



Retningslinjer for databeskyttelsesrådgivere

Vedtaget den 13. december 2016

Senest revideret og vedtaget den 5. april 2017

Denne arbejdsgruppe er nedsat ved artikel 29 i direktiv 95/46/EF. Den er et uafhængigt EU-rådgivningsorgan vedrørende beskyttelse af data og privatlivets fred. Dens opgaver er beskrevet i artikel 30 i direktiv 95/46/EF og artikel 15 i direktiv 2002/58/EF.

Sekretariatet varetages af Direktorat C (Grundlæggende rettigheder og retssikkerhed) i Europa-Kommissionen, Generaldirektoratet for Retlige Anliggender og Forbrugere, B-1049 Bruxelles, Belgien, Kontor MO59 05/35

Websted: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

**GRUPPEN VEDRØRENDE BESKYTTELSE AF PERSONER I FORBINDELSE MED
BEHANDLING AF PERSONOPLYSNINGER,**

som er nedsat ved Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995,

der henviser til artikel 29 og 30 i ovennævnte direktiv,

som henviser til gruppens forretningsorden,

HAR VEDTAGET FØLGENDE BESLUTNING:

Indholdsfortegnelse

1	INDLEDNING	4
2	UDPEGELSE AF EN DATABESKYTTELSESRÅDGIVER	5
2.1.	OBLIGATORISK UDPEGELSE	5
2.1.1	"Offentlige myndigheder eller organer"	6
2.1.2	"Kerneaktiviteter"	7
2.1.3	"Stort omfang"	7
2.1.4	"Regelmæssig og systematisk overvågning"	8
2.1.5	Særlige kategorier og personoplysninger vedrørende straffedomme og lovovertrædelser	9
2.2.	DATABEHANDLERENS DATABESKYTTELSESRÅDGIVER	9
2.3.	UDPEGNING AF EN FÆLLES DATABESKYTTELSESRÅDGIVER FOR FLERE ORGANISATIONER	10
2.4.	DATABESKYTTELSESRÅDGIVERENS TILGÆNGELIGHED OG PLACERING	11
2.5.	DATABESKYTTELSESRÅDGIVERENS EKSPERTISE OG KVALIFIKATIONER	11
2.6.	OFFENTLIGGØRELSE OG MEDDELELSE OM DATABESKYTTELSESRÅDGIVERENS KONTAKTOPLYSNINGER	13
3	DATABESKYTTELSESRÅDGIVERENS STILLING	14
3.1.	DATABESKYTTELSESRÅDGIVEREN INDDRAGES I ALLE SPØRGSMÅL VEDRØRENDE BESKYTTELSE AF PERSONOPLYSNINGER	14
3.2.	NØDVENDIGE RESSOURCER	15
3.3.	INSTRUKTIONER OG UDØVELSEN "AF DERES HVERV PÅ UAFHÆNGIG VIS"	15
3.4.	AFSKEDIGELSE ELLER STRAF FOR UDFØRELSE AF OPGAVER SOM DATABESKYTTELSESRÅDGIVER	16
3.5.	INTERESSEKONFLIKTER	17
4	DATABESKYTTELSESRÅDGIVERENS OPGAVER	18
4.1.	OVERVÅGNING AF OVERHOLDELSE AF DATABESKYTTELSESFORORDNINGEN	18
4.2.	DATABESKYTTELSESRÅDGIVERENS ROLLE I KONSEKVENSANALYSE VEDRØRENDE DATABESKYTTELSE	18
4.3.	SAMARBEJDE MED TILSYNSMYNDIGHEDEN OG FUNKTION SOM KONTAKTPUNKT	19
4.4.	RISIKOBASERET TILGANG	19
4.5.	DATABESKYTTELSESRÅDGIVERENS ROLLE I FØRING AF FORTEGNELSER	20
5	BILAG – RETNINGSLINJER VEDRØRENDE DATABESKYTTELSESRÅDGIVERE: HVAD DU BEHØVER AT VIDE 21	21
	UDPEGELSE AF DATABESKYTTELSESRÅDGIVER	21
1	HVILKE ORGANISATIONER SKAL UDPEGE EN DATABESKYTTELSESRÅDGIVER?	21
2	HVAD BETYDER KERNEAKTIVITETER?	21
3	HVAD BETYDER "STORT OMFANG"?	22
4	HVAD BETYDER "REGELMÆSSIG OG SYSTEMATISK" OVERVÅGNING?	22
5	KAN ORGANISATIONER UDPEGE EN FÆLLES DATABESKYTTELSESRÅDGIVER? I BEKRÆFTENDE FALD, PÅ HVILKE BETINGELSER?	23
6	HVOR BØR DATABESKYTTELSESRÅDGIVEREN VÆRE PLACERET?	23
7	ER DET MULIGT AT UDPEGE EN EKSTERN DATABESKYTTELSESRÅDGIVER?	23
8	HVILKE FAGLIGE KVALIFIKATIONER BØR DATABESKYTTELSESRÅDGIVEREN HAVE?	24
	DATABESKYTTELSESRÅDGIVERENS STILLING	24
9	HVILKE RESSOURCER BØR DEN DATAANSVARLIGE ELLER DATABEHANDLEREN GIVE TIL DATABESKYTTELSESRÅDGIVEREN?	24
10	HVILKE GARANTIER SIKRER, AT DATABESKYTTELSESRÅDGIVEREN KAN UDFØRE SINE OPGAVER UAFHÆNGIGT? HVAD BETYDER "INTERESSEKONFLIKT"?	25
	DATABESKYTTELSESRÅDGIVERENS OPGAVER	26
11	HVAD BETYDER "OVERVÅGNING AF OVERHOLDELSE"?	26
12	ER DATABESKYTTELSESRÅDGIVEREN PERSONLIGT ANSVARLIG FOR MANGLENDE OVERHOLDELSE AF KRAVENE TIL DATABESKYTTELSE?	26
13	HVILKEN ROLLE SPILLER DATABESKYTTELSESRÅDGIVEREN MED HENSYN TIL VURDERING AF KONSEKVENSANALYSE VEDRØRENDE DATABESKYTTELSE OG FORTEGNELSER OVER DATABEHANDLINGSAKTIVITETER?	26

1 Indledning

Databeskyttelsesforordningen,¹ der forventes at træde i kraft den 25. maj 2018, indeholder en moderniseret, ansvarsbaseret overholdelsesramme for databeskyttelse i Europa. Inden for denne nye ramme vil databeskyttelsesrådgivere have en central plads i mange organisationer ved at lette overholdelsen af bestemmelserne i databeskyttelsesforordningen.

Databeskyttelsesforordningen gør det obligatorisk for visse dataansvarlige og databehandlere at udpege en databeskyttelsesrådgiver². Dette vil være tilfældet for alle offentlige myndigheder og organer (uanset hvilke data de behandler) og for andre organisationer, der som deres kerneaktivitet systematisk og i stort omfang overvåger personer eller behandler særlige kategorier af personoplysninger i stort omfang.

Selv når databeskyttelsesforordningen ikke specifikt 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.

Begrebet databeskyttelsesrådgiver er ikke nyt. Selvom direktiv 95/46/EF³ ikke kræver, at organisationer udpeger en databeskyttelsesrådgiver, så er praksis med en sådan udpegelse ikke desto mindre gennem årene blevet udviklet i flere medlemsstater.

Før vedtagelsen af databeskyttelsesforordningen hævdede Artikel 29-gruppen, at databeskyttelsesrådgiveren er hjørnестenen i ansvarlighed, og at udpegelsen af en databeskyttelsesrådgiver kan lette overholdelse og desuden blive en konkurrencemæssig fordel for virksomheder⁴. Foruden at fremme overholdelse gennem implementering af ansvarlighedsværktøjer (som at lette udførelsen af konsekvensanalyser vedrørende databeskyttelse og revisioner, eller gøre dem lettere at udføre), så fungerer databeskyttelsesrådgivere som mellemlid mellem relevante aktører (f.eks. tilsynsførende myndigheder, registrerede og forretningsenheder inden for en organisation).

Databeskyttelsesrådgivere er ikke personligt ansvarlige i tilfælde af 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

¹Europa-Parlamentets og Rådets forordning (EU) nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (beskyttelse af personoplysninger) (EUT L 119 af 4.5.2016, s. 1). Databeskyttelsesforordningen er relevant for EØS og vil finde anvendelse efter dens indarbejdelse i EØS-aftalen.

² Udpegelsen af en databeskyttelsesrådgiver er også obligatorisk for kompetente myndigheder ifølge artikel 32 i Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT L 119 af 4.5.2016, s. 89-131) samt den nationale gennemførelseslovgivning. Mens disse retningslinjer vil fokusere på databeskyttelsesrådgivere ifølge databeskyttelsesforordningen, så er vejledningen også relevant for databeskyttelsesrådgivere ifølge direktiv 2016/680 med hensyn til deres tilsvarende bestemmelser.

³ Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT L 281 af 23.11.1995, s. 31).

⁴ Se http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

overensstemmelse med forordningens bestemmelser (artikel 24, stk. 1). Ansvar for overholdelse af databeskyttelsesbestemmelserne påhviler den dataansvarlige eller databehandleren.

Den dataansvarlige eller databehandleren spiller også en afgørende rolle i den faktiske udførelse af databeskyttelsesrådgiverens opgaver. Udpegelsen af en databeskyttelsesrådgiver er et første trin, men databeskyttelsesrådgiveren skal også gives tilstrækkelig autonomi og ressourcer til at kunne udføre sine opgaver.

Databeskyttelsesforordningen anerkender databeskyttelsesrådgiveren som en central aktør i det nye datastyringssystem og fastsætter betingelserne for udpegelsen af datarådgiveren samt dennes stilling og opgaver. Formålet med disse retningslinjer er at tydeliggøre de relevante bestemmelser i databeskyttelsesforordningen for at støtte dataansvarlige og databehandlere i at overholde loven, men også at støtte databeskyttelsesrådgiverne i deres rolle. Retningslinjerne indeholder også anbefalinger til bedste praksis, der bygger på erfaringerne fra nogle EU-medlemsstater. Artikel 29-gruppen vil overvåge gennemførelsen af disse retningslinjer og kan supplere dem med yderligere detaljer, såfremt den finder det passende.

2 Udpegelse af en databeskyttelsesrådgiver

2.1. Obligatorisk udpegelse

Artikel 37, stk. 1, i databeskyttelsesforordningen kræver, at en databeskyttelsesrådgiver udpeges i tre specifikke tilfælde⁵:

- a) når behandlingen foretages af en offentlig myndighed eller et offentligt organ⁶;
- b) når den dataansvarliges eller databehandlerens kerneaktiviteter kræver regelmæssig og systematisk overvågning af registrerede i stort omfang eller
- c) når den dataansvarliges eller databehandlerens kerneaktiviteter består af behandling i stort omfang af særlige kategorier af oplysninger⁷ eller⁸ personoplysninger vedrørende straffedomme og lovovertrædelser⁹.

I de følgende underafsnit giver Artikel 29-gruppen vejledning med hensyn til de kriterier og den terminologi, der er anvendt i artikel 37, stk. 1.

Medmindre det er indlysende, at en organisation ikke er forpligtet til at udpege en databeskyttelsesrådgiver, så anbefaler Artikel 29-gruppen, at dataansvarlige og databehandlere dokumenterer den interne analyse, som er udført med henblik på at bestemme, hvorvidt en databeskyttelsesrådgiver skal udpeges, for dermed at kunne demonstrere, at de relevante faktorer er

⁵ Bemærk, at ifølge artikel 37, stk. 4, kan EU- eller medlemsstatslovgivning eventuelt også kræve udpegelse af databeskyttelsesrådgivere i andre situationer.

⁶ Med undtagelse af domstole, der handler i deres egenskab af domstol. Se artikel 32 i direktiv (EU) 2016/680.

⁷ Ifølge artikel 9 omfatter disse personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

⁸ Artikel 37, stk. 1, litra c), benytter ordet "og". Se afsnit 2.1.5 herunder for en forklaring af brugen "eller" i stedet for "og".

⁹ Artikel 10.

blevet taget korrekt i betragtning¹⁰. Denne analyse er en del af dokumentationen vedrørende ansvarlighedsprincippet. Den kan pålægges af tilsynsmyndigheden og skal opdateres, når det er nødvendigt. For eksempel, hvis den dataansvarlige eller databehandleren påtager sig nye aktiviteter eller nye tjenesteydelser, der kan falde inden for tilfældene, der er anført i artikel 37, stk. 1.

Når en organisation udpeger en databeskyttelsesrådgiver på frivillig basis, gælder kravene i henhold til artikel 37-39 for hans eller hendes udpegelse, stilling og opgaver, som hvis udpegelsen havde været obligatorisk.

Der er intet til hinder for, at en organisation, som ikke er juridisk forpligtet til at udpege en databeskyttelsesrådgiver, og som ikke ønsker at udpege en databeskyttelsesrådgiver på frivillig basis, ikke desto mindre benytter personale eller eksterne rådgivere til opgaver, der relaterer til beskyttelse af personoplysninger. I dette tilfælde er det vigtigt at sikre, at der ikke er forvirring med hensyn til deres titel, status, stilling og opgaver. Det bør derfor tydeliggøres i enhver kommunikation inden for virksomheden samt med databeskyttelsesmyndighederne, registrerede og den brede offentlighed, at titlen på denne person eller rådgiver ikke er en databeskyttelsesrådgiver.¹¹

Databeskyttelsesrådgiveren, uanset om obligatorisk eller frivillig, udpeges for alle databehandlingsprocesser, som udføres af den dataansvarlige eller databehandleren.

2.1.1 "OFFENTLIGE MYNDIGHEDER ELLER ORGANER"

Databeskyttelsesforordningen definerer ikke, hvad der udgør en "*offentlig myndighed eller organ*". Artikel 29-gruppen mener, at et sådant begreb skal fastsættes i den nationale lovgivning. Derfor omfatter offentlige myndigheder og organer nationale, regionale og lokale myndigheder, men i gældende national lovgivning omfatter konceptet typisk også en række andre offentligretlige organer¹². I disse tilfælde er udpegelse af en databeskyttelsesrådgiver obligatorisk.

Det er ikke kun offentlige myndigheder eller organer, der kan udføre offentlige opgaver¹³ og udøve offentlig myndighed. Dette kan også udføres af fysiske eller juridiske personer, der er underlagt offentligretlige eller privatretlige bestemmelser i hvert enkelt medlemsland, inden for sektorer som offentlige transportydelser, vand- og energiforsyning, vejinfrastruktur, public service-radio- og tv- virksomhed, socialt boligbyggeri og organer for lovregulerede erhverv.

I disse tilfælde kan de registrerede befinde sig i en situation, der minder meget om, når deres data behandles af en offentlig myndighed eller organ. Data kan blive behandlet til lignende formål, og personerne har ofte lignende næsten intet eller intet valg vedrørende, hvorvidt og hvordan deres data bliver behandlet, og kan derfor eventuelt behøve den yderligere beskyttelse, som udpegelse af en databeskyttelsesrådgiver kan bringe.

¹⁰ Jf. artikel 24, stk. 1.

¹¹ Dette er også relevant for databeskyttelsesansvarlige ledere og andre databeskyttelsesekspertes, som allerede er på plads i nogle virksomheder, og som måske ikke altid opfylder kriterierne i databeskyttelsesforordningen hvad f.eks. angår tilgængelige ressourcer eller garanti for uafhængighed, og som, hvis de ikke opfylder kriterierne, ikke kan betragtes eller omtales som databeskyttelsesrådgivere.

¹² Se for eksempel definitionen af "*offentlig myndighed*" og "*offentligretligt organ*" i artikel 2, stk. 1, og stk. 2, Europa-Parlamentets og Rådets direktiv 2003/98/EF af 17. november 2003 om videreanvendelse af den offentlige sektors informationer (EUT L 345 af 31.12.2003, s. 90).

¹³ Artikel 6, stk. 1, litra e).

Selvom der ikke er nogen forpligtelse i sådanne tilfælde, så anbefaler Artikel 29-gruppen, at private organisationer, der udfører offentlige opgaver eller udøver offentlig myndighed, som god praksis udpeger en databeskyttelsesrådgiver. Databeskyttelsesrådgiverens aktivitet dækker alle databehandlingsprocesser, der udføres, herunder dem, som ikke er relateret til udførelsen af en offentlig opgave eller til udøvelsen af officielle pligter (f.eks. administration af en medarbejderdatabase).

2.1.2 "KERNEAKTIVITETER"

Artikel 37, stk. 1, litra b), og c), i databeskyttelsesforordningen henviser til "*den dataansvarliges eller databehandlerens kerneaktiviteter*". Betragtning 97 specificerer, at en dataansvarligs kerneaktiviteter vedrører "*hovedaktiviteter og ikke behandling af personoplysninger som biaktivitet*". "Kerneaktiviteter" kan betragtes som de centrale aktiviteter, der er nødvendige for at opnå den dataansvarliges eller databehandlerens mål.

Dog skal "kerneaktiviteter" ikke fortolkes som udelukkelse af aktiviteter, hvor databehandling udgør en uundgåelig del af den dataansvarliges eller databehandleres aktivitet. For eksempel er et hospitals kerneaktivitet at yde sundhedspleje. Et hospital kan imidlertid ikke yde sikker og effektiv sundhedspleje uden at behandle sundhedsdata som blandt andet patientjournaler. Derfor skal behandlingen af disse data betragtes som en af ethvert hospitals kerneaktiviteter, og hospitaler skal derfor udpege databeskyttelsesrådgivere.

Et andet eksempel er et privat vagtselskab, som udfører overvågning af en række private indkøbscentre og offentlige rum. Overvågning er virksomhedens kerneaktivitet, som til gengæld er uløseligt forbundet med behandling af personoplysninger. Derfor skal denne virksomhed udpege en databeskyttelsesrådgiver.

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

2.1.3 "STORT OMFANG"

Artikel 37, stk. 1, litra b) og c), fastsætter, at behandling af personoplysninger i stort omfang kræver udpegelse af en databeskyttelsesrådgiver. Databeskyttelsesforordningen definerer ikke, hvad der forstås ved behandling i stort omfang, men betragtning 91 giver en vis vejledning¹⁴.

¹⁴ Ifølge betragtningen vil navnlig "*omfattende behandlingsaktiviteter til behandling af meget store mængder personoplysninger på regionalt, nationalt eller overnationalt plan, der kan berøre mange registrerede, og som sandsynligvis vil indebære en høj risiko*" være inkluderet. På den anden side fastslår betragtningen udtrykkeligt, at "*behandling af personoplysninger bør ikke anses for at være omfattende, hvis der er tale om læges, en sundhedsmedarbejders eller en advokats individuelle behandling af personoplysninger om patienter eller klienter*". Det er vigtigt at tage i betragtning, at mens betragtningen giver eksempler på omfangets yderpunkter (den enkelte læges databehandling versus databehandling af et helt land eller i hele Europa), så findes der en stor gråzone mellem disse yderpunkter. Desuden bør det også huskes, at denne betragtning henviser til konsekvensanalyser vedrørende databeskyttelse. Dette indebærer, at nogle elementer kan være specifikke i den

Desuden er det heller ikke muligt at fremsætte et præcist tal hverken med hensyn til den behandlede datamængde eller for antallet af behandlede personer, som vil være gældende i alle situationer. Dette udelukker dog ikke muligheden for, at det med tiden vil være muligt at udvikle en standardpraksis for identifikation af mere specifikke og/eller kvantitative udtryk for, hvad der udgør "*stort omfang*" med hensyn til visse former for almindelige databehandlingsaktiviteter. Artikel 29-gruppen planlægger også at bidrage til denne udvikling gennem deling og offentliggørelse af eksempler på relevante tærskler for udpegning af en databeskyttelsesrådgiver.

Artikel 29-gruppen anbefaler under alle omstændigheder, at navnlig de følgende faktorer tages i betragtning, når det bestemmes, om der gennemføres databehandling 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 tjenester
- behandling af kundedata i forbindelse med den almindelige forretningsgang i et forsikringsselskab 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

2.1.4 "REGELMÆSSIG OG SYSTEMATISK OVERVÅGNING"

Begrebet regelmæssig og systematisk overvågning af registrerede er ikke defineret i databeskyttelsesforordningen, men konceptet om "*overvågning af registreredes adfærd*" er nævnt i betragtning 24¹⁵ og inkluderer klart alle former for sporing og profilering på internettet, herunder med henblik på adfærdsbaseret annoncering.

pågældende sammenhæng og ikke nødvendigvis også vil medføre krav om udpegelse af databeskyttelsesrådgivere på nøjagtig samme måde.

¹⁵ "*For at afgøre, om en behandlingsaktivitet kan betragtes som overvågning af registreredes adfærd, bør det undersøges, om fysiske personer spores på internettet, herunder mulig efterfølgende brug af teknikker til behandling af personoplysninger, der består i profilering af en fysisk person, navnlig med det formål at træffe beslutninger om den pågældende eller analysere eller forudsige den pågældendes præferencer, adfærd og holdninger.*"

Begrebet overvågning er imidlertid ikke kun begrænset til onlinemiljøet, og onlinesporing bør kun betragtes som et eksempel på overvågning af registreredes adfærd¹⁶.

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 på aktiviteter, der kan udgøre regelmæssig og systematisk overvågning af registrerede: drift af et telekommunikationsnet, levering af telekommunikationstjenester, e-mail-retargeting, datadrevne marketingaktiviteter, 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.

2.1.5 SÆRLIGE KATEGORIER OG PERSONOPLYSNINGER VEDRØRENDE STRAFFEDOMME OG LOVOVERTRÆDELSER

Artikel 37, stk. 1, litra c), omhandler behandling af særlige kategorier af oplysninger, jf. artikel 9, og personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10. Selvom bestemmelsen benytter ordet "og", er der ingen grund til, at de to kriterier skal anvendes samtidig. Teksten bør der læses med betydningen "eller".

2.2. Databehandlerens databeskyttelsesrådgiver

Artikel 37 gælder for både dataansvarlige¹⁷ og databehandlere¹⁸ med hensyn til udpegelse af en databeskyttelsesrådgiver. Afhængigt af kriterierne for hvem, der er forpligtet til at udpege en databeskyttelsesrådgiver, så kan det i nogle tilfælde kun være den dataansvarlige eller kun databehandleren, mens både den dataansvarlige og dennes databehandler i andre tilfælde er forpligtet til at udpege en databeskyttelsesrådgiver (som derefter bør samarbejde).

¹⁶ Bemærk, at betragtning 24 fokuserer på den eksterritoriale anvendelse af databeskyttelsesforordningen. Desuden er der også en forskel mellem ordlyden "overvågning af sådanne registreredes adfærd" (artikel 3, stk. 2, litra b)) og "regelmæssig og systematisk overvågning af registrerede", (artikel 37, stk.1, litra b)), som derfor bør ses som forskellige begreber.

¹⁷ Den dataansvarlige er i artikel 4, stk. 7, defineret som den person eller det organ, der afgør, til hvilke formål og med hvilke hjælpemidler behandlingen skal udføres.

¹⁸ Databehandleren er i artikel 4, stk. 8, defineret som den person eller det organ, der behandler dataene på vegne af den dataansvarlige.

Det er vigtigt at fremhæve, at selvom den dataansvarlige opfylder kriterierne for obligatorisk udpegelse af en databeskyttelsesrådgiver, så kræver dette ikke nødvendigvis, at databehandlere er forpligtet til at udpege en databeskyttelsesrådgiver. Det kan dog være en god praksis.

Eksempler:

- En lille familievirksomhed, som er aktiv inden for distribution af husholdningsapparater i en enkelt by, benytter tjenester fra en databehandler, hvis kerneaktivitet er at levere webstedsanalysetjenester og assistance med målrettet reklame og markedsføring. Familievirksomhedens aktiviteter og dens kunder genererer ikke databehandling "i stort omfang" i betragtning af det lille antal kunder og de relativt begrænsede aktiviteter. Dog kan behandlerens aktiviteter, der behandler mange kunder som denne lille virksomhed, sammenlagt udgøre databehandling i stort omfang. Databehandleren skal derfor udpege en databeskyttelsesrådgiver ifølge artikel 37, stk. 1, litra b). Familievirksomheden er derimod ikke forpligtet til at udpege en databeskyttelsesrådgiver.
- En mellemstor fliseproduktionsvirksomhed udliciterer sin bedriftssundhedstjeneste til en ekstern databehandler, som har et stort antal tilsvarende kunder. Databehandleren skal udpege en databeskyttelsesrådgiver ifølge artikel 37, stk. 1, litra c), under forudsætning af, at databehandlingen sker i stort omfang. Dog er producenten ikke nødvendigvis forpligtet til at udpege en databeskyttelsesrådgiver.

Databeskyttelsesrådgiveren, som udpeges af en databehandler, overvåger også aktiviteter, der udføres af databehandlerens organisation, når denne selv handler som dataansvarlig (f.eks. HR, IT, logistik).

2.3. Udpegning af en fælles databeskyttelsesrådgiver for flere organisationer

Artikel 37, stk. 2, giver en koncern mulighed for at udnævne en fælles databeskyttelsesrådgiver, forudsat at vedkommende er "*let tilgængelig fra hver enkel virksomhed*". Begrebet om adgang henviser til databeskyttelsesrådgiverens opgaver som kontaktpunkt i forhold til de registrerede¹⁹ og tilsynsmyndigheden²⁰, men også internt i organisationen, i betragtning af, at det er databeskyttelsesrådgiverens opgave at "*at underrette og rådgive den dataansvarlige eller databehandleren og de ansatte, der behandler personoplysninger, om deres forpligtelser i henhold til denne forordning*"²¹.

Med henblik på at sikre, at databeskyttelsesrådgiveren, hvad enten intern eller ekstern, er tilgængelig, er det vigtigt at sørge for, at dennes kontaktoplysninger er tilgængelige ifølge kravene i databeskyttelsesforordningen²².

¹⁹ I artikel 38, stk. 4: "*registrerede kan kontakte databeskyttelsesrådgiveren angående alle spørgsmål om behandling af deres oplysninger og om udøvelse af deres rettigheder i henhold til denne forordning.*"

²⁰ Artikel 39, stk. 1, litra e): "*fungere som tilsynsmyndighedens kontaktpunkt i spørgsmål vedrørende behandling, herunder den forudgående høring, der er omhandlet i artikel 36, og at høre tilsynsmyndigheden, når det er hensigtsmæssigt, om eventuelle andre spørgsmål.*"

²¹ Artikel 39, stk. 1, litra a).

²² Se også afsnit 2.6 nedenfor.

Vedkommende skal, eventuelt med hjælp fra et team, være i stand til effektivt at kunne kommunikere med de registrerede²³ og samarbejde²⁴ med de kompetente tilsynsmyndigheder. Dette betyder også, at denne kommunikation skal finde sted på det eller de sprog, som anvendes af tilsynsmyndighederne og de registrerede. Databeskyttelsesrådgiverens 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.

I henhold til artikel 37, stk. 3, kan flere myndigheder eller organer udpege en fælles databeskyttelsesrådgiver under hensyntagen til deres organisationsstruktur og størrelse. De samme overvejelser gælder med hensyn til ressourcer og kommunikation. I betragtning af, at databeskyttelsesrådgiveren er ansvarlig for en række opgaver, skal den dataansvarlige eller databehandleren sikre, at en enkelt databeskyttelsesrådgiver, eventuelt med hjælp af et team, effektivt kan udføre sine opgaver trods udpegelsen til flere offentlige myndigheder og organer.

2.4. Databeskyttelsesrådgiverens tilgængelighed og placering

I henhold til afsnit 4 i databeskyttelsesforordningen skal databeskyttelsesrådgiverens tilgængelighed være effektiv.

Artikel 29-gruppen anbefaler, at databeskyttelsesrådgiveren, for at være tilgængelig, placeres inden for EU, uanset om den dataansvarlige eller databehandleren er etableret i Den Europæiske Union.

Dog kan det ikke udelukkes, at databeskyttelsesrådgiveren i nogle situationer, hvor den dataansvarlige eller databehandleren ikke har nogen etablering inden for EU²⁵, kan være i stand til at udføre sine aktiviteter mere effektivt, hvis vedkommende er placeret uden for EU.

2.5. Databeskyttelsesrådgiverens ekspertise og kvalifikationer

Artikel 37, stk. 5, fastlægger, 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.*" Betragtning 97 bestemmer, at den nødvendige ekspertise bør fastlægges i henhold til de databehandlingsaktiviteter, der foretages, og den beskyttelse de behandlede personoplysninger kræver.

- **Ekspertiseniveau**

Det påkrævede ekspertiseniveau er ikke præcist defineret, men skal være rimeligt i forhold til behandlingsaktiviteternes følsomhed, kompleksitet og omfang i den pågældende organisation. Hvis for

²³ Artikel 12, stk. 1: "*Den dataansvarlige træffer passende foranstaltninger til at give enhver oplysning som omhandlet i artikel 13 og 14 og enhver meddelelse i henhold til artikel 15-22 og 34 om behandling til den registrerede i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog, navnlig når oplysninger specifikt er rettet mod et barn.*"

²⁴ Artikel 39, stk. 1, litra d): "*at samarbejde med tilsynsmyndigheden*"

²⁵ Se artikel 3 i databeskyttelsesforordningen om territorialt anvendelsesområde.

eksempel databehandlingen er særlig kompleks, eller hvor der behandles følsomme data i stort omfang, kan databeskyttelsesrådgiveren have brug for en større grad af ekspertise og støtte. Der er også forskel afhængigt af, om organisationen systematisk overfører personoplysninger til uden for EU, eller om sådanne overførsler er lejlighedsvis. Databeskyttelsesrådgiveren skal derfor vælges med omhu under hensyntagen til spørgsmålene om databeskyttelse, som opstår inden for organisationen.

- **Faglige kvalifikationer**

Selvom artikel 37, stk. 5, ikke angiver de faglige kvalifikationer, bør der, når databeskyttelsesrådgiverne udpeges, tages hensyn til, at det er et relevant element, at databeskyttelsesrådgiveren har ekspertise i national og europæisk databeskyttelseslovgivning og -praksisser samt en indgående forståelse af databeskyttelsesforordningen. Det er også nyttigt, hvis de tilsynsførende myndigheder fremmer passende og regelmæssig uddannelse af databeskyttelsesrådgivere.

Kendskab til erhvervsområdet og den dataansvarliges organisation er nyttig. Databeskyttelsesrådgiveren bør også have en god forståelse af de behandlingsaktiviteter, som udføres, informationssystemer og datasikkerhed samt den dataansvarliges databeskyttelsesbehov.

Hvis der er tale om en offentlig myndighed eller et organ, bør databeskyttelsesrådgiveren også have et solidt kendskab til administrative regler og procedurer i organisationen.

- **Evne til at udføre opgaverne**

Evnen til at udføre de opgaver, der påhviler databeskyttelsesrådgiveren, bør fortolkes både med henvisning til dennes personlige kvalifikationer og viden, men også med hensyn til deres stilling i organisationen. Personlige kvalifikationer bør for eksempel omfatte integritet og høj faglig etik. Databeskyttelsesrådgiveren skal først og fremmest medvirke til overholdelse af databeskyttelsesforordningen. Databeskyttelsesrådgiveren spiller en central rolle i fremme af en databeskyttelseskultur inden for organisationen og bistår med implementeringen af centrale elementer i databeskyttelsesforordningen som for eksempel principperne om databehandling²⁶, den registreredes rettigheder²⁷, indbygget databeskyttelse og databeskyttelse gennem indstillinger²⁸, registrering af behandlingsaktiviteter²⁹, sikkerhed i behandlingen³⁰ og anmeldelse og kommunikation af brud på datasikkerheden³¹.

- **Databeskyttelsesrådgiver på grundlag af en tjenesteydelseskontrakt**

Databeskyttelsesrådgiverens funktion kan også udøves på grundlag af en tjenesteydelseskontrakt, som indgås med en person eller organisation uden for den dataansvarliges/databehandlerens organisation. I sidstnævnte tilfælde er det vigtigt, at hvert enkelt medlem af organisationen, som udøver funktionerne som databeskyttelsesrådgiver, opfylder alle gældende krav i afsnit 4 i databeskyttelsesforordningen (for eksempel er det vigtigt, at ingen af dem befinder sig i en interessekonflikt). Det er også lige så

²⁶ Kapitel II.

²⁷ Kapitel III.

²⁸ Artikel 25.

²⁹ Artikel 30.

³⁰ Artikel 32.

³¹ Artikel 33 og 34.

vigtigt, at ethvert sådant medlem af organisationen er beskyttet af bestemmelserne i databeskyttelsesforordningen (for eksempel ingen unfair opsigelse af tjenesteydelseskontrakt for aktiviteter som databeskyttelsesrådgiver, men heller ikke nogen unfair afskedigelse af noget enkelt medlem af organisationen, som udfører en databeskyttelsesrådgivers opgaver). På samme tid kan individuelle færdigheder og styrker kombineres, så flere personer, der arbejder i et team, mere effektivt kan betjene deres kunder.

Af hensyn til juridisk klarhed og god organisation og for at forebygge interessekonflikter for teammedlemmerne, anbefales en klar fordeling af opgaverne i databeskyttelsesrådgiverens team, samt at der udpeges en enkelt person som overordnet kontakt og "ansvarlig" for kunden. Det vil i almindelighed også være nyttigt at angive disse punkter i tjenesteydelseskontrakten.

2.6. Offentliggørelse og meddelelse om databeskyttelsesrådgiverens kontaktoplysninger

Artikel 37, stk. 7, i databeskyttelsesforordningen kræver, at den dataansvarlige eller databehandleren:

- offentliggør databeskyttelsesrådgiverens kontaktoplysninger
- meddeler databeskyttelsesrådgiverens kontaktoplysninger til de relevante tilsynsmyndigheder.

Formålet med disse krav er at sikre, at de registrerede (både i og uden for organisationen) og tilsynsmyndighederne nemt og direkte kan kontakte databeskyttelsesrådgiveren uden at behøve kontakte nogen anden del af organisationen. Fortrolighed er et lige så vigtigt punkt: For eksempel kan medarbejdere være tilbageholdende med at klage til databeskyttelsesrådgiveren, hvis fortroligheden i deres kommunikation ikke er sikret.

Databeskyttelsesrådgiveren er underlagt tavshedspligt eller fortrolighed vedrørende udførelsen af sine opgaver i overensstemmelse med EU-retten eller medlemsstaternes nationale ret (artikel 38, stk. 5).

Databeskyttelsesrådgiverens kontaktoplysninger bør indeholde oplysninger, som gør det nemt for registrerede og tilsynsmyndighederne at nå databeskyttelsesrådgiveren (en postadresse, et dedikeret telefonnummer og/eller en dedikeret e-mailadresse). Når det er relevant, kan andre kommunikationsmidler også benyttes til kommunikation med offentligheden, for eksempel en dedikeret hotline eller en dedikeret kontaktformular rettet til databeskyttelsesrådgiveren på organisationens hjemmeside.

Artikel 37, stk. 7, kræver ikke, at de offentliggjorte oplysninger også omfatter navnet på databeskyttelsesrådgiveren. Mens det kan være god praksis at oplyse dette, så er det op til den dataansvarlige og databehandleren samt databeskyttelsesrådgiveren at beslutte, om dette er nødvendigt eller nyttigt under de særlige omstændigheder³².

Meddelelse om databeskyttelsesrådgiverens navn til tilsynsmyndigheden er imidlertid afgørende for at databeskyttelsesrådgiveren kan fungere som kontaktpunkt mellem organisationen og tilsynsmyndigheden (artikel 39, stk. 1, litra e).

³² Det er bemærkelsesværdigt, at artikel 33, stk. 3, litra b), der beskriver oplysningerne, som skal gives til tilsynsmyndigheden og de registrerede i tilfælde af brud på persondatasikkerheden, i modsætning til artikel 37, stk. 7, specielt også kræver at navnet (og ikke kun kontaktoplysningerne) på databeskyttelsesrådgiveren skal oplyses.

Som god praksis anbefaler Artikel 29-gruppen også, at en organisation oplyser sine medarbejdere om navnet på databeskyttelsesrådgiveren og dennes kontaktoplysninger. For eksempel kan databeskyttelsesrådgiverens navn og kontaktoplysninger offentliggøres internt via organisationens intranet, interne telefonbog og organisatoriske diagrammer.

3 Databeskyttelsesrådgiverens stilling

3.1. Databeskyttelsesrådgiveren inddrages i alle spørgsmål vedrørende beskyttelse af personoplysninger

Artikel 38 i databeskyttelsesforordningen fastsætter, at den dataansvarlige og databehandleren sikrer, at databeskyttelsesrådgiveren "*inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger*".

Det er afgørende, at databeskyttelsesrådgiveren, eller dennes team, inddrages på så tidligt et trin som muligt i alle spørgsmål vedrørende databeskyttelse. I forbindelse med konsekvensanalyser vedrørende databeskyttelse foreskriver databeskyttelsesforordningen udtrykkeligt en tidlig inddragelse af databeskyttelsesrådgiveren og angiver, at den dataansvarlige skal søge råd hos databeskyttelsesrådgiveren, når sådanne konsekvensanalyser udføres³³. Ved at sikre, at databeskyttelsesrådgiveren holdes informeret lige fra starten, bliver det nemmere at overholde databeskyttelsesforordningen og fremme en indbygget databeskyttelse. Det bør derfor være standardprocedure inden for organisationens ledelse. Derudover er det vigtigt, at databeskyttelsesrådgiveren opfattes som en samtalepartner i organisationen, og at han eller hun indgår i de relevante arbejdsgrupper, der beskæftiger sig med databehandlingsaktiviteter inden for organisationen.

Endelig bør organisationen for eksempel sikre, at:

- databeskyttelsesrådgiveren regelmæssigt inviteres til at deltage i møder på senior- og mellemliderniveau
- databeskyttelsesrådgiverens tilstedeværelse er ønskværdig, når der skal tages beslutninger, som har en databeskyttelsesdimension. Alle relevante oplysninger skal videregives rettidigt til databeskyttelsesrådgiveren, så denne kan give passende rådgivning
- databeskyttelsesrådgiverens udtalelser altid tillægges behørig vægt. I tilfælde af uenighed anbefaler Artikel 29-gruppen som god praksis at dokumentere årsagerne til, at databeskyttelsesrådgiverens henstillinger ikke følges.
- databeskyttelsesrådgiveren omgående høres i tilfælde af, at et brud på datasikkerheden eller en anden hændelse har fundet sted.

Når det er relevant kan den dataansvarlige eller databehandleren udvikle retningslinjer eller programmer for databeskyttelse som fastlægger, hvornår databeskyttelsesrådgiveren skal høres.

³³ Artikel 35, stk. 2.

3.2. Nødvendige ressourcer

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"*. Navnlig skal følgende punkter tages i betragtning:

- Aktiv støtte til databeskyttelsesrådgiverens funktion fra seniorledelsen (såsom på bestyrelsesniveau).
- Tilstrækkelig tid til databeskyttelsesrådgiverne til at gennemføre deres opgaver. Dette er især vigtigt, hvor en intern databeskyttelsesrådgiver udpeges på deltidsbasis, eller hvor den eksterne databeskyttelsesrådgiver udfører databeskyttelse i tilslutning til andre opgaver. Ellers vil modstridende prioriteter kunne resultere i, at databeskyttelsesrådgiverens pligter forsømmes. Det er altafgørende, at der er tilstrækkelig tid til databeskyttelsesrådgiverens opgaver. Det er god praksis at afsætte en procentdel af tiden til databeskyttelsesrådgiverfunktionen, når den ikke udføres på heltidsbasis. Det er også god praksis at bestemme tiden, som er nødvendig til at udføre funktionen, det passende prioritetsniveau for databeskyttelsesrådgiverens pligter og at databeskyttelsesrådgiveren (eller organisationen) udarbejder en arbejdsplan.
- Passende støtte i form af finansielle ressourcer, infrastruktur (lokaler, faciliteter, udstyr) og eventuelt personale.
- Officiel kommunikation af udpegelsen af databeskyttelsesrådgiveren til alt personale for at sikre, at dennes eksistens og funktion er kendt inden for organisationen.
- Nødvendig adgang til andre afdelinger som personale, juridisk, IT, sikkerhed osv., så databeskyttelsesrådgiverne kan modtage afgørende støtte, input og oplysninger fra disse andre afdelinger.
- Løbende efter- og videreuddannelse. Datasikkerhedsrådgivere skal have mulighed for at holde sig ajour med hensyn til udviklingen inden for databeskyttelse. Målet bør være konstant at øge datasikkerhedsrådgivernes ekspertiseniveau, og de bør tilskyndes til at deltage i kurser om databeskyttelse og andre former for professionel udvikling, såsom at deltage i fora for privatlivets fred, workshops osv.
- Afhængigt af organisationens størrelse og struktur kan det være nødvendigt at oprette et databeskyttelsesrådgivningsteam (en databeskyttelsesrådgiver og dennes personale). I sådanne tilfælde skal teamets interne struktur samt opgaver og ansvar for hvert enkelt medlem være tydeligt fastsat. Tilsvarende, når databeskyttelsesrådgiverens funktion udøves af en ekstern tjenesteyder, kan et team af personer, som arbejder for denne enhed, effektivt udføre databeskyttelsesrådgiverens funktioner som team under en persons ansvar, der er udpeget som overordnet kontakt for kunden.

Generelt forholder det sig således, at jo mere komplekse og/eller følsomme behandlingsprocesserne er, jo flere ressourcer skal databeskyttelsesrådgiveren tildeles. Databeskyttelsesfunktionen skal være effektiv og tilstrækkeligt veludstyret med ressourcer i forhold til den databehandling, som udføres.

3.3. Instruktioner og udøvelsen "af deres hverv på uafhængig vis"

Artikel 38, stk. 3, fastsætter nogle grundlæggende garantier for at sikre, at databeskyttelsesrådgivere er i stand til at udføre deres aktiviteter med tilstrækkelig grad af uafhængighed inden for deres

organisation. Navnlig er dataansvarlige og databehandlere forpligtet til at sikre, at databeskyttelsesrådgiveren "*ikke modtager instrukser vedrørende udførelsen af disse opgaver*". Betragtning 97 tilføjer, at databeskyttelsesrådgivere, "*uanset om de er ansat hos den dataansvarlige eller ej, skal være i stand til at udøve deres hverv på uafhængig vis*".

Dette betyder, at databeskyttelsesrådgivere under opfyldelsen af deres opgaver ifølge artikel 39 ikke må modtage instruktioner om, hvordan de skal behandle en sag, for eksempel hvilket resultat, der skal opnås, hvordan en klage skal undersøges, eller om tilsynsmyndigheden skal høres. Desuden må de ikke instrueres om at have en bestemt opfattelse af et problem relateret til databeskyttelseslovgivningen, for eksempel en bestemt fortolkning af loven.

Databeskyttelsesrådgivernes uafhængighed betyder imidlertid ikke, at de har beslutningskompetence, der strækker sig ud over deres opgaver ifølge artikel 39.

Den dataansvarlige eller databehandleren er stadig ansvarlig for overholdelse af databeskyttelseslovgivningen og skal kunne dokumentere overholdelsen³⁴. Hvis den dataansvarlige eller databehandleren tager beslutninger, som er uforenelige med databeskyttelsesforordningen og databeskyttelsesrådgiverens rådgivning, bør databeskyttelsesrådgiveren have mulighed for at give sin holdning til kende på det højeste ledelsesniveau og til dem, der tager beslutningerne. I denne henseende bestemmer artikel 38, stk. 3, at databeskyttelsesrådgiveren "*rapporterer direkte til det øverste ledelsesniveau hos den dataansvarlige eller databehandleren*". En sådan direkte indberetning sikrer, at seniorledelsen (f.eks. bestyrelsen) er opmærksom på databeskyttelsesrådgiverens indstilling og henstillinger som en del af databeskyttelsesrådgiverens mission om at informere og rådgive den dataansvarlige eller databehandleren. En andet eksempel på direkte indberetning er udarbejdelsen af en årsrapport leveret til det højeste ledelsesniveau om databeskyttelsesrådgiverens aktiviteter.

3.4. Afskedigelse eller straf for udførelse af opgaver som databeskyttelsesrådgiver

Artikel 38, stk. 3, fastlægger, at databeskyttelsesrådgivere "*ikke må afskediges eller straffes af den dataansvarlige eller databehandleren for at udføre [sine] opgaver*".

Dette krav styrker databeskyttelsesrådgiveres uafhængighed og medvirker til at sikre, at de handler uafhængigt og nyder tilstrækkelig beskyttelse i udførelsen af deres databeskyttelsesopgaver.

Sanktioner er kun forbudt i databeskyttelsesforordningen, hvis de er pålagt som et resultat af databeskyttelsesrådgiverens udførelse af sine opgaver i forbindelse med denne funktion. For eksempel kan en databeskyttelsesrådgiver mene, at en bestemt behandling med stor sandsynlighed vil resultere i en høj risiko og råde den dataansvarlige eller databehandlere til at udføre en konsekvensanalyse vedrørende databeskyttelsen, men den dataansvarlige eller databehandleren er uenig med databeskyttelsesrådgiverens vurdering. I en sådan situation kan databeskyttelsesrådgiveren ikke afskediges for denne rådgivning.

Sanktioner kan antage forskellige former og kan være direkte eller indirekte. De kan for eksempel bestå af udebleven eller forsinket forfremmelse, forhindringer for karriereudvikling, udelukkelse fra personalegoder, som andre medarbejdere modtager. Det er ikke nødvendigt, at disse sanktioner faktisk

³⁴ Artikel 5, stk. 2.

udføres; den blotte trussel er tilstrækkelig, så længe de bruges til at straffe databeskyttelsesrådgiveren på grund af årsager relateret til dennes aktiviteter.

Som det gælder for en normal lederstilling, og som det ville være tilfældet for enhver anden medarbejder eller kontrahent under og underlagt gældende national kontrakt-, arbejds- eller strafferet, kan en databeskyttelsesrådgiver stadig afskediges legitimt af andre grunde end udførelsen af opgaverne som databeskyttelsesrådgiver (f.eks. i tilfælde af tyveri, fysisk, psykologisk eller seksuel chikane eller lignende grov forseelse).

I denne forbindelse skal det bemærkes, at databeskyttelsesforordningen ikke specificerer, hvordan og hvornår en databeskyttelsesrådgiver kan afskediges eller erstattes af en anden person. Dog vil det forholde sig sådan, at jo mere stabil en databeskyttelsesrådgivers kontrakt er, og jo flere garantier, der eksisterer mod uberettiget afskedigelse, jo mere sandsynligt vil de være i stand til at handle uafhængigt. Der hilser Artikel 29-gruppen virksomhedernes bestræbelser i denne retning velkommen.

3.5. Interessekonflikter

Artikel 38, stk. 6, tillader databeskyttelsesrådgiveren at "*udføre andre opgaver og have andre pligter*". Artiklen kræver imidlertid, at organisationen sikrer, "*at sådanne opgaver og pligter ikke medfører en interessekonflikt*".

Undgåelse af interessekonflikter er tæt knyttet til kravet om uafhængighed i udførelsen af opgaverne. Selvom det er tilladt databeskyttelsesrådgivere at have andre funktioner, må de kun tildeles andre opgaver og pligter, forudsat at disse ikke giver anledning til interessekonflikter. Dette betyder især, at databeskyttelsesrådgiveren ikke kan have en stilling inden for organisationen, som indebærer, at han eller hun 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 i organisationen omfatte stillinger i seniorledelsen (for eksempel administrerende direktør, teknisk direktør, økonomidirektør, 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. Derudover kan en interessekonflikt også opstå hvis for eksempel en ekstern databeskyttelsesrådgiver anmodes om at repræsentere den dataansvarlige eller databehandleren ved domstolene i sager, som involverer databeskyttelsesspørgsmål.

Afhængigt af organisationens aktiviteter, størrelse og struktur kan det være god praksis for dataansvarlige eller databehandlere at:

- identificere de stillinger, som er uforenelige med databeskyttelsesrådgiverens funktioner
- udarbejde interne regler herom for at udgå interessekonflikter
- inkludere en mere generel forklaring om interessekonflikter
- erklære, at deres databeskyttelsesrådgiver ikke befinder sig i en interessekonflikt med hensyn til funktionen som databeskyttelsesrådgiver med henblik på at øge bevidstheden om dette krav
- inkludere sikkerhedsforanstaltninger i organisationens interne regler og sikre, at opslaget af stillingen som databeskyttelsesrådgiver eller tjenesteydelseskontrakten er tilstrækkeligt præcist og detaljeret til at undgå en interessekonflikt. I denne sammenhæng bør det også tages i

betragtning, at interessekonflikter kan antage forskellige former afhængigt af, om databeskyttelsesrådgiveren er rekrutteret internt eller eksternt.

4 Databeskyttelsesrådgiverens opgaver

4.1. Overvågning af overholdelse af databeskyttelsesforordningen

Artikel 39, stk. 1, litra b), overdrager blandt andet databeskyttelsesrådgiverne opgaven med at overvåge overholdelsen af databeskyttelsesforordningen. Betragtning 97 anfører yderligere, at databeskyttelsesrådgivere skal "*bistå den dataansvarlige eller databehandleren med at overvåge den interne overholdelse af denne forordning*".

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 rette henstillinger til den dataansvarlige eller databehandleren.

Overvågning af overholdelse betyder ikke, at det er databeskyttelsesrådgiveren, som er personligt ansvarlig i tilfælde af manglende overholdelse. Databeskyttelsesforordningen gør det klart, at det er den dataansvarlige og ikke databeskyttelsesrådgiveren, som skal sikre og være i stand til at demonstrere, at databehandlingen gennemføres med "*passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning*" (artikel 24, stk. 1). Ansvar for overholdelse af databeskyttelsesbestemmelserne er den databeskyttelsesansvarliges virksomheds ansvar, ikke databeskyttelsesrådgiverens.

4.2. Databeskyttelsesrådgiverens rolle i konsekvensanalyse vedrørende databeskyttelse

Ifølge artikel 35, stk. 1, er det den dataansvarliges opgave, og ikke databeskyttelsesrådgiverens, at udføre en konsekvensanalyse vedrørende databeskyttelsen, hvis nødvendigt. Databeskyttelsesrådgiveren kan imidlertid spille en meget vigtig og nyttig rolle med at bistå den dataansvarlige. Ifølge princippet om indbygget databeskyttelse kræver artikel 35, stk. 2, udtrykkeligt, at den dataansvarlige "*rådfører sig*" med databeskyttelsesrådgiveren, når der udføres en konsekvensanalyse vedrørende databeskyttelsen. Artikel 39, stk. 1, litra c), tildeler til gengæld databeskyttelsesrådgiveren pligt til at "*rådgive, når der anmodes herom, med hensyn til konsekvensanalysen vedrørende databeskyttelse og overvåge dens opfyldelse i henhold til artikel 35*".

Artikel 29-gruppen anbefaler, at den dataansvarlige søger rådgivning hos databeskyttelsesrådgiveren om blandt andet følgende spørgsmål³⁵:

- om der skal gennemføres en konsekvensanalyse vedrørende databeskyttelse
- hvilken metode, der skal følges, ved gennemførelsen af en konsekvensanalyse vedrørende databeskyttelse

³⁵ Artikel 39, stk. 1, nævner databeskyttelsesrådgiverens opgaver, og at databeskyttelsesrådgiveren "*som minimum*" skal have følgende opgaver. Der er således intet til hinder for, at den dataansvarlige tildeler databeskyttelsesrådgiveren andre opgaver end dem, der udtrykkeligt er nævnt i artikel 39, stk. 1, eller angiver disse opgaver i en mere detaljeret form.

- 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.

Hvis den dataansvarlige er uenig med databeskyttelsesrådgiverens rådgivning, skal dokumentationen for konsekvensanalysen for databeskyttelse indeholde en skriftlig begrundelse for, hvorfor rådgivningen ikke er blevet fulgt³⁶.

Artikel 29-gruppen anbefaler endvidere, at den dataansvarlige i for eksempel databeskyttelsesrådgiverens kontrakt, men også i oplysningerne til medarbejdere, ledelse (og andre interessenter, hvor det er relevant) oplyser nøjagtigt, hvad databeskyttelsesrådgiverens opgaver er og deres formål, navnlig hvad angår udførelsen af konsekvensanalysen vedrørende databeskyttelse.

4.3. Samarbejde med tilsynsmyndigheden og funktion som kontaktpunkt

Ifølge artikel 39, stk. 1, litra d), og litra e), skal databeskyttelsesrådgiveren "*samarbejde med tilsynsmyndigheden*" og "*fungere som tilsynsmyndighedens kontaktpunkt i spørgsmål vedrørende behandling, herunder den forudgående høring, der er omhandlet i artikel 36, og til at høre når det er hensigtsmæssigt, om eventuelle andre spørgsmål.*"

Disse opgaver refererer til databeskyttelsesrådgiverens rolle som "formidler" som nævnt i indledningen til disse retningslinjer. Databeskyttelsesrådgiveren fungerer som kontaktpunkt for at lette tilsynsmyndighedens adgang til dokumenter og oplysninger om udførelsen af de opgaver, der er nævnt i artikel 57, samt om udførelsen af tilsynsmyndighedens undersøgende, korrigerende, godkendende og rådgivende beføjelser som nævnt i artikel 58. Som allerede nævnt, er databeskyttelsesrådgiveren underlagt tavshedspligt eller fortrolighed vedrørende udførelsen af sine opgaver i overensstemmelse med EU-lovgivningen eller medlemsstaternes nationale lovgivning (artikel 38, stk. 5). Dog forbyder tavshedspligten og fortroligheden ikke databeskyttelsesrådgiveren at kontakte og søge rådgivning hos tilsynsmyndigheden. Artikel 39, stk. 1, litra e), bestemmer, at databeskyttelsesrådgiveren kan høre tilsynsmyndigheden om ethvert spørgsmål, hvor det er relevant.

4.4. Risikobaseret tilgang

Artikel 39, stk. 2, kræver, at databeskyttelsesrådgiveren "*under udførelsen af sine opgaver (tager) behørigt hensyn til den risiko, der er forbundet med behandlingsaktiviteter, under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål.*"

Denne artikel henviser til et generelt princip om sund fornuft, som kan være relevant for mange aspekter af en databeskyttelsesrådgivers daglige arbejde. Grundlæggende kræves det, at

³⁶ Artikel 24, stk. 1, fastslår, at "*under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning. Disse foranstaltninger skal om nødvendigt revideres og ajourføres.*"

databeskyttelsesrådgivere kan prioritere deres aktiviteter og fokusere deres indsats på spørgsmål, som indebærer større risici for databeskyttelsen. Dette betyder ikke, at de bør forsømme kontrollen med overholdelse for databehandlingsprocesser, som indebærer et forholdsvist lavere risikoniveau. Det betyder, at de først og fremmest skal fokusere på områderne med større risiko.

Denne selektive og pragmatiske tilgang bør hjælpe databeskyttelsesrådgivere i deres rådgivning af den dataansvarlige med at beslutte hvilken metode, der skal anvendes til udførelsen af konsekvensanalysen vedrørende databeskyttelse, hvilke områder, der skal gøres til genstand for intern eller eksternt revision af databeskyttelsen, hvilke interne uddannelsesaktiviteter, der skal gives til personale eller ledelse, der er ansvarlig for databehandlingsaktiviteter, og hvilke databehandlingsaktiviteter databeskyttelsesrådgiveren skal afsætte mere eller mindre tid til.

4.5. Databeskyttelsesrådgiverens rolle i føring af fortegnelser

I henhold til artikel 30, stk. 1, og stk. 2, er det den dataansvarlige eller databehandleren, og ikke databeskyttelsesrådgiveren, som skal føre "*fortegnelser over behandlingsaktiviteter under deres ansvar*" eller "*fortegnelser over alle kategorier af behandlingsaktiviteter, der foretages på vegne af en dataansvarlig*".

I praksis opretter databeskyttelsesrådgivere ofte oversigter og fører fortegnelser over databehandlingsaktiviteterne baseret på oplysninger, som de modtager fra de forskellige afdelinger i deres organisation, som er ansvarlige for behandling af personoplysninger. Denne praksis er blevet etableret under mange nuværende nationale love og under de databeskyttelsesregler, der finder anvendelse for EU-institutioner og -organer³⁷.

Artikel 39, stk. 1, indeholder en liste over opgaver, som databeskyttelsesrådgiveren skal have som minimum. Der er derfor intet til hinder for, at den dataansvarlige eller databehandleren tildeler databeskyttelsesrådgiveren opgaven med at føre fortegnelser over databehandlingsaktiviteterne under den dataansvarliges eller databehandlerens 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.

Under alle omstændigheder bør fortegnelsen, som skal føres i henhold til artikel 30, også ses som et værktøj, som giver den dataansvarlige og på anmodning den tilsynsførende myndighed en oversigt over alle de databehandlingsaktiviteter, som en organisation udfører på personoplysninger. Forteignelsen er således en forudsætning for overholdelse og som sådan en effektivt ansvarlighedsmåler.

³⁷ Artikel 24, stk. 1, litra d), i forordning (EF) nr. 45/2001.

5 BILAG – RETNINGSLINJER VEDRØRENDE DATABESKYTTELSESRÅDGIVERE: HVAD DU BEHØVER AT VIDE

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 databeskyttelsesrådgiver

1 Hvilke organisationer skal udpege en databeskyttelsesrådgiver?

Udpegelse af en databeskyttelsesrådgiver er obligatorisk:

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

Bemærk, at EU- eller medlemsstatslovgivning eventuelt også kan kræve udpegelse af databeskyttelsesrådgivere i andre situationer. Selvom udnævnelse af en databeskyttelsesrådgiver ikke er obligatorisk, kan organisationer undertiden finde det nyttigt at udpege en sådan rådgiver på frivillig basis. Artikel 29-gruppen vedrørende databeskyttelse tilskynder til denne frivillige indsats. Når en organisation udpeger en databeskyttelsesrådgiver på frivillig basis, gælder kravene til hans eller hendes udpegelse, stilling og opgaver, som hvis udpegelsen havde været obligatorisk.

Kilde: Artikel 37, stk. 1, i databeskyttelsesforordningen

2 Hvad betyder kerneaktiviteter?

"Kerneaktiviteter" kan betragtes som de centrale aktiviteter, der er nødvendige for at nå 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 standard databehandling som støtte i deres aktiviteter. Disse er eksempler på nødvendige støttefunktioner for organisationens kerneaktiviteter eller hovedvirksomhed. Selvom disse aktiviteter er nødvendige eller vigtige, så betragtes de normalt som biaktiviteter snarere end kerneaktiviteter.

Kilde: Artikel 37, stk. 1, litra b) og c), i databeskyttelsesforordningen

3 Hvad betyder "stort omfang"?

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 gennemføres databehandling 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

Kilde: Artikel 37, stk. 1, litra b) og c), i databeskyttelsesforordningen

4 Hvad betyder "regelmæssig og systematisk" overvågning?

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.

Eksempler på aktiviteter, der kan udgøre regelmæssig og systematisk overvågning af registrerede: drift af et telekommunikationsnet, levering af telekommunikationstjenester, e-mail-retargeting, datadrevne marketingaktiviteter, 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.

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.

Kilde: Artikel 37, stk. 1, litra b), i databeskyttelsesforordningen

5 Kan organisationer udpege en fælles databeskyttelsesrådgiver? I bekræftende fald, på hvilke betingelser?

Ja. En koncern kan udnævne en fælles databeskyttelsesrådgiver, forudsat at vedkommende er "*let tilgængelig fra hver enkel virksomhed*". Begrebet om 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, uanset om denne er intern eller ekstern, er tilgængelig, er det vigtigt at sikre, at dennes kontaktoplysninger er tilgængelige. Databeskyttelsesrådgiveren skal, eventuelt med hjælp af et team, være i stand til effektivt at kunne kommunikere med de registrerede og samarbejde med de kompetente tilsynsmyndigheder. Dette betyder, at denne kommunikation skal finde sted på det eller de sprog, som anvendes af tilsynsmyndighederne og de registrerede. Databeskyttelsesrådgiverens 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.

Flere myndigheder eller organer kan udpege en fælles databeskyttelsesrådgiver under hensyntagen til deres organisationsstruktur og størrelse. De samme overvejelser gælder med hensyn til ressourcer og kommunikation. I betragtning af, at databeskyttelsesrådgiveren er ansvarlig for en række opgaver, skal den dataansvarlige eller databehandleren sikre, at en enkelt databeskyttelsesrådgiver, eventuelt med hjælp af et team, effektivt kan udføre sine opgaver trods udpegelsen til flere offentlige myndigheder og organer.

Kilde: Artikel 37, stk. 2 og 3, i databeskyttelsesforordningen

6 Hvor bør databeskyttelsesrådgiveren være placeret?

Artikel 29-gruppen anbefaler, at databeskyttelsesrådgiveren, for at være tilgængelig, placeres inden for EU, uanset om den dataansvarlige eller databehandleren er etableret i Den Europæiske Union. Dog kan det ikke udelukkes, at databeskyttelsesrådgiveren i nogle situationer, hvor den dataansvarlige eller databehandleren ikke har nogen etablering inden for EU, kan være i stand til at udføre sine aktiviteter mere effektivt, hvis vedkommende er placeret uden for EU.

7 Er det muligt at udpege en ekstern databeskyttelsesrådgiver?

Ja. Databeskyttelsesrådgiveren kan 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.

Når databeskyttelsesrådgiverens funktion udøves af en ekstern tjenesteyder, kan et team af personer, som arbejder for denne enhed, effektivt udføre databeskyttelsesrådgiverens funktioner som team under ansvar af en udpeget hovedkontakt og "ansvarlig person" over for kunden. I dette tilfælde er det vigtigt, at hvert enkelt medlem af organisationen, som udøver funktionerne som databeskyttelsesrådgiver, opfylder alle gældende krav i databeskyttelsesforordningen.

Af hensyn til juridisk klarhed og god organisation og for at forebygge interessekonflikter for teammedlemmerne, anbefaler retningslinjerne, at der i tjenesteydelseskontrakten gives en klar fordeling af opgaverne i den eksterne databeskyttelsesrådgiver team, samt at der udpeges en enkelt person som overordnet kontakt og "ansvarlig" for kunden.

Kilde: Artikel 37, stk. 6, i databeskyttelsesforordningen

8 Hvilke faglige kvalifikationer bør databeskyttelsesrådgiveren have?

Databeskyttelsesrådgiveren udpeges på grundlag af sine faglige kvalifikationer, navnlig ekspertise inden for databeskyttelsesret og -praksis samt evne til at udføre sine opgaver.

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 større grad af ekspertise og støtte.

Relevante færdigheder og ekspertise 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.

Kilde: Artikel 37, stk. 5, i databeskyttelsesforordningen

Databeskyttelsesrådgiverens stilling

9 Hvilke ressourcer bør den dataansvarlige eller databehandleren give til databeskyttelsesrådgiveren?

Databeskyttelsesrådgiveren skal have de nødvendige ressourcer til at kunne udføre sine opgaver.

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

Kilde: Artikel 38, stk. 2, i databeskyttelsesforordningen

10 Hvilke garantier sikrer, at databeskyttelsesrådgiveren kan udføre sine opgaver uafhængigt? Hvad betyder "interessekonflikt"?

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

- 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

Databeskyttelsesrådgiverens andre opgaver og pligter må ikke resultere i en interessekonflikt. Dette betyder især, at databeskyttelsesrådgiveren ikke kan have en stilling inden for organisationen, som indebærer, at han eller hun 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 i organisationen omfatte stillinger i seniorledelsen (for eksempel administrerende direktør, teknisk direktør, økonomidirektør, 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. Derudover kan en interessekonflikt også opstå hvis for eksempel en ekstern databeskyttelsesrådgiver anmodes om at repræsentere den dataansvarlige eller databehandleren ved domstolene i sager, som involverer databeskyttelsesspørgsmål.

Kilde: Artikel 38, stk. 3, og artikel 38, stk. 6, i databeskyttelsesforordningen

11 Hvad betyder "overvågning af overholdelse"?

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 rette henstillinger til den dataansvarlige eller databehandleren.

Kilde: Artikel 39, stk. 1, litra b), i databeskyttelsesforordningen

12 Er databeskyttelsesrådgiveren personligt ansvarlig for manglende overholdelse af kravene til databeskyttelse?

Nej, databeskyttelsesrådgivere er ikke personligt ansvarlige for manglende overholdelse af kravene til databeskyttelse. Det er den dataansvarlige eller databehandleren, som skal sikre og være i stand til at demonstrere, at databehandlingen udføres i overensstemmelse med denne forordning. Ansvar for overholdelse af databeskyttelsesbestemmelserne påhviler den dataansvarlige eller databehandleren.

13 Hvilken rolle spiller databeskyttelsesrådgiveren med hensyn til vurdering af konsekvensanalyse vedrørende databeskyttelse og fortegnelser over databehandlingsaktiviteter?

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

- om der skal gennemføres en konsekvensanalyse vedrørende databeskyttelse
- hvilken metode der skal følges ved gennemførelsen 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 korrekt udført, og hvorvidt dens konklusioner (om databehandlingen skal fortsætte, og hvilke garantier der skal anvendes) er i overensstemmelse med kravene til databeskyttelse

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 eller databehandlerens ansvar. Sådanne fortegnelser bør betragtes som et af de værktøjer, der sætter databeskyttelsesrådgiveren i stand til at udføre sine opgaver med at overvåge overholdelsen, informere og rådgive den dataansvarlige eller databehandleren.

Kilde: Artikel 39, stk. 1, litra c) og artikel 30 i databeskyttelsesforordningen

Udfærdiget i Bruxelles, den 13. december 2016

*På gruppens vegne,
Formanden*

Isabelle FALQUE-PIERROTIN

Senest revideret og vedtaget den 5. april 2017

*På gruppens vegne
Formanden*

Isabelle FALQUE-PIERROTIN