Koncernservice
Økonomiforvaltningen

Orienteringssag

Til Økonomiudvalget

Orientering om afgørelse fra Datatilsynet vedr. klage over behandling af personoplysninger

21. august 2020

Sagsnummer
2020-0197571

Dokumentnummer
2020-0197571-1

Sagsbehandler
Nina Devantier

Resumé
Datatilsynet har udtalt alvorlig kritik af Københavns Kommune (KK) i en sag om et databrud fra januar 2019. Databruddet relaterer sig til Koncernservices (KS) implementering af KK's sagsbehandlingssystem, ServiceNow, hvor en menneskelig fejl gjorde, at en testsag blev behandlet på en fratrådt medarbejder. KS har sidenhen implementeret skærpede retningslinjer og øget fokus på datasikkerhed i testsituationer, hvorfor en lignende hændelse ikke forventes at ske igen. Notatet er til orientering.

Problemstilling
Databruddet er sket i januar 2019 i forbindelse med test af KK's nye sagsbehandlingssystem, ServiceNow. Her blev en testsag ved en menneskelig fejl behandlet på en fratrådt medarbejder.

KS har efter databruddet udarbejdet et forbedret testkoncept, der sikrer, at tests kun udføres af udvalgte uddannede medarbejdere og med data fra medarbejdere, der har afgivet skriftligt samtykke.

Datatilsynets kritik baserer sig på tre af databeskyttelsesforordningens artikler:

1. KK har fejlagtigt benyttet den fratrådte medarbejder, der nu har klaget over KK, som testperson uden samtykke og har dermed ikke levet op til kravet om at gennemføre passende sikkerhedsforanstaltninger ved brug af persondata (artikel 32, stk. 1).
2. KK har ikke været effektiv nok i forhold til at sikre, at fejlen blev berigtiget i hele aktørkæden (artikel 5, stk. 1, litra a).
3. KK har ikke levet op til kravet om at anmelde datasikkerhedsbrud uden unødig forsinkelse og om muligt senest 72 timer efter bruddet er sket (artikel 33, stk. 1).

Af Datatilsynets afgørelse fremgår det fejlagtigt, at der er tale om afprøvning af et nyt refusionssystem. Dette er ikke korrekt, idet der rettelig er tale om KS' sagsbehandlingssystem ServiceNow.

Koncernservice
Analyse og Stab
Borups Allé 177
2400 København NV

EAN-nummer
5798009809124

Datatilsynet har i deres afgørelse noteret sig, at KK har skærpet proces og retningslinjer for test, heriblandt korrekt mærkning og sletning af testsager samt indhentning af samtykke. Herudover at KK har skærpet opmærksomheden på pligten til at anmelde sikkerhedsbrud.

Økonomi
Ikke relevant.

Videre proces
Med KS' retningslinjer for brug af persondata til tests forventes en lignende situation ikke at kunne opstå igen.

Datatilsynet har meddelt, at de anser sagen for afsluttet og ikke foretager sig yderligere i sagen.

Bilag
Bilag 1: Afgørelsen fra Datatilsynet er vedlagt til orientering (fremgår i anonymiseret form).

DATATILSYNET

Københavns Kommune
Rådhuspladsen 1
1599 København V

Sendt med Digital Post

5. august 2020

J.nr. 2019-32-0629
Dok.nr. 208777
Sagsbehandler
Ditte Koefoed

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk

CVR 11883729

Klage over behandling af personoplysninger

Datatilsynet vender hermed tilbage til sagen, hvor [x] den 11. februar 2019 har klaget til tilsynet over Københavns Kommunes behandling af personoplysninger.

1. Afgørelse

Efter en gennemgang af sagen finder Datatilsynet, at der er grundlag for at udtale **alvorlig kritik** af, at Københavns Kommunes behandling af personoplysninger ikke er sket i overensstemmelse med reglerne i databeskyttelsesforordningens[1] artikel 32, stk. 1, artikel 5, stk. 1, litra a, og artikel 33, stk. 1.

Nedenfor følger en nærmere gennemgang af sagen og en begrundelse for Datatilsynets afgørelse.

2. Sagsfremstilling

Det fremgår af sagen, at klager var ansat i Københavns Kommune, og at hun i oktober 2018 fratrådte sin stilling. Klager modtog efterfølgende – blandt andet den 18. december 2018, 7. januar 2019 og den 23. januar 2019 – flere skrivelser fra Udbetaling Danmark om, at Københavns Kommune, som hendes arbejdsgiver, havde indberettet, at hun var sygemeldt på grund af graviditet, selvom hun hverken var sygemeldt eller gravid.

Klager rettede henvendelse til Københavns Kommune den 7. januar 2019 angående fejlen.

[1] Europa-Parlamentets og Rådets forordning (EU) 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 (generel forordning om databeskyttelse).

Københavns Kommune har oplyst, at kommunen i 2018 implementerede et nyt sagsbehandlingssystem, ServiceNow. Der blev i forbindelse med test af produktionsmiljøet i systemet benyttet testpersoner.

Der blev i den forbindelse givet adgang til at indrapportere for en lille organisatorisk enhed på under 10 medarbejdere. Medarbejderne i enheden fik ret til at foretage indberetninger af testpersonerne men ikke til at få adgang til at tilgå oplysninger om dem. Forud for testen blev der indhentet samtykkeerklæringer fra 14 relevante ledere og medarbejdere i forhold til at måtte benytte disse i test i produktion. Alle medarbejdere i enheden gav samtykke til at indgå i testen. I systemet er der imidlertid adgang til at indberette på medarbejdere, der er fratrådt op til seks måneder tidligere, hvilket Københavns Kommune har oplyst kan være nødvendigt for at håndtere ferie og lignende.

På grund af en menneskelig fejl var klager blevet benyttet som testperson i forbindelse med test af produktionsmiljøet i sagsbehandlingssystemet. Fejlen skyldtes, at den pågældende medarbejder, som oprettede klager som testperson, ikke handlede i overensstemmelse med Københavns Kommunes retningslinjer.

Den fejloprettede testsag blev ved endnu en fejl ikke slettet inden idriftsættelse af systemet, hvorfor testsagen i december 2018 blev sagsbehandlet. Københavns Kommune videregav i den forbindelse urigtige oplysninger til Udbetaling Danmark om, at klager var syg og gravid.

Københavns Kommune har oplyst, at det følger af lovgrundlaget for sagsbehandling af graviditetsbetinget sygdom, at oplysninger herom kan sendes til Udbetaling Danmark, som generelt håndterer disse oplysninger for arbejdsgivere. Myndigheder, herunder Københavns Kommune og Udbetaling Danmark, kan udveksle oplysninger, når det er nødvendigt for at behandle en sag. Videregivelse af den fejlagtige oplysning for klager til Udbetaling Danmark er således en konsekvens af den sagsbehandling, som normalt finder sted ved behandling af graviditetsbetinget sygdom. Oplysningerne blev sendt til Udbetaling Danmark via systemet virk.dk.

Københavns Kommune har endvidere oplyst, at foranlediget af klagers henvendelse til kommunen den 7. januar 2019, blev oplysningerne om klager rettet i kommunens lønsystem og i virk.dk., hvorfra de tilrettede oplysninger automatisk gik videre til Udbetaling Danmark. Oplysningerne var hermed – ifølge kommunen – blevet berigtiget i hele kæden af aktører. Foranlediget af Datatilsynets henvendelse af 1. april 2019, har kommunen den 4. april 2019 kontaktet Udbetaling Danmark, som bekræftede, at oplysningerne var berigtigede i deres systemer. Kommunen er ikke bekendt med, at oplysningerne er sendt til andre aktører.

Klager har ved e-mail af 16. januar 2020 til Datatilsynet oplyst, at der på borger.dk fortsat fremgår fejlagtige oplysninger om, at hun har forventet termin den 7. januar 2019.

Københavns Kommune har i den forbindelse oplyst, at kommunen ikke har mulighed for at berigtige oplysninger, der behandles på borger.dk. Foranlediget af Datatilsynets henvendelse af 17. marts 2020 kontaktede Københavns Kommune derfor Udbetaling Danmark og Digitaliseringsstyrelsen med henblik på at få den fejlagtige oplysning fjernet. Ifølge Digitaliseringsstyrelsen skulle rettelsen foretages af Udbetaling Danmark, da oplysningen på borger.dk var hentet fra denne myndighed.

Københavns Kommune har endvidere oplyst, at Udbetaling Danmark den 20. marts 2020 telefonisk meddelte kommunen, at myndigheden efter kommunen den 7. januar 2019 anmodede om at sagen blev slettet, i stedet annullerede sagen. Ved annulleringen blev alle fremtidige konsekvenser ved sagen stoppet. Oplysningen "Forventet fødsel/Faktisk fødselsdato" blev

imidlertid ikke slettet. Udbetaling Danmark har den 20. marts 2020 slettet oplysningen, hvilket ifølge Udbetaling Danmark er slået igennem per 23. marts 2020.

2.1. Klagers bemærkninger

Klager har overordnet anført, at Københavns Kommunes behandling af personoplysninger om hende har været uberettiget.

Klager har endvidere anført, at klager den 7. januar 2019 rettede henvendelse til sin arbejdsgiver – Københavns Kommunes Økonomiforvaltning – vedrørende de breve, hun havde modtaget fra Udbetaling Danmark. Klagers tidligere teamleder beklagede i et svar af 10. januar 2019 til klager, at klager var registreret hos Udbetaling Danmark og Borger.dk som sygemeldt grundet graviditet, og at økonomiforvaltningen havde anvendt klagers personoplysninger i forbindelse med afprøvning af et nyt refusionssystem. En uge senere modtog klager et nyt brev fra Udbetaling Danmark, hvor hun fejlagtigt stod registreret som værende på barselsorlov og med forventet termin den 7. januar 2019. Klager modtog herefter breve ca. hver tredje uge med anmodninger om besvarelser af spørgsmål vedrørende graviditet og orlov.

2.2. Københavns Kommunes bemærkninger

Københavns Kommune har anført, at det var nødvendigt at gennemføre enkelte afsluttende tests op til "go live" i produktionsmiljøet i det pågældende sagsbehandlingssystem. Testcases skulle ske med skriftligt samtykke, og kommunen havde udarbejdet retningslinjer for overholdelse af de databeskyttelsesretlige regler i relation til implementering af det nye sagsbehandlingssystem, men i forbindelse med de afsluttende tests skete der en menneskelig fejl, hvorved retningslinjerne ikke blev overholdt. Fejlen bestod i, at der blev oprettet en testsag vedrørende graviditetsbetinget fravær omhandlende klager uden den påkrævede samtykkeerklæring og dermed uden hjemmel. Denne fejl medførte efterfølgende en række utilsigtede følgevirkninger.

Københavns Kommune har endvidere anført, at da kommunen blev bekendt med fejlen, kontaktede kommunen klager og orienterede hende om, at oplysningerne blev rettet med det samme. Klager kontaktede Koncernservice i kommunen via en tillidsrepræsentant den 7. januar 2019, og den 10. januar 2019 videresendte tillidsrepræsentanten henvendelsen til en ledelsesrepræsentant. Klager blev samme dag kontaktet, og oplysningerne blev berigtiget via Virk.dk. Herudover blev klager orienteret om at smide brevene fra Udbetaling Danmark ud.

Der har ifølge Københavns Kommune ikke været andre konsekvenser for klager, end at terminsdatoen fortsat har fremgået af borger.dk. Københavns Kommune har i den forbindelse bemærket, at de eneste, der kan tilgå en borgers side på borger.dk, er Udbetaling Danmark og borgeren selv. Der er derfor ikke andre, der kan have fået adgang til oplysningen, ligesom Københavns Kommune ikke har haft mulighed for at følge op på, om sletningen gik igennem.

For så vidt angår de tiltag Københavns Kommune har implementeret for at undgå fremtidige lignende fejl, har kommunen oplyst, at vigtigheden af overholdelsen af retningslinjerne for det nye sagsbehandlingssystem er indskærpet over for testmedarbejderne, ligesom kommunen også har skærpet proces og retningslinjer for udvælgelse af testpersoner og korrekt mærkning og sletning af testsager.

Københavns Kommune har afslutningsvis anført, at kommunen ikke har anmeldt hændelsen til Datatilsynet i begyndelsen af 2019 grundet manglende opmærksomhed på Københavns Kommunes interne indrapporteringskrav, og det forhold at hændelsen skyldes en fejl, der umiddelbart blev forsøgt rettet, uden den fornødne opmærksomhed på, at der var tale om et sikkerhedsbrud. At Københavns Kommune ikke har anmeldt bruddet til Datatilsynet efter tilsynets henvendelse den 1. april 2019 skyldes, at Københavns Kommune vurderede, at Datatil-

synet på daværende tidspunkt var bekendt med hændelsen. I forlængelse heraf var Københavns Kommunes opfattelse, at forpligtelsen til at foretage anmeldelse efter artikel 33 ikke længere var relevant. Kommunen vurderede på baggrund heraf, at hændelsen allerede var registreret hos Datatilsynet. Kommunen har dog skærpet opmærksomheden på datasikkerhed og for pligten til at anmelde sikkerhedsbrud.

3. Begrundelse for Datatilsynets afgørelse

Datatilsynet finder, at Københavns Kommune – ved fejlagtigt at have benyttet klager som testperson i produktionsmiljøet i sagsbehandlingssystemet, ServiceNow, hvormed oplysninger om klager uberettiget er blevet videregivet til Udbetaling Danmark – ikke har levet op til kravet om at gennemføre passende sikkerhedsforanstaltninger i databeskyttelsesforordningens artikel 32, stk. 1.

Datatilsynet finder endvidere, at Københavns Kommune ved først at rette direkte henvendelse til Udbetaling Danmark 87 dage efter klagers henvendelse, ikke har levet op til databeskyttelsesforordningens artikel 5, stk. 1, litra a.

Datatilsynet finder endelig, at Københavns Kommune ikke har levet op til kravet om at anmelde bruddet på persondatasikkerheden uden unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med bruddet, jf. databeskyttelsesforordningens artikel 33, stk. 1.

Datatilsynet finder på den baggrund anledning til at udtale **alvorlig kritik** af, at Københavns Kommunes behandling af personoplysninger ikke er sket i overensstemmelse med databeskyttelsesforordningens artikel 32, stk. 1, artikel 5, stk. 1, litra a, og artikel 33, stk. 1.

Datatilsynet har i den forbindelse lagt vægt på, **at** der er sket en fejlregistrering af en testsag med klagers oplysninger i ServiceNow-systemet, **at** testsagen ved endnu en fejl ikke blev slettet inden idriftsættelse af systemet, **at** fejlregistreringen har medført, at oplysninger om klager uberettiget er blevet videregivet til uvedkommende, og **at** fejlregistreringen har medført en risiko for kompromittering af klagers rettigheder, idet der er blevet videregivet urigtige oplysninger om, at klager er gravid og sygemeldt, hvormed klager er blevet tilknyttet sager hos myndigheder, som hun ikke har haft reel tilknytning til.

Datatilsynet har endvidere lagt vægt på, **at** det er tilsynets opfattelse, at den dataansvarlige i medfør af princippet om rimelighed i artikel 5, stk. 1, litra a, – hvis personoplysninger er kommet til uvedkommendes kendskab – skal sørge for at rydde op efter fejlen eller sikkerhedsbristen og søge at begrænse skadevirkningerne heraf. Ved uberettiget videregivelse skal den dataansvarlige eksempelvis sikre, at data bliver slettet eller eventuelt afhentet eller returneret fra uberettigede modtagere. Datatilsynet har derved lagt vægt på, **at** Københavns Kommune ikke umiddelbart efter, at kommunen den 7. januar 2019 blev bekendt med sikkerhedsbruddet, rettede direkte henvendelse til Udbetaling Danmark. Datatilsynet skal i den forbindelse understrege, at en dataansvarlig som udgangspunkt ikke alene ved gennemførelse af foranstaltninger i egne systemer – i dette tilfælde virk.dk og lønsystemet – kan forudsætte, at foranstaltningerne også effektivt gennemføres i de uberettigede modtageres systemer. Den dataansvarlige skal som udgangspunkt rette en konkret og direkte henvendelse til de uberettigede modtagere angående fejlen.

Datatilsynet har endelig lagt vægt på, **at** alle brud på persondatasikkerheden som udgangspunkt skal anmeldes til Datatilsynet inden for 72 timer, og **at** Københavns Kommune ikke anmeldte bruddet til Datatilsynet 72 timer efter klagers henvendelse den 7. januar 2019.

Datatilsynet bemærker, at bruddet konkret indebar en risiko for klager, hvorfor undtagelsen i artikel 33, stk. 1 – hvorefter anmeldelse af brud kan undlades, hvis det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, der kan fritage for anmeldelse – ikke er opfyldt.

Datatilsynet har for så vidt angår valg af reaktion i formildende retning lagt vægt på, at der er tale om et enkeltstående tilfælde, og at der har været en meget lille gruppe testpersoner. I skærpende retning har tilsynet lagt vægt på karakteren af overtrædelserne, herunder at det var to uafhængige af hinanden fejl, der medførte sikkerhedsbruddet, ligesom tilsynet har lagt vægt på, at risikoen ved sikkerhedsbrud ved oprettelse af testsager var høj, idet testsagen medfører en automatiseret proces, der knytter sig til oprettelsen af sager hos myndigheder, som kan have retsvirkninger for de pågældende.

Datatilsynet har noteret sig, at Københavns Kommune har indskærpet vigtigheden af overholdelse af retningslinjerne for det nye sagsbehandlingssystem over for testmedarbejderne. Datatilsynet har endvidere noteret sig, at kommunen har skærpet proces og retningslinjer for udvælgelse af testpersoner og korrekt mærkning og sletning af testsager, og at kommunen har skærpet opmærksomheden på pligten til at anmelde sikkerhedsbrud.

4. Afsluttende bemærkninger

Datatilsynet beklager den lange sagsbehandlingstid, der skyldes stor travlhed i tilsynet.

Datatilsynet skal oplyse, at Københavns Kommune i denne sag ikke skal foretage særskilt anmeldelse af det skete brud på persondatasikkerheden. Datatilsynet har i den forbindelse lagt vægt på, at bruddet er tilstrækkeligt belyst i forbindelse med sagens behandling i tilsynet.

Kopi af dette brev sendes dags dato til klager til orientering.

Datatilsynets afgørelser kan indbringes for domstolene i medfør af grundlovens § 63.

Datatilsynet anser hermed sagen for afsluttet og foretager sig herefter ikke yderligere i sagen.

Med venlig hilsen

Ditte Koefoed

Bilag: Retsgrundlag.

Bilag: Retsgrundlag

Uddrag af Europa-Parlamentets og Rådets forordning (EU) 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 (generel forordning om databeskyttelse).

Artikel 2, stk. 1. Denne forordning finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Artikel 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; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål (»formålsbegrænsning«)
c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (»dataminimering«)
d) være korrekte og om nødvendigt ajourførte; 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 (»rigtighed«)
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; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder (»opbevaringsbegrænsning«)
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 (»integritet og fortrolighed«).

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

Artikel 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:

a) pseudonymisering og kryptering af personoplysninger
b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

Stk. 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 personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Stk. 3. Overholdelse af en godkendt adfærdskodeks som omhandlet i artikel 40 eller en godkendt certificeringsmekanisme som omhandlet i artikel 42 kan bruges som et element til at påvise overholdelse af kravene i nærværende artikels stk. 1.

Stk. 4. Den dataansvarlige og databehandleren tager skridt til at sikre, at enhver fysisk person, der udfører arbejde for den dataansvarlige eller databehandleren, og som får adgang til personoplysninger, kun behandler disse efter instruks fra den dataansvarlige, medmindre behandling kræves i henhold til EU-retten eller medlemsstaternes nationale ret.

Artikel 33. Ved brud på persondatasikkerheden anmelder den dataansvarlige uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, bruddet på persondatasikkerheden til den tilsynsmyndighed, som er kompetent i overensstemmelse med artikel 55, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Foretages anmeldelsen til tilsynsmyndigheden ikke inden for 72 timer, ledsages den af en begrundelse for forsinkelsen.

Stk. 2. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden.

Stk. 3. Den i stk. 1 omhandlede anmeldelse skal mindst:

a) beskrive karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
b) angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
c) beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden
d) beskrive de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

Stk. 4. Når og for så vidt som det ikke er muligt at give oplysningerne samlet, kan oplysningerne meddeles trinvist uden unødig yderligere forsinkelse.

Stk. 5. Den dataansvarlige dokumenterer alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne afhjælpende foranstaltninger. Denne dokumentation skal kunne sætte tilsynsmyndigheden i stand til at kontrollere, at denne artikel er overholdt.