine Søndergaard Byrne

Partner, PwC Legal, Employment, GDPR and Dataethics
E: catrine.sondergaard.byrne@pwc.com
T: 2448 9299

Fatih Gülhan

Associate, PwC Legal
E: fatih.guelhan@pwc.com
T: 2129 90362

Agenda

GDPR-krav ved whistleblowerordningen

1. Hvorfor er GDPR relevant ved whistleblowerordninger?
2. Dataansvarlig/databehandler-konstruktion i en whistleblowerordning
3. De grundlæggende principper
4. Informations- og dokumentationspligten
5. De registreredes rettigheder

Hvorfor er GDPR relevant ved whistleblowerordninger?

Hvem beskyttes af GDPR-reglerne?

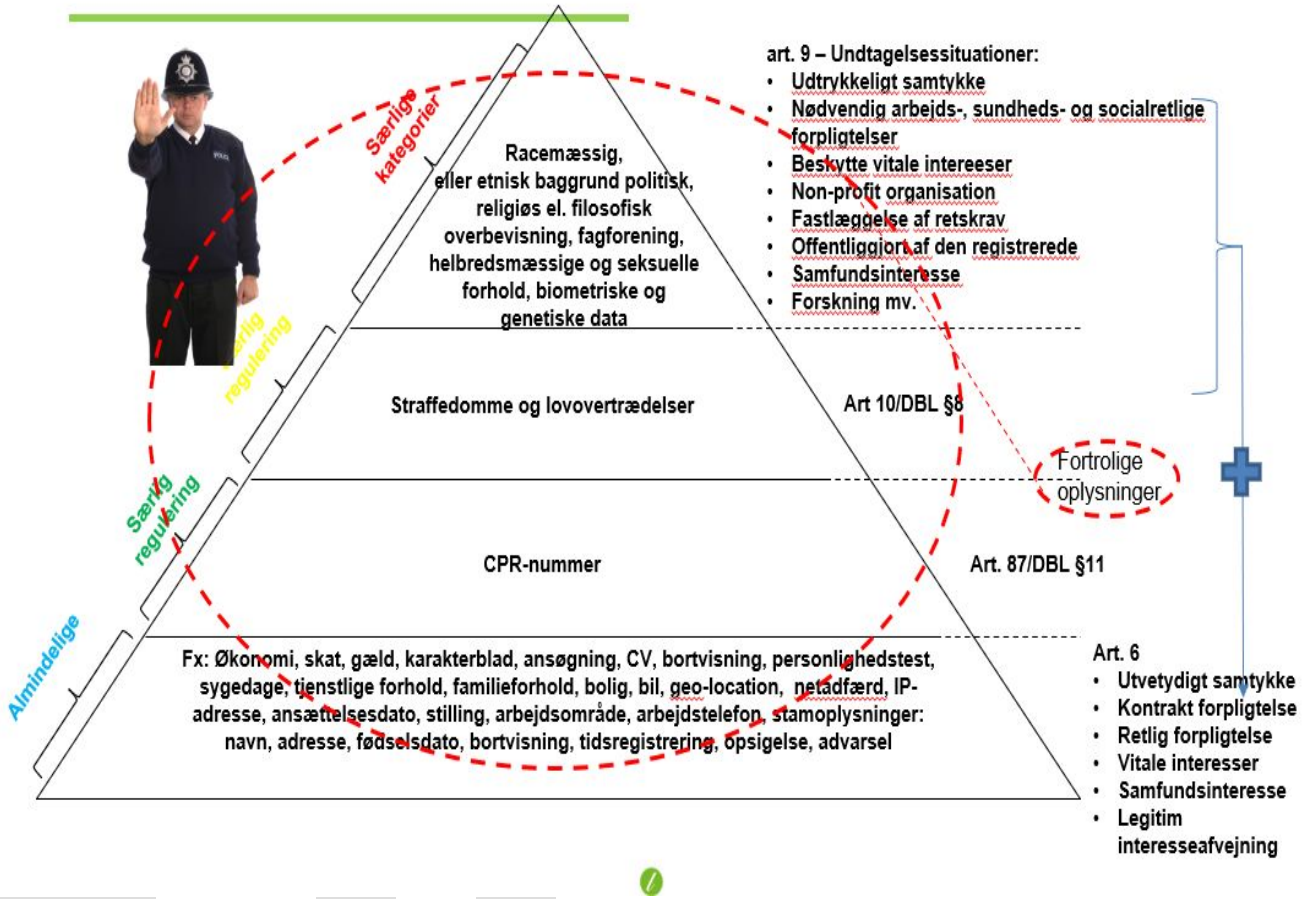
- Efter whistleblowerloven beskyttes ”whistleblowere”

- Efter GDPR-reglerne beskyttes fysiske personer (”de registrerede”)
  - Whistlebloweren
  - De(n) berørte
  - Involverede

Hvad er personoplysninger?

- Personoplysninger er enhver form for information, der kan relateres til en identificeret person, eller data der direkte eller indirekte kan identificere en person.
    - *Eller med andre ord: Al information, der kan identificere en bestemt person*
- Almindelige personoplysninger (ikke-følsomme personoplysninger)
- Særlige kategorier af personoplysninger (følsomme personoplysninger)
- Oplysninger om straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger

Hvad er personoplysninger?



- ”Personoplysninger” skal fortolkes bredt
- Novak-sagen
  - *”…skriftlig besvarelse, som en deltager har givet i forbindelse med en faglig prøve, og eksaminatorens eventuelle rettelser og kommentarer til denne besvarelse udgør personoplysninger i denne bestemmelses forstand”*

Hvad er en behandling?

Enhver form for håndtering af personoplysninger. Behandling kan fx være indsamling, registrering, systematisering, opbevaring og videregivelse, herunder offentliggørelse. Sletning af personoplysninger er også en behandling.

Hvordan behandles personoplysninger i en whistleblowerordning?

Behandling af personoplysninger må kun ske, hvis der er et behandlingsgrundlag, dvs. en hjemmel til behandlingen!

Behandlingshjemmel

- Man skal have hjemmel i forordningen, databeskyttelsesloven eller særlovgivningen, før man lovligt må behandle personoplysninger.

- Hvad er hjemmelen til at behandle personoplysninger ved whistleblowerordninger?

Dataansvarlig/ databehandler-konstruktion i en whistleblowerordning

Dataansvarlig og databehandler

- **Dataansvarlig:** ”en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.” (databeskyttelsesforordningens artikel 4, nr. 7).

- **Databehandler:** ”en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne”. (databeskyttelsesforordningens artikel 4, nr. 8).

- …og hvem er så hvad i en whistleblowerordning?

Dataansvarlig og databehandler

1. scenarie

En ”almindelig” administration af en whistleblowerordning, hvorved der menes, at en ekstern leverandør (whistleblowerадministrator) varetager følgende opgaver på vegne af en arbejdsgiver:

- Modtagelse af indberetninger fra whistleblowere via ”almindelige” kommunikationskanaler såsom e-mail, fysisk post, telefon og evt. fysisk fremmøde
- Vurdering af, om indberetningen falder inden for whistleblowerordningens anvendelsesområde (”scope”), og herefter videresende indberetningen til arbejdsgiveren, hvis den gør, og afvise indberetningen, hvis den ikke gør
- Varetagelse af al kommunikation med whistlebloweren, herunder at bekræfte modtagelsen af indberetningen, give feedback til whistlebloweren, mv.
- Om nødvendigt bistå arbejdsgiveren med rådgivning om, hvordan indberetningen bør håndteres”

Dataansvarlig og databehandler

2. scenarie

- Administration af whistleblowerordningen på samme måde som beskrevet under scenarie 1, dog med den tilføjelse, at whistlebloweradministratoren også stiller en it-platform (fx en hjemmeside) til rådighed, som kan fungere som indberetningskanal. Whistlebloweradministratoren kan enten selv stå for driften af denne platform, eller levere denne via en (under)leverandør.

Dataansvarlig og databehandler

3. scenarie

- Leverandøren stiller alene en it-platform til rådighed for den arbejdsgiver, der etablerer whistleblowerordningen. Det er leverandøren, der driver (hoster) platformen. Platformen kan anvendes til at indberette overtrædelser, men det er arbejdsgiverens egne medarbejdere, der tilgår platformen og behandle indberetningerne (dvs. arbejdsgiveren forestår opgaverne selv).

De grundlæggende principper

De grundlæggende principper

Databeskyttelsesrettens ”grundlov” – art. 5

Personoplysninger skal

A. behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede *(»lovlighed, rimelighed og gennemsigtighed*«)

B. indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål *(» formålsbegrænsning«)*

C. være korrekte og om nødvendigt ajourførte (»rigtighed«)

De grundlæggende principper

Databeskyttelsesrettens ”grundlov” – art. 5

D. opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles *(»opbevaringsbegrænsning«)*

E. behandles på en sikker måde (»integritet og fortrolighed«).

Stk. 2: Den dataansvarlige er ansvarlig for og skal påvise, at stk. 1 overholdes *(»ansvarlighed«)*

Dataminimering

GDPR art. 5(1)(c):

*(…) være tilstrækkelige, relevante og begrænset til, hvad der er **nødvendigt** i forhold til de formål, hvortil de behandles (»dataminimering«)*

- Oplysninger skal være nødvendige for undersøgelsen
- Hvordan identificeres ”nødvendige” personoplysninger
- Kontinuerlig ”oprydning” og klassificering
- Ingen fisketure

Rigtighed

GDPR art. 5(1)(d):

*.. der skal tages ethvert **rimeligt** skridt for at sikre, at personoplysninger, der er **urigtige i forhold til de formål, hvortil de behandles**, straks slettes eller berigtiges*

- Hvordan identificeres urigtige personoplysninger
- Kontinuerlig klassificering mhp. enten sletning eller berigtigelse
- Hvordan håndteres urigtige personoplysninger – skal de berigtiges, og i givet fald, hvordan

Vurdér løbende, hvordan det sikres, at oplysninger, der behandles i undersøgelsen, er korrekte (kan/skal anvendes til bevis?).

Vurdér løbende, om oplysninger skal ajourføres.

Rigtighed

W 07. JUL. 22

SAMFUND KULTUR BØGER IDEER

MeToo. Tidligere korpiger på Sankt Annæ siger, at de fejlagtigt blev udpeget som ofre og – forgæves – forlangte at blive skrevet ud af en advokatrapport.

Krænket på anden hånd

POUL PILGAARD JOHNSEN

Opbevaringsbegrænsning

GDPR art. 5(1)(d):

*(...) der skal tages ethvert **rimeligt** skridt for at sikre, at personoplysninger, der er **urigtige i forhold til de formål, hvortil de behandles**, straks slettes eller berigtiges*

GDPR art. 5(1)(e):

(...) opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles;

Hvor længe er det nødvendigt at identificere de registrerede?

- Beskriv slettepolitik fx baseret på persontyper og klassifikation af personoplysningen
- Hvornår skal oplysninger i en ”whistleblower-sag” slettes?

Sikkerhed og fortrolighed

GDPR art. 5(1)(f):

(...) behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger

GDPR art. 32:

Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant: (…)
2. Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til person oplysninger, der er transmitteret, opbevaret eller på anden måde behandlet

Sikkerhed og fortrolighed

Organisatoriske sikkerhedsforanstaltninger:

- Procesbeskrivelse med fokus på it-sikkerhed, div. politikker, instrukser, uddannelse, awareness

Tekniske sikkerhedsforanstaltninger:

- It-sikkerhed, krypteringsteknologier, sikring af anonymitet, ingen auto-complete i mailprogram, ingen transportable devices, adgangskontrol, uautoriseret videregivelse af data gemt i skabeloner/blanketter, etc.

Informations- og dokumentationspligten

Informationspligten

Sikring af transparens - informationspligt

(GDPR art. 13/14 og WBL §13 og §20)

Som led i undersøgelsesplanen addresseres hvordan informations- og underretningspligt skal opfyldes, eller hvorvidt der kan sker undtagelse fra informationspligten.

Afgørelser

- Datatilsynets afgørelse af den 3. februar 2022 (TV2)
- Datatilsynets afgørelse af den 6. september 2022 (KF)

Informationspligt

Iagttagelse af oplysningspligten

TV2: ”Behandlingens omfang, indgribende karakter og personoplysningernes alder stiller efter Datatilsynets opfattelse skærpede krav til oplysningernes klarhed og gennemsigtighed”.

KF: ”Det er herudover Datatilsynets opfattelse, at undersøgelsens omfang og karakter stiller skærpede krav til behandlingens gennemsigtighed, og dermed ligeledes klarheden af de informationer som klager burde have modtaget i forbindelse med undersøgelsens påbegyndelse”.

- Skal der udarbejdes en særskilt oplysningsskrivelse?
- Tidspunktet for iagttagelse af oplysningspligten?
- Gælder der et krav om løbende iagttagelse af oplysningspligten?

Dokumentationspligt

- Husk at opdatere GDPR-dokumentation jævnligt
- Du skal kunne påvise over for Datatilsynet, at du overholder reglerne og kravene. Hvis du ikke kan det, overholder du dem de facto ikke
- En whistleblowerhotline er en behandlingsaktivitet efter GDPR
- Krav om fortegnelse for behandlingsaktiviteter

De registreredes rettigheder

De registreredes rettigheder

Den registrerede har en række rettigheder til at kontrollere behandling af sine personoplysninger

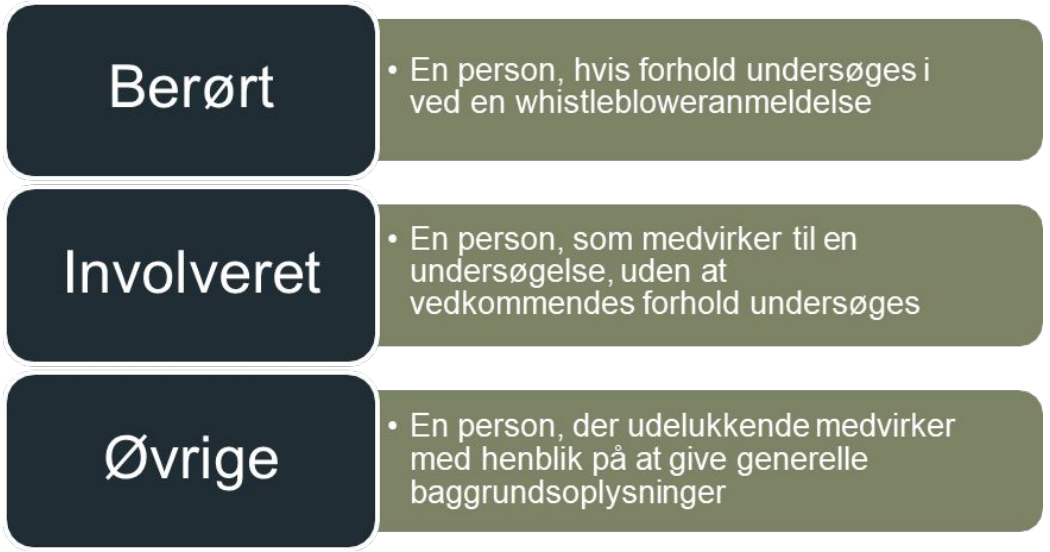
- Hvordan håndteres udnyttelse af rettighedskatalog?
  - Ret til indsigt (art. 15)
  - Ret til berigtigelse (art. 16)
  - Ret til sletning (retten til at blive glemt) (art. 17)
  - Ret til begrænsning af behandlingen (Forbudsbestemmelsen) (art. 18)
  - Ret til indsigelse til behandling efter art. 6, litra e) eller f) (art. 21)

Husk ovenstående ved oplysningspligten!

De registreredes rettigheder

- Der er forskellige rettigheder for forskellige persongrupper - klassificér dem
- De kan ændre sig undervejs
- Forsigtighedsprincip ved tvivl - behandl som berørt

Eksempler persongrupper:



Retten til indsigt

- De registrerede har ret til at anmode om og modtage en kopi af de personoplysninger, som den dataansvarlige eller databehandleren har om dem, samt yderligere oplysninger om behandlingen.
- …også ved en igangværende undersøgelse ?

Ret til berigtigelse

- De registrerede har ret til at anmode om, at urigtige eller ufuldstændige personoplysninger om dem bliver rettet eller suppleret.

- … også hvis den berørte er uenig i anklagerne?

Retten til sletning

- De registrerede har ret til at anmode om, at deres personoplysninger bliver slettet:
    - Hvis de ikke længere er nødvendige til det formål, de blev indsamlet til
    - Hvis de har trukket deres samtykke tilbage
    - Hvis de gør indsigelse mod behandlingen
    - Hvis behandlingen er ulovlig
    - Hvis der er en retlig forpligtelse til at slette dem.
- … kan den berørte 'bare' kræve oplysningerne slettet?

På gensyn

Husk at tilmelde dig et eller flere af de kommende webinarer og gense afholdte webcasts på

www.pwc.dk/whistleblower

Tak for i dag