

WP243 BILAG – OFTE STILLEDE SPØRGSMÅL

Formålet med dette bilag er at besvare, i et forenklet og letlæseligt format, nogle af de centrale spørgsmål, som organisationer eventuelt har med hensyn til de nye krav i databeskyttelsesforordningen om udpegelse af en databeskyttelsesrådgiver.

Udpegelse af databeskyttelsesrådgiveren (artikel 37)

1 Hvilke organisationer er forpligtet til at udpege en databeskyttelsesrådgiver? (artikel 37, stk. 1)

Den generelle databeskyttelsesforordning kræver udpegelse af en databeskyttelsesrådgiver i tre specifikke tilfælde:

- når behandlingen foretages af en offentlig myndighed eller et offentligt organ (uanset hvilke data, der behandles)
- når den dataansvarliges eller databehandlerens kerneaktiviteter kræver regelmæssig og systematisk overvågning af registrerede i stort omfang, og
- når den dataansvarliges eller databehandlerens kerneaktiviteter består af behandling i stort omfang af særlige kategorier af oplysninger, eller personoplysninger vedrørende straffedomme og lovovertrædelser.

Bemærk, at EU- eller medlemsstatslovgivning eventuelt også kan kræve udpegelse af databeskyttelsesrådgivere i andre situationer. Endelig, hvis databeskyttelsesforordningen ikke udtrykkeligt kræver udnævnelse af en databeskyttelsesrådgiver, kan organisationer undertiden finde det nyttigt at udpege en sådan rådgiver på frivillig basis. Artikel 29-gruppen vedrørende databeskyttelse tilskynder til denne frivillige indsats.

Se yderligere oplysninger i retningslinjernes afsnit 2.1.

2 Hvad betyder begrebet "kerneaktiviteter"? (artikel 37, stk. 1, litra b) og c))

"Kerneaktiviteter" kan betragtes som de centrale aktiviteter, der er nødvendige for at opnå den dataansvarliges eller databehandlerens mål. Disse omfatter alle aktiviteter, hvor databehandling udgør en uundgåelig del af den dataansvarliges eller databehandleres aktivitet. For eksempel skal behandling af sundhedsdata som patientjournaler betragtes som en af ethvert hospitals kerneaktiviteter, og hospitaler skal derfor udpege en databeskyttelsesrådgiver.

På den anden side har alle organisationer brug for at udføre visse støtteaktiviteter som for eksempel at betale deres ansatte eller bruge standardiseret databehandling som støtte i deres aktiviteter. Disse er nødvendige støttefunktioner for organisationens kerneaktiviteter eller hovedvirksomhed. Selvom disse aktiviteter er nødvendige eller vigtige, så betragtes de normalt som biaktiviteter snarere end kerneaktiviteter.

Se yderligere oplysninger i retningslinjernes afsnit 2.1.2.

3 Hvad betyder begrebet "i stort omfang"? (artikel 37, stk. 1, litra b) og c))

Databeskyttelsesforordningen definerer ikke, hvad der udgør et stort omfang. Artikel 29-gruppen anbefaler, at navnlig de følgende faktorer tages i betragtning, når det bestemmes, om der behandles data i stort omfang:

- antallet af registrerede, som behandles – enten som specifikt tal eller som en procentdel af den relevante befolkningsgruppe
- mængden af data og/eller omfanget af forskellige datatyper, som behandles
- databehandlingsaktivitetens varighed eller permanens
- databehandlingsaktivitetens geografiske udstrækning.

Eksempler på databehandling i stort omfang inkluderer:

- behandling af patientdata i forbindelse med den almindelige forretningsgang på et hospital
- behandling af rejsedata for personer, som benytter en bys offentlige transportsystem (f.eks. sporing via rejsekort)
- behandling af kunders geolokaliseringsdata i realtid i en international fastfood-kæde til statistiske formål udført af en databehandler, der er specialiseret i disse aktiviteter
- behandling af kundedata i forbindelse med den almindelige forretningsgang i et forsikringselskab eller en bank
- behandling af personoplysninger for adfærdsbaseret annoncering i en søgemaskine
- behandling af data (indhold, trafik, position) af telefon- eller internetudbydere.

Eksempler, der ikke udgør databehandling i stort omfang, inkluderer:

- en enkelt læges behandling af patientdata
- en enkelt advokats behandling af personoplysninger vedrørende straffedomme og lovovertrædelser

Se yderligere oplysninger i retningslinjernes afsnit 2.1.3.

4 Hvad betyder begrebet "regelmæssig og systematisk" overvågning? (artikel 37, stk. 1, litra b))

Begrebet regelmæssig og systematisk overvågning af registrerede er ikke defineret i databeskyttelsesforordningen men inkluderer klart alle former for sporing og profilering på internettet, herunder med henblik på adfærdsbaseret annoncering. Begrebet overvågning er imidlertid ikke begrænset til onlinemiljøet.

Artikel 29-gruppen fortolker "regelmæssig" som havende en eller flere af følgende betydninger:

- vedvarende eller forekommende med bestemte intervaller i en bestemt periode
- tilbagevendende eller gentaget på faste tidspunkter
- konstant eller periodisk forekommende.

Artikel 29-gruppen fortolker "systematisk" som havende en eller flere af følgende betydninger:

- forekommer ifølge et system
- forudarrangeret, organiseret eller metodisk
- finder sted som led i en generel plan for dataindsamling
- udføres som en del af en strategi.

Eksempler: drift af et telekommunikationsnet, levering af telekommunikationstjenester, e-mail-retargeting profilering og bedømmelse med henblik på risikovurdering (f.eks. anvendelse til kreditvurdering, fastlæggelse af forsikringspræmier, forebyggelse af svig, afsløring af hvidvaskning af penge), sporing af opholdssted, for eksempel ved hjælp af mobilapps, loyalitetsprogrammer, adfærdsbaseret annoncering, overvågning af wellness-, fitness- og sundhedsdata via bærbare enheder, intern TV-overvågning, netforbundne enheder, f.eks. intelligente målere, intelligente biler, automatisering i hjemmet osv.

Se yderligere oplysninger i retningslinjernes afsnit 2.1.4.

5 Kan organisationer udpege en fælles databeskyttelsesrådgiver? I bekræftende fald, på hvilke betingelser? (artikel 37, stk. 2, og stk. 3)

Databeskyttelsesforordningen fastsætter, at en koncern kan udnævne en fælles databeskyttelsesrådgiver, forudsat at vedkommende er "*let tilgængelig fra hver enkel virksomhed*". Begrebet tilgængelighed henviser til databeskyttelsesrådgiverens opgaver som kontaktpunkt i forhold til de registrerede og tilsynsmyndigheden, men også internt i organisationen. Med henblik på at sikre, at den databeskyttelsesansvarlige, hvad enten intern eller ekstern, er tilgængelig, er det vigtigt at sikre, at dennes kontaktoplysninger er tilgængelige ifølge kravene i databeskyttelsesforordningen. Databeskyttelsesrådgiveren skal være i stand til effektivt at kunne kommunikere med de registrerede og samarbejde med de berørte tilsynsmyndigheder. Dette betyder, at denne kommunikation skal finde sted på det eller de sprog, som anvendes af tilsynsmyndighederne og de registrerede. Databeskyttelsesrådgiverens personlige tilgængelighed (uanset, om det er i form af fysisk tilstedeværelse i de samme lokaler som medarbejderne, via en hotline eller andre sikre kommunikationsmidler) er afgørende for at sikre, at registrerede vil være i stand til at kontakte databeskyttelsesrådgiveren.

Se yderligere oplysninger i retningslinjernes afsnit 2.3.

6 Er det muligt at udpege en ekstern databeskyttelsesrådgiver (artikel 37, stk. 6)?

Ja. Ifølge artikel 37, stk. 6, kan databeskyttelsesrådgiveren være den dataansvarliges eller databehandlerens medarbejder (intern databeskyttelsesrådgiver) eller kan "udføre hvervet på grundlag af en tjenesteydelseskontrakt". Dette betyder, at databeskyttelsesrådgiveren kan være ekstern, og i dette tilfælde kan dennes funktion udøves på grundlag af en tjenesteydelseskontrakt indgået med en enkeltperson eller en organisation.

Hvis databeskyttelsesrådgiveren er ekstern, finder alle bestemmelser i artikel 37-39 anvendelse på en sådan databeskyttelsesrådgiver. Som anført i retningslinjerne, hvis databeskyttelsesrådgiverens funktion udøves af en ekstern tjenesteyder, kan et team af personer, som arbejder for denne enhed, effektivt udføre databeskyttelsesrådgiverens funktioner som et team under ansvar af en udpeget hovedkontakt og "ansvarlig person" over for kunden. I dette tilfælde er det vigtigt, at hvert enkelt medlem af den eksterne organisation, som udøver funktionerne som databeskyttelsesrådgiver, opfylder alle relevante krav i databeskyttelsesforordningen.

Af hensyn til juridisk klarhed og god organisation anbefaler retningslinjerne, at der i tjenesteydelseskontrakten gives en klar fordeling af opgaverne i den eksterne

databeskyttelsesrådgivers team, samt at der udpeges en enkelt person som overordnet kontakt og "ansvarlig" over for kunden.

Se yderligere oplysninger i retningslinjernes afsnit 2.3, 2.4 og 3.5.

7 Hvilke faglige kvalifikationer bør databeskyttelsesrådgiveren have (artikel 37, stk. 5)?

Databeskyttelsesforordningen kræver, at databeskyttelsesrådgiveren "*udpeges på grundlag af sine faglige kvalifikationer, navnlig ekspertise inden for databeskyttelsesret og -praksis samt evne til at udføre de opgaver, der er omhandlet i artikel 39*".

Den nødvendige ekspertise bør fastlægges i henhold til de databehandlingsaktiviteter, der foretages, og den beskyttelse de behandlede personoplysninger kræver. Hvis for eksempel databehandlingen er særlig kompleks, eller hvor der behandles følsomme data i stort omfang, kan databeskyttelsesrådgiveren have brug for en højere grad af ekspertise og støtte.

De nødvendige færdigheder og ekspertiser omfatter:

- ekspertise i national og europæisk databeskyttelseslovgivning og -praksisser, herunder en dybdegående forståelse af databeskyttelsesforordningen
- forståelse af de databehandlingsaktiviteter, som udføres
- forståelse af informationsteknologi og datasikkerhed
- kendskab til erhvervsområdet og organisationen
- evne til at fremme en databeskyttelseskultur inden for organisationen.

Se yderligere oplysninger i retningslinjernes afsnit 2.4.

Databeskyttelsesrådgiverens stilling (artikel 38)

8 Hvilke ressourcer bør stilles til rådighed for databeskyttelsesrådgiveren til udførelsen af dennes opgaver?

Artikel 38, stk. 2, i databeskyttelsesforordningen kræver at organisationen støtter databeskyttelsesrådgiveren ved at "*tilvejebringe de nødvendige ressourcer til at udføre [dennes] opgaver, tilgå personoplysninger og behandlingsaktiviteter samt til opretholdelse af databeskyttelsesrådgiverens ekspertise*".

Afhængigt af organisationens størrelse og arten af de databehandlingsaktiviteter, der udføres, skal følgende ressourcer stilles til rådighed for databeskyttelsesrådgiveren:

- aktiv støtte til databeskyttelsesrådgiverens funktion fra seniorledelsen
- tilstrækkelig tid til databeskyttelsesrådgiverne til at gennemføre deres opgaver
- passende støtte i form af finansielle ressourcer, infrastruktur (lokaler, faciliteter, udstyr) og eventuelt personale
- officiel meddelelse til personalet om udpegelsen af databeskyttelsesrådgiveren
- adgang til andre afdelinger inden for organisationen, så databeskyttelsesrådgiverne kan modtage afgørende støtte, input og oplysninger fra disse andre afdelinger

- løbende efter- og videreuddannelse.

Se yderligere oplysninger i retningslinjernes afsnit 3.2.

9 Hvilke garantier sikrer, at databeskyttelsesrådgiveren kan udføre sine opgaver uafhængigt (artikel 38, stk. 3)?

Der findes flere garantier, som sætter databeskyttelsesrådgiveren i stand til at handle uafhængigt som anført i betragtning 97:

- ingen instruktioner fra dataansvarlige eller databehandlere vedrørende databeskyttelsesrådgiverens udøvelse af sine opgaver
- ingen afskedigelse eller straf fra den dataansvarlige for databeskyttelsesrådgiverens udførelse af sine opgaver
- ingen interessekonflikt med eventuelle andre opgaver og pligter.

Se yderligere oplysninger i retningslinjernes afsnit 3.3 til 3.5.

10 Hvilke andre af databeskyttelsesrådgiverens "opgaver og pligter" kan resultere i en interessekonflikt (artikel 38, stk. 6)?

Databeskyttelsesrådgiveren kan ikke have en stilling inden for organisationen, som indebærer, at denne fastlægger databehandlingens formål og bestemmer hjælpemidlerne hertil. På grund af hver enkelt organisations specifikke struktur skal hvert enkelt tilfælde overvejes fra sag til sag.

Som en tommelfingerregel kan modstridende stillinger omfatte stillinger i den øverste ledelse (for eksempel administrerende direktør, teknisk direktør, økonomidirektør, bedriftslæge, marketingchef, personalechef eller leder af IT-afdelinger), men også stillinger længere nede i organisationens struktur, hvis sådanne stillinger eller roller indebærer beslutninger om databehandlingens formål og hjælpemidler.

Se yderligere oplysninger i retningslinjernes afsnit 3.5.

Databeskyttelsesrådgiverens opgaver (artikel 39)

11 Hvad betyder begrebet "overvågning af overholdelse" med databeskyttelsesforordningen (artikel 39, stk. 1, litra b)?

Som en del af disse opgaver med overvågning af overholdelse skal databeskyttelsesrådgivere navnlig:

- indsamle oplysninger, der identificerer databehandlingsaktiviteter
- analysere og kontrollere databehandlingsaktiviteternes overholdelse af bestemmelserne
- informere, rådgive og udstede anbefalinger til den dataansvarlige eller databehandleren.

Se yderligere oplysninger i retningslinjernes afsnit 4.1.

12 Er databeskyttelsesrådgiveren personligt ansvarlig for manglende overholdelse af databeskyttelsesforordningen?

Nej, databeskyttelsesrådgivere er ikke personligt ansvarlige for manglende overholdelse af databeskyttelsesforordningen. Databeskyttelsesforordningen gør det klart, at det er den dataansvarlige eller databehandleren, som skal sikre og være i stand til at demonstrere, at databehandlingen udføres i overensstemmelse med denne forordning (artikel 24, stk. 1). Ansvar for overholdelse af databeskyttelsesbestemmelserne påhviler den dataansvarlige eller databehandleren.

13 Hvilken rolle spiller databeskyttelsesrådgiveren med hensyn til konsekvensanalysen vedrørende databeskyttelse (artikel 37, stk. 1, litra c), og fortegnelsen over databehandlingsaktiviteter (artikel 30)?

Med hensyn til konsekvensanalyse vedrørende databeskyttelse skal den dataansvarlige eller databehandleren søge rådgivning hos databeskyttelsesrådgiveren angående blandt andet følgende spørgsmål:

- om der skal udføres en konsekvensanalyse vedrørende databeskyttelse
- hvilken metode, der skal følges, ved gennemførelse af en konsekvensanalyse vedrørende databeskyttelse
- om konsekvensanalysen vedrørende databeskyttelse skal udføres internt eller udliciteres.
- hvilke garantier (herunder tekniske og organisatoriske foranstaltninger), der skal anvendes for at afbøde eventuelle risici for de registreredes rettigheder og interesser
- hvorvidt konsekvensanalysen vedrørende databeskyttelse er blevet korrekt udført, og hvorvidt dens konklusioner (om databehandlingen skal fortsætte, og hvilke garantier der skal anvendes) er i overensstemmelse med databeskyttelsesforordningen.

Se yderligere oplysninger i retningslinjernes afsnit 4.2.

Med hensyn til fortegnelser over databehandlingsaktiviteter er det den dataansvarlige eller databehandleren, som er forpligtet til at føre fortegnelser over databehandlingsaktiviteterne. Der er dog intet til hinder for, at den dataansvarlige eller databehandleren tildeler databeskyttelsesrådgiveren opgaven med at føre fortegnelser over databehandlingsaktiviteterne under den dataansvarliges ansvar. En sådan fortegnelse bør betragtes som et af de værktøjer, der sætter databeskyttelsesrådgiveren i stand til at udføre sine opgaver med at overvåge overholdelsen samt informere og rådgive den dataansvarlige eller databehandleren.

Se yderligere oplysninger i retningslinjernes afsnit 4.4.