KØBENHAVNS KOMMUNE
Økonomiforvaltningen
Koncern IT

NOTAT

Til Borgerrepræsentationen

5. oktober 2018

Sagsnr.
2018-0262801

Dokumentnr.
2018-0262801-1

Sagsbehandler
Frederik Siegumfeldt

Svar på spørgsmål fra Jakob Næsager vedr. omfang af persondatabrud

På Økonomiudvalgets møde den 25. september 2018 har Jakob Næsager bestilt en oversigt over indberetninger af databrud pr. 1. oktober 2018 fra alle forvaltninger.

Et persondatabrud er normalt kendetegnet ved, at det fører eller kan føre til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger. Persondatabrud skal anmeldes til Datatilsynet medmindre, at det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder.

I Københavns Kommune håndteres persondatabrud som udgangspunkt af de enkelte forvaltninger, som også har ansvaret for, at bruddet først indberettes til Koncern IT og eventuelt efterfølgende anmeldes til Datatilsynet.

Koncern IT kan i den anledning oplyse, at der i Københavns Kommunes interne system (ServiceNow) for indberetninger af bl.a. potentielle persondatabrud er foretaget følgende antal indberetninger fra forvaltningerne siden persondataforordningen trådte i kraft den 25. maj 2018:

2018	Maj	Juni	Juli	Aug	Sept	Okt	Nov	Dec	I alt
BIF	0	1	1	4	5	0	0	0	**11**
BUF	0	3	1	4	7	0	0	0	**15**
KFF	0	0	0	3	2	0	0	0	**5**
SOF	0	5	5	5	7	2	0	0	**24**
SUF	0	0	0	2	0	0	0	0	**2**
TMF	0	0	0	2	4	0	0	0	**6**
ØKF	1	0	1	2	6	1	0	0	**11**
Berører flere forvaltninger	0	1	1	1	4	0	0	0	**7**
Samlet antal indberetninger i ServiceNow									**81**

Tabel 1: Anmeldelser i Københavns Kommunes interne system for indberetninger af bl.a. potentielle persondatabrud

Af de pågældende 81 indberetninger er der efterfølgende foretaget en vurdering af bruddets karakter. 51 er vurderet til faktisk at omhandle persondata, og heraf har 20 haft en karakter, som har påkrævet en anmeldelse til Datatilsynet, jf. tabel nedenfor.

Vejledende Sikkerhed

Borups Allé 177
2400 København NV

EAN nummer
5798009809308

Karakteren af de 81 indberetninger til Koncern IT	Evt. anmeldt til Datatilsynet (status pr. 3. oktober 2018)	
Persondatabrud	Anmeldt til Datatilsynet	20
	Ikke anmeldt til Datatilsynet	31
Ikke persondatabrud	Ikke anmeldt til Datatilsynet	30

Tabel 2: Anmeldelser foretaget af de enkelte forvaltninger til Datatilsynet

Indberetninger under kategorien *ikke-persondatabrud* er typisk karakteriseret ved, at det ved vurderingen af indberetningen har vist sig, at der slet ikke har været tale om brud på informationssikkerheden, eller at bruddet ikke omfattede personoplysninger.

Det bemærkes endvidere, at *ikke-anmeldte persondatabrud* typisk er karakteriseret ved, at bruddet ikke i sig selv har givet anledning til, at oplysninger rent faktisk er kommet til uvedkommendes kendskab, og at oplysninger alene har været potentielt tilgængelige for et afgrænset antal medarbejdere i kommunen. Det kan i tilknytning hertil oplyses, at kommunens medarbejdere er instrueret i ikke at tilgå oplysninger, som de ikke har et fagligt behov for anvende.

For så vidt angår de 20 *anmeldelser af persondatabrud* fordeler indberetningerne sig på de enkelte forvaltninger som anført nedenfor:

	Antal
BIF	3
BUF	7
KFF	2
SOF	4
SUF	0
TMF	1
ØKF	2
BIF/SOF	1
I alt	**20**

Tabel 3: Anmeldelser til Datatilsynet fordelt på forvaltninger

Indholdsmæssigt fordeler de 20 indberetninger sig på følgende 'sagstyper':

	Antal
Ukrypterede mails	3
Sager behandlet uden fuldmagt	2
Afgørelse sendt til forkerte modtagere	7
Fejl i fagsystemer	2
Fejl i autorisationer	1
Andet	5
I alt	**20**

Tabel 4: Fordeling af brud på forskellige 'sagstyper'

I tilknytning hertil bemærkes, at hovedparten af indberettede brud knytter sig til menneskelige fejl, men at enkelte brud kan henføres til tekniske/systemmæssige fejl. Koncern IT kan endvidere oplyse, at enkelte sager har omfattet videregivelse af fortrolige oplysninger, men at der ikke er forekommet tilfælde, hvor store mængder af personoplysninger er kommet til uvedkommendes kendskab uden for kommunen.

For en god ordens skyld skal Koncern IT i øvrigt bemærke, at der er betydelig forskel på omfanget af behandling af personoplysninger i de enkelte forvaltninger, og at et større antal indberetninger for en forvaltning ikke nødvendigvis er udtryk for forvaltningens generelle evne til at håndtere personoplysninger – tværtimod kan det være et udtryk for, at der i den pågældende forvaltning er en særlig opmærksomhed i forhold til, at uregelmæssigheder kan være persondatabrud og derfor skal indberettes.

Fælles uddannelsesindsats i alle forvaltninger
Økonomiudvalget er tidligere blevet orienteret om, at der i regi af det nu afsluttede forvaltningsfælles GDPR-program blev igangsat et e-læringsforløb for alle medarbejdere. Formålet med e-læringsforløbet har været at styrke og skabe et fælles niveau for beskyttelsen af personoplysninger i hele kommunen. Uddannelsen indeholder handlingsorienteret information til medarbejderne om kravene i den nye databeskyttelsesforordning, herunder definitionen af persondata, den registreredes rettigheder mv.

Fællesadministrativ forretningsgang for persondatabrud
Koncern IT kan oplyse, at der er vedtaget en 'Fællesadministrativ forretningsgang for persondatabrud'. Forretningsgangen vedlægges som bilag 1.

I hovedtræk fastsætter forretningsgangen,

- At forvaltningernes *DPO Business Partners* skal modtage og vurdere potentielle persondatabrud og oprette disse i ServiceNow, standse bruddet i det omfang, det er muligt, anmelde brud til Datatilsynet, underrette den registrerede og dokumentere sikkerhedshændelsernes forløb i ServiceNow fra start til slut.
- At *forvaltningerne* i øvrigt skal have it-kompetencer, juridiske kompetencer og kommunikative kompetencer til rådighed i tilfælde af persondatabrud.
- At *Koncern IT* er ansvarlig for systemunderstøttelsen og opsamlingen af sikkerhedshændelser i kommunen og skal bistå forvaltningerne med efterforskning og analyse efter behov.
- At *Databeskyttelsesrådgiveren* bl.a. skal orienteres ved anmeldelse til Datatilsynet.

KØBENHAVNS KOMMUNE

FÆLLES
ADMINISTRATIV
FORRETNINGSGANG

Persondatabrud

Ejerskab:	Koncern IT, Kontoret for Vejledende sikkerhed
Version:	1.0
Gældende fra:	25-05-2018
Sidst opdateret:	23-05-2018
Anvendelse:	Københavns Kommune
Journalnr.:	2017-0265775-12

Indholdsfortegnelse

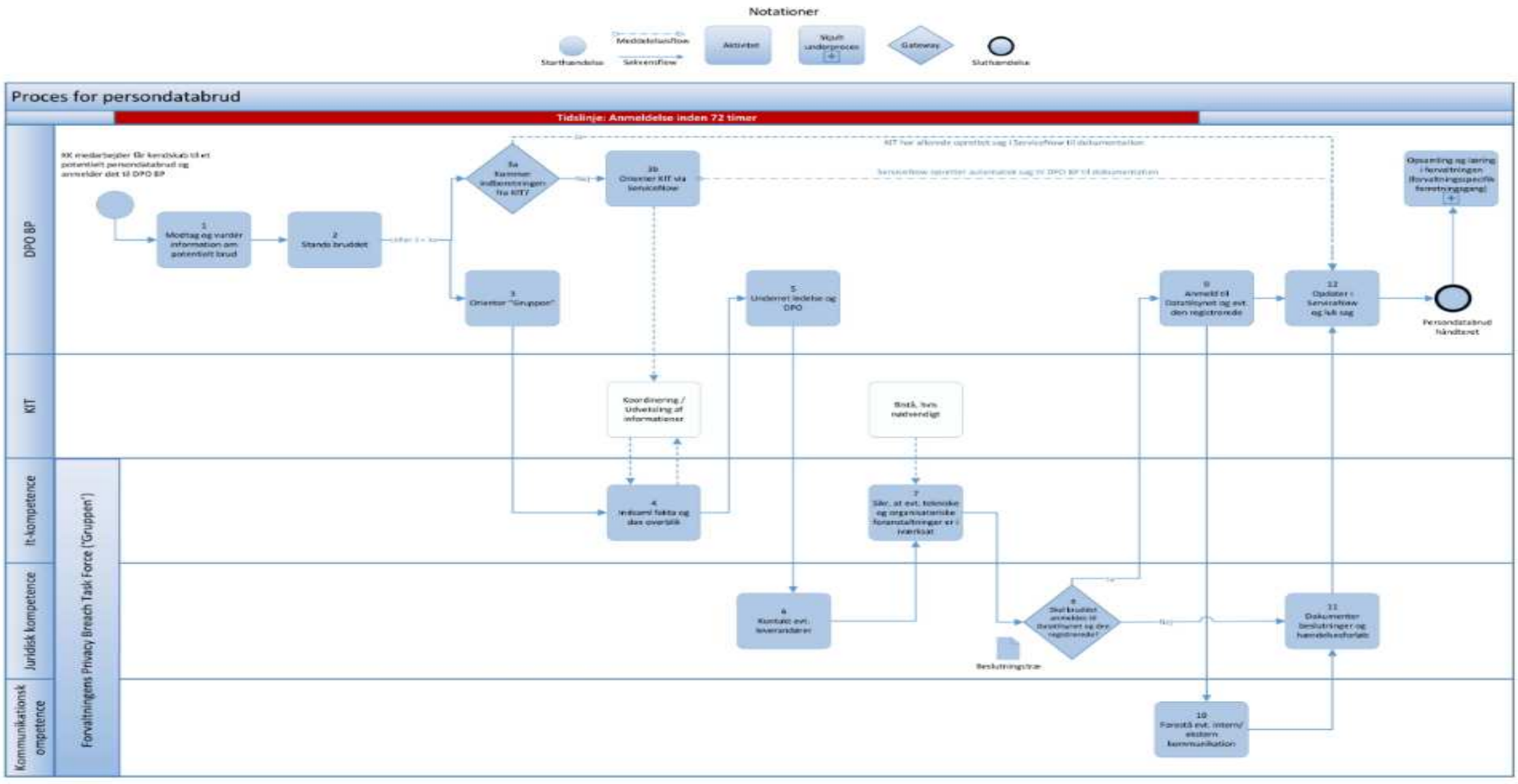
1.1 Persondatabrud

Omfang og afgrænsning	
HOVEDPROCES	**Databeskyttelse**
DELPROCES	Persondatabrud
HJEMMEL:	Informationssikkerhedsregulativ (vedtages juni 2018)
OMFANG OG AFGRÆNSNING:	Denne forretningsgang beskriver delprocessen Persondatabrud. Processen er afgrænset til at omfatte håndtering og anmeldelse af brud på persondatasikkerheden i alle juridiske enheder under Københavns Kommune.
PROCESINPUT:	En medarbejder i Københavns Kommune får kendskab til et potentielt persondatabrud.
PROCESOUTPUT:	Persondatabruddet er håndteret, anmeldt, dokumenteret, og sagen er lukket i ServiceNow.

Processen

Formålet med denne fælles administrative forretningsgang er at sikre lovmedholdeligheden i Københavns Kommune i forbindelse med persondatabrud. Processen er udarbejdet med afsæt i det arbejde, der er udført i *"Legal Compliance Projektet"*. Processen skal understøtte og sikre en effektiv varetagelse af de nødvendige opgaver, der opstår i forbindelse med et sikkerhedsbrud, som det er defineret i Databeskyttelsesforordningens artikel 4, stk. 1, nr. 12.
Triggeren i processen er når en medarbejder i Københavns Kommune får kendskab til et potentielt persondatabrud. Det er derfor værd at præcisere det ansvar medarbejderne i Københavns Kommune har i relation til indeværende proces; **alle medarbejdere i kommunen har pligt til at anmelde informationssikkerhedshændelser, herunder potentielle persondatabrud.**

Procestegning: Persondatabrud



Rollebeskrivelse: Persondatabrud		
Rolle/funktion	Beskrivelse	Ansvar/opgaver
DPO BP	DPO Business Partner (DPO BP) er forvaltningens kontaktpunkt til DPO-funktionen og skal understøtte varetagelsen af dennes opgaver - herunder rådgivning og tilsyn med forvaltningens efterlevelse af Databeskyttelsesforordningen. Der henvises til stillingsbeskrivelse for DPO BP.	DPO BP har ansvaret for følgende opgaver: - Sikre forvaltningsspecifik vejledning til medarbejdernes indmeldelse af persondatabrud til DPO BP - Modtage potentielle persondatabrud og oprette disse i ServiceNow - Straks standse bruddet i det omfang, det er muligt - Orientere 'gruppen' - Koordinere og udveksle relevante informationer med KIT - Anmeldelse af persondatabrud til Datatilsynet og eventuel underretning af den registrerede. - Dokumentere persondatabrudenes forløb i ServiceNow fra start til slut. - Der henvises til disposition for beredskabsplan for håndtering af persondatabrud i Københavns Kommune.
KIT	KIT er vidensorganisation og sparringspartner for forvaltningerne i forbindelse med potentielle persondatabrud.	KIT har ansvaret for følgende opgaver: - Opsamle og opbevare information om persondatabrud - Bistå forvaltningerne med efterforskning og analyse ved behov - Orientere ØU om sikkerhedsbrud en gang årligt - Afrapportere til DPO-funktionen
Privacy Breach Task Force/ 'Gruppen'	En pre-defineret gruppe af medarbejdere, der varetager de tekniske, juridiske og kommunikationsmæssige opgaver i forbindelse med persondatabrud. Gruppen består af medarbejdere i forvaltningen med relevante it-, juridiske og kommunikationskompetencer.	'Gruppen' har ansvaret for udførslen af de it-, juridiske- og kommunikationsmæssige opgaver i forbindelse med beredskabet ved persondatabrud. For Gruppens opgaver henvises der til disposition for beredskabsplan for håndtering af persondatabrud i Københavns Kommune.

Procesbeskrivelse: Persondatabrud				
NR.	AKTIVITET	UDFØRER	HANDLINGER I AKTIVITETEN	VEJLEDNING
Start	KK medarbejder får kendskab til et potentielt persondatabrud og anmelder det til DPO BP	KK medarbejder	KK medarbejder orienterer forvaltningens DPO BP om det potentielle sikkerhedsbrud via telefon, mail til en speciel postkasse eller gennem it-portalen.	Forvaltningsspecifikke vejledninger
1	Modtag og vurdér information om potentielt brud	DPO BP	DPO BP modtager indberetningen fra medarbejderen og vurderer, hvorvidt det kan betragtes som et sikkerhedsbrud.	Bilag 3: Vejledning til arbejdet med brud på persondatasikkerheden Bilag 4: Datatilsynets vejledning om håndtering af brud på persondatasikkerheden
2	Stands bruddet	DBO BP	DPO BP iværksætter straks alle relevante tiltag for at stoppe sikkerhedsbruddet og minimere skaden.	
3	Orienter "Gruppen"	DPO BP	Når en notifikation om et potentielt sikkerhedsbrud modtages, underrettes de øvrige medlemmer af Gruppen, og beredskabet iværksættes. Herefter tages der stilling til aktivitet 3a: Kommer indberetningen fra KIT? - Ja: KIT har allerede oprettet sag i ServiceNow til dokumentation. - Nej: Aktivitet nr. 3b: "*Orienter KIT via ServiceNow*." ServiceNow opretter automatisk sag til DPO BP og KIT til dokumentation.	

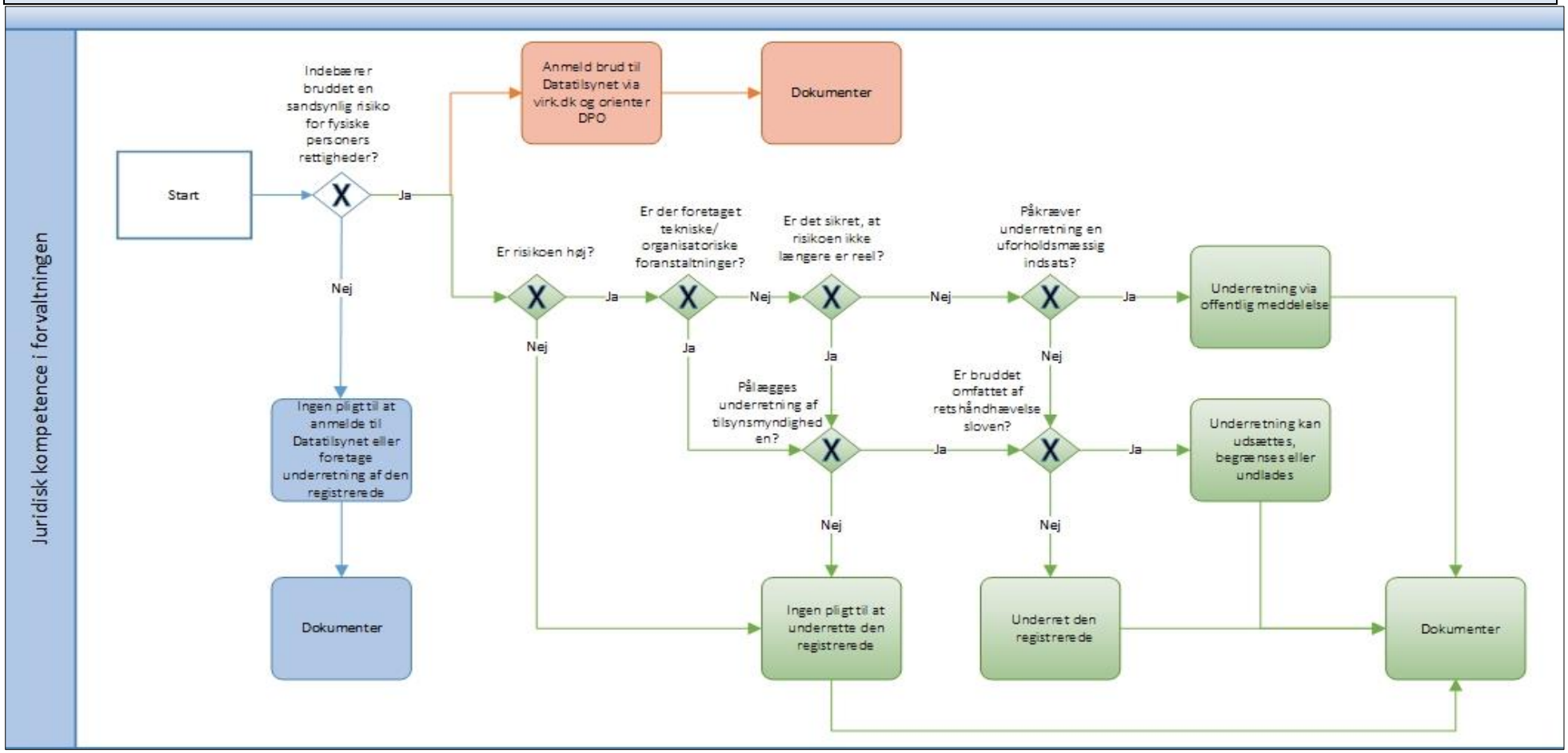
4	Indsaml fakta og dan overblik	Gruppen: It-kompetence	Gruppen søger hurtigst muligt at danne sig et overblik over sikkerhedsbruddet, navnlig omstændighederne omkring:
			- Type af hændelse (de tekniske omstændigheder bag hændelsen)
			- Omfanget af skaden, herunder:
			  ○ Hvilke kategorier af personoplysninger er berørt
			  ○ Hvilke foranstaltninger er allerede truffet for at håndtere og/eller begrænse skaden (kryptering eller lignende)
			  ○ Cirka antal berørte
			- Om eksterne leverandører er involveret.	

5	Underret ledelse og DPO	DPO BP	Ledelsen underrettes om situationen og orienteres løbende om udviklingen. KK's DPO underrettes om situationen. DPO'en anmodes om en tilkendegivelse af, i hvilket omfang DPO'en ønsker at holdes underrettet om situationens videre udvikling.	
6	Kontakt evt. leverandører	Gruppen: Juridisk kompetence	Underretning af den eller de involverede leverandører, hvis de ikke allerede er informeret. Leverandørerne anmodes om udarbejdelse af en detaljeret redegørelse over hændelsesforløbet, baggrunden for fejlen, konsekvenserne heraf, hvordan fejlen er rettet og hvordan det sikres, at det ikke kan ske igen. Leverandørens redegørelse af sikkerhedsbruddet bedes udarbejdet særligt med henblik på at oplyse de informationspunkter, som ikke allerede er indsamlet under aktivitet nr. 4 *"Indsaml fakta og dan overblik"*.	
7	Iværksæt evt. tekniske og organisatoriske foranstaltninger	Gruppen: It-kompetence	Alle relevante tiltag for at stoppe sikkerhedsbruddet og minimere skaden iværksættes straks. I tilfælde af anvendt it-system, træffes om nødvendigt beslutning om foreløbig suspension af det pågældende system.	
8	Skal bruddet anmeldes til Datatilsynet og den registrerede?	Gruppen: Juridisk kompetence	Der foretages en indledende vurdering af fejlens omfang og konsekvenser – evt. i samarbejde med leverandøren eller andre implicerede aktører. Vurderingen skal medføre en beslutning om, hvorvidt bruddet skal anmeldes til Datatilsynet og evt. registrerede? - Ja: → Aktivitet nr. 9: "*Anmeld til Datatilsynet og evt. registrerede"* - Nej: → Aktivitet nr. 11: "*Dokumenter beslutninger og hændelsesforløb"* Den juridiske vurdering udføres på baggrund af overblikket fra aktivitet nr. 4 og 6 ovenfor om de mulige konsekvenser for de registrerede, og hvorvidt underretninger kan undtages.	Bilag 1: Beslutningstræ - Anmeldelse til Datatilsynet og den registrerede?
9	Anmeld til Datatilsynet og evt. registrerede	DPO BP	Fremsendelse af underretninger til Datatilsynet samt evt. registrerede. Med "registrerede" forstås de personer (oftest borgere), hvis oplysninger er omfattet af sikkerhedsbruddet, og som dermed er berørte. Kopi af alle underretninger, som sendes til Datatilsynet og/eller de berørte registrerede, sendes samtidig til KK's DPO uanset DPO'ens tilkendegivelse beskrevet i aktivitet nr. 5 "*Underret ledelse"* ovenfor.	Bilag 5: Vejledning til anmeldelse til tilsynsmyndigheden Bilag 6: Skabelon til underretning af den registrerede Bilag 7: Standardvejledninger til Borgeren om afhjælpning

			Det er kun de borgere, som er direkte berørt af sikkerhedsbruddet, som – i denne forbindelse – skal underrettes i henhold til Databeskyttelsesforordningen. Ikke-berørte borgere vil evt. blive orienteret via pressen som følge af aktivitet nr. 10: *"Forestå evt. intern/ekstern kommunikation"*. Ved den evt. udarbejdelse af underretninger til de berørte registrerede, bør de juridiske kompetencer – i nødvendigt omfang og inden for rammerne af Databeskyttelsesforordningen – søge inputs fra kommunikationskompetencerne med henblik på at udforme underretningerne således, at antallet af efterfølgende henvendelser fra borgere i form af f.eks. (akt)indsigtsanmodninger minimeres. Det er fx relevant ved større brud samt ved brud, som grundet deres (type)indhold og omfang må forventes at medføre en vis bevågenhed. Vedlagte bilag 5 for udarbejdelse af anmeldelse til Datatilsynet og bilag 6 & 7 for underretning af berørte registrerede kan bruges.	af konsekvenserne for Sikkerhedsbruddet
10	Forestå evt. intern/ekstern kommunikation	Gruppen: Kommunikationskompetence	**Evt. øvrig intern og ekstern kommunikation** På baggrund af aktivitets nr. 9: *"Anmeld til Datatilsynet og evt. registrerede"* ovenfor udarbejdes en plan for den øvrige interne og eksterne kommunikation. Sørg for, at al intern og ekstern kommunikation udsendes samtidigt, hvis dette er påkrævet, og at budskaberne er ens. **Evt. pressestrategi** Varetage pressestrategi i samråd med ledelsen og evt. ekstern kommunikation/presserådgiver. **Evt. kommunikation til øvrige medarbejdere** Udarbejdelse af eventuelle meddelelser til relevante medarbejdere.	
11	Dokumenter beslutninger og hændelsesforløb	Gruppen: Juridisk kompetence	Der udarbejdes endelig dokumentation for sikkerhedsbruddet med henblik på opfyldelse af dokumentationskravet samt at iagttage foranstaltninger for at minimere risiko for gentagelser. Dokumentationen skal udarbejdes uagtet evt. beslutninger om undladelse af underretning til Datatilsynet samt evt. berørte registrerede. Dokumentationen journaliseres i ServiceNow.	

12	Opdater i ServiceNow og luk sag	DPO BP	Beslutninger og håndtering af brud dokumenteres i ServiceNow.	
Slut	Persondatabrud håndte-ret	DPO BP	Processen afsluttes og informationer om håndteringen af persondatabruddet lagres.	

BILAG 1: BESLUTNINGSTRÆ - ANMELDELSE TIL DATATILSYNET OG DEN REGISTRERede?



- Dokumentationen angives i de dertil indrettede felter i systemunderstøttelsen (ServiceNow).
  - For den blå dokumentationsboks anvendes feltet: [opdateres d. 25/5]
  - For den orange dokumentationsboks anvendes feltet: [opdateres d. 25/5]
  - For den grønne dokumentationsboks anvendes feltet: [opdateres d. 25/5]

BILAG 2: RISIKOVURDERING

RISIKOREFNR.	AKTIVITETREF.	RISIKOTYPE				BESKRIVELSE AF RISIKOEN	RISIKO-VURDERING			UDDYBENDE RISIKOVURDERING OG RATIONALE SÅFREMT DET BESLUTTES AT RISIKOEN IKKE SKAL AFDÆKKES/MITIGERES
		FINANSIEL	BESVIGELSE	OPERATIONEL	COMPLIANCE		SANDSYNLIGHED	KONSEKVENS	VURDERING AF IBOENDE RISIKO	
R.001	1.1.0 (start)			X	X	<u>Medarbejdere indberetter ikke et potentielt brud</u> Hændelsen indberettes ikke, fordi medarbejderen ikke har kendskab til hvilke informationer der kan karakteriseres som persondata *og/eller* hvornår der kan være tale om et brud.	3	2	Høj	**Sandsynlighed** Det vurderes meget sandsynligt da persondatalovgivningen er ny, kompleks og stiller store krav til opmærksomheden fra samtlige medarbejdere i KK. **Konsekvens** Vurderes væsentlig da KK ikke er compliant ift. persondataforordningen eller KK's egen it-sikkerhedspolitik. Det vurderes, at de brud, der ***ikke*** vil blive indberettet, vil have en begrænset påvirkning ift. image og lovgivning. **Konklusion** Den enkelte forvaltning forestår egne awarenes- og undervisningskampagner for at uddanne medarbejderne for at mitigere risikoen.

R.002	1.1.1			X		<u>DPO BP'en modtager ikke indberetningen</u> Som følge af manglende personlig tilgængelighed, forkerte kontakt oplysninger, nedbrudte systemer, for lang ventetid i serviceindgangen mv. risikerer DPO BP'en ikke at modtage en medarbejders indberetning.	1	2	Lav	**Sandsynlighed** Vurderes usandsynligt da der primært vil være tale om personlige fejl, idét it-systemer og serviceprocesser vil understøtte størstedelen af indberetningerne. **Konsekvens** Vurderes væsentlig da, der her ikke vil blive taget hånd om potentielle brud med imagemæssige og lovgivningsmæssige konsekvenser. **Konklusion** Som følge af den lave sandsynlighed vurderes det ikke nødvendigt med forvaltningsspecifikke kontroller i relation til forretningsgangen. Kontrol af systemunderstøttelsen og serviceindgangens virke er placeret andetsteds i KK.
	6			X	X	<u>Manglende juridisk hjemmel til at få den nødvendige information</u> Det kan i visse tilfælde være vanskeligt at få de informationer, KK vurderer der er behov for. Enten fordi leverandøren ikke er i stand til at oplyse dem eller databehandler aftalen ikke giver hjemmel hertil.	1	3	Lav	**Sandsynlighed** Sandsynligheden vurderes lav som følge af KK's politik om brug af KK's standard databehandleraftale. **Konsekvens** Ved manglende juridisk hjemmel kan KK ikke være sikre på at modtage alle oplysninger, der skal anvendes for at stoppe bruddet og anmelde til datatilsynet. Konsekvenserne er store både af hensyn til evt. systemfunktionalitet, image og lovgivning. **Konklusion** I KK er aftaler med leverandører altid indgået skriftligt, hvorfor de interne KK processer tilskynder, at der forelægger en databehandleraftale. Kvalitetssikringen, kontrol af databehandleraftalen samt leverandørsamarbejdet i øvrigt placeres i andre KK processer. Derfor vurderes det ikke nødvendigt med ekstra forvaltningsspecifikke kontroller ift. den beskrevne risiko.

	8					Bruddet vurderes fejlagtigt Det indmeldte brud vurderes ikke at udgøre en *"sandsynlig risiko for fysiske personers rettigheder"* og anmeldes derfor ikke til datatilsynet.	2	3	Høj	**Sandsynlighed** Sandsynligheden for fejlvurderinger vurderes rimelig sandsynlig, som følge af de nye opstillede retningslinjer og manglende præcedens. **Konsekvens** Fejlvurderingerne kan medføre store konsekvenser fx i forbindelse med statslige tilsyn. Særligt vil der i forbindelse med ikrafttrædelsen i 2018 være en stor mediebevågenhed, der kan føre til store image-mæssige konsekvenser. **Konklusion** Der skal udarbejdes retningslinjer, der kan anvendes i forbindelse med vurderingerne. Retningslinjerne, risikovurderingen og indførelsen af evt. kontroller vurderes når KK får mere viden om de brud, der ind-meldes.
	11				X	Manglende journalisering af beslutninger, nye for-anstaltninger mv. Opklaringen og tekniske informationer kan være spredt imellem DPO BP, medlemmer af gruppen og andre aktører. Derfor kan manglende journalise-ring fra en eller flere individer medføre ukorrekt dokumentation af bruddet.	2	3	Mel-lem	**Sandsynlighed** Sandsynligheden for manglende journalisering vurderes rimelig, sær-ligt i de situationer, hvor aktiviteter i forbindelse med bruddet vareta-ges af medarbejdere, der ikke har adgang til systemunderstøttelsen (ServiceNow). **Konsekvens** Manglende dokumentation kan medføre store konsekvenser af både imagemæssig- og lovgivningsmæssig karakter i forbindelse med akt-indsigter, statslige tilsyn mv. **Konklusion** Den enkelte forvaltning forestår egne kontroller, arbejdsgange og ud-dannelse for at sikre den relevante dokumentation.

Bilag 3: Vejledning til arbejdet med brud på persondatasikkerheden

"Brud på persondatasikkerheden"

Et brud på persondatasikkerheden ("Sikkerhedsbrud") er i databeskyttelsesforordningens artikel 4, stk. 1, nr. 12, defineret som:

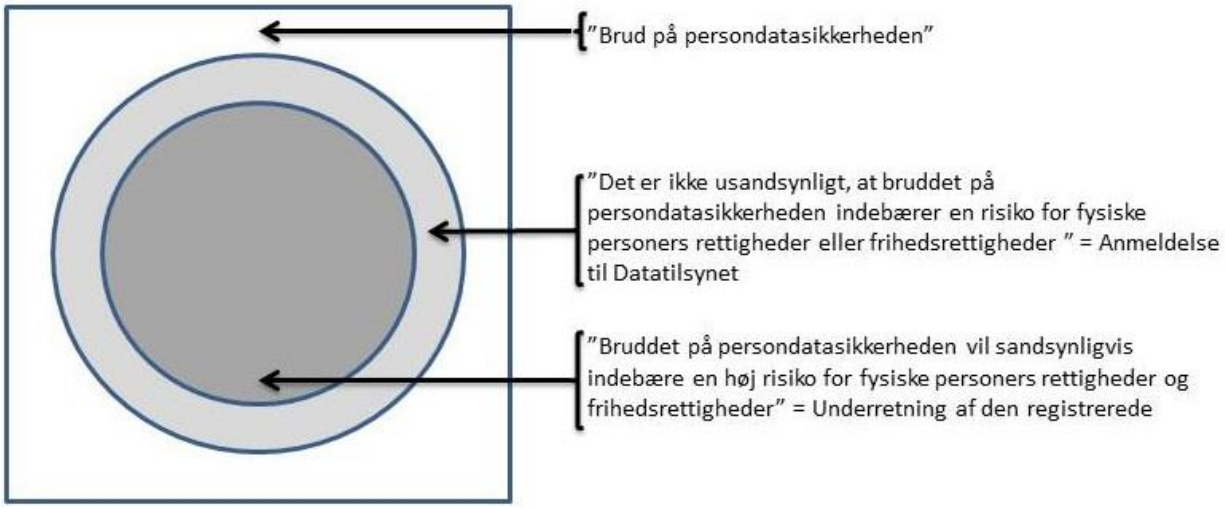
"Et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet."

Definitionen af Sikkerhedsbrud sigter dermed mod at rumme alle tænkelige tilfælde, hvor personoplysninger behandles på en utilsigtet måde.

Det følger herefter af databeskyttelsesforordningens artikel 33, at der skal foretages anmeldelse til Datatilsynet, hvis Sikkerhedsbruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Det betyder, at delmængden af ovenstående definition af Sikkerhedsbrud, "som indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder", udløser en pligt til at foretage anmeldelse til Datatilsynet.

Hertil følger det endvidere af databeskyttelsesforordningens artikel 34, at der skal foretages underretning til den registrerede (herefter "Borger"), hvis Sikkerhedsbruddet sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder. Det betyder, at en yderligere delmængde af ovenstående også medfører en pligt til underretning til Borgere, "hvis sikkerhedsbruddet sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder".

Sammenhængen mellem de tre delmængder kan – lidt forsimplet – illustreres således:



Hvornår skal der foretages anmeldelse til Datatilsynet

Som nævnt ovenfor, skal der foretages anmeldelse til Datatilsynet, hvis det ikke er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

Det vil i praksis betyde, at udgangspunktet er, at alle Sikkerhedsbrud medfører en pligt til anmeldelse til Datatilsynet.

En risiko for fysiske personers rettigheder og frihedsrettigheder omfatter bl.a. diskrimination, identitetstyveri eller -svindel, økonomisk tab, skade på omdømme, tab af fortrolighed af data underlagt tavshedspligt eller enhver anden væsentlig økonomisk eller social ulempe for Borgeren. Det kan fx være i følgende situationer:

- Offentliggørelse af beskyttet adresse: Kommunen offentliggør et brev på kommunens hjemmeside, hvor en borgers beskyttede adresse fremgår. Sådan en offentliggørelse medfører en pligt til anmeldelse til Datatilsynet og til at foretage underretning til Borgeren.

- Offentliggørelse af login og password: Kommunen offentliggør en række Borgeres login og password til en kommunal hjemmeside. Hjemmesiden indeholder kun få og ikke følsomme oplysninger. Da mange Borgere bruger de samme login- og passwordoplysninger til forskellige hjemmesider og tjenester, kan oplysningerne derfor give uvedkommende – indirekte – adgang til andre hjemmesider, som indeholder de berørte Borgeres følsomme oplysninger. Sådan en offentliggørelse vil derfor medføre pligt til anmeldelse til Datatilsynet og til at foretage underretning til Borgerne.

Hvornår anmeldelse til Datatilsynet ikke er nødvendig.

Selvom udgangspunktet er, at alle Sikkerhedsbrud medfører en pligt til anmeldelse til Datatilsynet, er der situationer, hvor det er usandsynligt, at Sikkerhedsbruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Det kan fx være i følgende situationer:

- Tabt lagringsmedie: Hvis det konstateres, at et lagringsmedie (fx USB-nøgle eller harddisk) indeholdende personoplysninger er mistet, men at mediet er krypteret så stærkt, at det er usandsynligt, at uvedkommende kan bryde krypteringen.

- Utilsigtet offentliggørelse på hjemmeside: Hvis det konstateres, at der ved en fejl er uploadet personoplysninger på en kommunal ejet hjemmeside, men at det ved gennemgang af loggen kan konkluderes, at den pågældende hjemmeside ikke har haft besøgende (fx hvis der er tale om en specialiseret underside), og at det samtidig kan konkluderes, at hjemmesiden ikke er blevet "crawlet" af fx Googles søgemaskine.

- Strømnedbrud: En forvaltning i kommunen rammes af et strømnedbrud, der varer i ca. 10 minutter, hvor det ikke er muligt at tilgå forvaltningens it-systemer, herunder elektroniske journaler. Ingen oplysninger er mistet, og arbejdet kan herefter fortsætte.

- Vildfaren krypteret e-mail: En sagsbehandler sender via digital post en besvarelse af en aktindsigtsanmodning fra en sag om sygedagpenge til en forkert borger. Dog er besvarelsen af aktindsigtsanmodningen pakket i en krypteret fil, hvortil sagsbehandleren havde planlagt at eftersende kodeord, hvorfor modtageren ikke kan åbne den krypterede fil.

- Nabofesten: En kommune vil sende et brev vedrørende nabovarsel om en stor fest i nabolaget. Ved en fejl sender kommunen via digital post brevet til en forkert borger. Brevet indeholder den oprindelige borgers navn og adresse og intet andet. Borgeren, der modtager brevet, gør straks kommunen opmærksom på fejlen. Kommunen aftaler skriftligt med borgeren, der har modtaget brevet, at vedkommende sletter det.

Hvor skal der foretages underretning til Borgeren

Forskellen fra, hvornår det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder – som medfører en pligt til anmeldelse til Datatilsynet – til hvor Sikkerhedsbruddet sandsynligvis vil indebære en høj risiko for

fysiske personers rettigheder og frihedsrettigheder – som medfører en pligt til underretning til Borgeren – er ikke stor.

I mange tilfælde vil en pligt til anmeldelse til Datatilsynet ligeledes medføre pligt til også at foretage underretning til Borgeren. Undtaget herfra synes kun at være de tilfælde, hvor man ikke kan afvise, at Sikkerhedsbruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, men hvor man samtidig har en begrundet forventning om, at risikoen ikke realiseres.

Det praktiske udgangspunkt er derfor, at hvis der foretages anmeldelse til Datatilsynet, skal der ligeledes foretages underretning til Borgeren.

Hvis der foretages anmeldelse til Datatilsynet, kan underretning til Borgeren dog undtages, hvis:

- Hvis Sikkerhedsbruddet ikke medfører en høj risiko for fysiske personers rettigheder eller frihedsrettigheder – fx hvis det kan konstateres, at der er blevet fremsendt en e-mail til få og identificerede borgere, som ikke kan tænkes at kunne – og ville – udnytte oplysningerne.

- Hvis der er gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, og disse foranstaltninger er blevet anvendt til beskyttelsen af personoplysninger, som er berørt af Sikkerhedsbruddet – se fx eksemplet med det tabte lagringsmedie med høj kryptering ovenfor.

- Hvis der er truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for Borgernes rettigheder og frihedsrettigheder ikke længere er reel – fx hvis der konstateres et "hul" i sikkerheden på en hjemmeside, men at hullet hurtigt lukkes, og det samtidig kan dokumenteres, at hullet ikke har været udnyttet.

- Hvis individuel underretning vil kræve en uforholdsmæssig indsats – fx hvis ét af kommunens byggesagsarkiver oversvømmes, og dokumenter på byggesager, som har været afsluttet i over 25 år, mistes. I så fald vil en meddelelse på kommunens hjemmeside være tilstrækkelig.

Operationel spørgeguide

På baggrund af ovenstående pointer foreslås herefter en spørgeguide til brug for afklaring af, om der skal foretages anmeldelse til Datatilsynet samt eventuel underretning til Borgeren.

Spørgsmål til brug for afklaring af, om der skal der foretages anmeldelse til Datatilsynet

Ved ethvert Sikkerhedsbrud, skal der som udgangspunkt foretages anmeldelse til Datatilsynet. Anmeldelsen kan dog undtages, hvis det kan afvises, at Sikkerhedsbruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Det kan navnlig afvises, hvis følgende forhold alle kan dokumenteres:

- Starttidspunktet for Sikkerhedsbruddet.

- Sluttidspunktet for Sikkerhedsbruddet.

- Omfanget af Sikkerhedsbruddet.

- Årsagen til Sikkerhedsbruddet.

- Personoplysninger er ikke kommet til uvedkommendes kendskab – og selvom personoplysninger er kommet til uvedkommendes kendskab, kan det påvises:

- Hvem de uvedkommende modtagere af oplysninger er,
- at de uvedkommende modtagere af personoplysningerne mangler enten viljen eller muligheden for at udnytte oplysningerne, og
- at de uvedkommende modtagere af oplysninger ikke længere er i besiddelse af oplysningerne.

Spørgsmål til brug for afklaring af, om der skal der foretages underretning til Borgeren

Hvis det er besluttet, at der skal foretages anmeldelse til Datatilsynet, er udgangspunktet, at der ligeledes skal foretages underretning til Borgeren.

Underretning kan dog undtages, hvis det kan afvises, at Sikkerhedsbruddet indebærer en høj risiko for fysiske personers rettigheder eller frihedsrettigheder. Det kan navnlig afvises, hvis ét af følgende forhold kan dokumenteres:

- Risikoen for Sikkerhedsbruddet er ikke høj. Risikoen vurderes ud fra en samlet vurdering af:
  - Hvilken type Sikkerhedsbrud er der tale om? Er personoplysningerne offentliggjort på internettet (høj risiko), eller har man bare glemt, hvor præcist i et opbevaringsarkiv, man har gemt oplysningerne (lav risiko)?
  - Hvad er konteksten, følsomheden og mængden af oplysningerne?
  - Hvor nemt er det for uvedkommende at identificere de personer, som oplysningerne vedrører?
  - Hvor stor er risikoen for, at Borgeren oplever et tab af rettigheder og frihedsrettigheder som følge af Sikkerhedsbruddet?
  - Er der tale om en særlig udsat type af Borger – fx børn eller socialt udsatte?
  - Hvor mange Borgere vedrører oplysningerne?
  - Hvilken forvaltning/enhed er ansvarlig for Sikkerhedsbruddet?
- Der er gennemført passende tekniske og organisatoriske foranstaltninger, således at det kan påvises, at:
  - Eventuelle uvedkommende modtagere af oplysningerne er forhindret i at tilgå og benytte oplysningerne – fx hvis oplysningerne er krypterede.
- Den høje risiko for Borgernes tab af rettigheder og frihedsrettigheder er ikke længere reel, og det kan påvises, at:
  - Oplysningerne ikke har været tilgået og benyttet af uvedkommende, mens risikoen stadig var reel.
- Hvis underretning kræver en uforholdsmæssig indsats – fx i tilfælde af, at indsatserne for at foretage individuelle underretninger ikke står i mål de – negligerbare – konsekvenser, som de registrerede potentielt kan opleve.

Bilag 4: Vejledning om håndtering af brud på persondatasikkerheden

Vejledningen findes på følgende URL: https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_sikkerhedsbrud.pdf

Nedenfor er forordet for versionen fra februar 2018 gengivet:

Når databeskyttelsesforordningen finder anvendelse i Danmark og resten af EU fra den 25. maj 2018, vil der – som noget nyt – gælde en generel forpligtelse for alle dataansvarlige til som udgangspunkt at anmelde brud på persondatasikkerheden til Datatilsynet. Anmeldelsen skal ske uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet. Samtidig fastsættes der en forpligtelse, som allerede i dag tolkes ud af persondatalovens grundregel om god databehandlingsskik og Datatilsynets praksis, til som udgangspunkt at underrette de registrerede i tilfælde af brud på persondatasikkerheden.

Begge forpligtelser er udtryk for databeskyttelsesforordningens fokus på ansvarlighed, når det kommer til at overholde databeskyttelsesreglerne. Reglerne har til formål at tilvejebringe gennemsigtighed og især at sikre, at dataansvarlige reagerer, når der opstår et brud på persondatasikkerheden.

Det skal i tilknytning hertil nævnes, at hvis reglerne om anmeldelse af brud på persondatasikkerheden og underretning af de registrerede ikke overholdes, har Datatilsynet en række korrigerende beføjelser. Tilsynet kan f.eks. udtale kritik eller udstede et påbud. Afhængigt af omstændighederne i hver enkelt sag kan der imidlertid også blive tale om at sanktionere den manglende efterlevelse af reglerne med bøde – enten i kombination med eller i stedet for en af Datatilsynets korrigerende beføjelser.

Denne vejledning er målrettet de dataansvarlige private virksomheder, offentlige myndigheder, fysiske personer, institutioner og andre organer, som i tilfælde af et sikkerhedsbrud, der involverer personoplysninger, skal vurdere, om der i den forbindelse er pligt til at anmelde bruddet til Datatilsynet og pligt til at underrette de registrerede. Herudover indeholder vejledningen en gennemgang af de indholdsmæssige krav til en anmeldelse/underretning om et sikkerhedsbrud, ligesom der i vejledningen vil blive redegjort for forordningens krav til tidspunktet for, hvornår der skal ske anmeldelse/underretning, og måden hvorpå anmeldelsen skal indgives til Datatil-synet.

Ønskes en nærmere gennemgang af reglerne, henvises der bl.a. til selve lovteksten i databeskyttelsesforordningens kapitel IV, afdeling 2 (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) samt afsnittene 5.11. og 5.12. i betænkning nr. 1565/2017 om databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning.

Artikel 29-gruppen (fremover Det Europæiske Databeskyttelsesråd) har også offentliggjort en vejledning om underretning af brud på persondatasikkerheden ("Guidelines on personal data breach notification under Regulation 2016/679") (WP 250 rev 01). Vejledningen kan findes på www.datatilsynet.dk.

Det bemærkes, at vejledningen vil blive opdateret, når forslaget til den nye databeskyttelseslov er vedtaget.

Bilag 5: Vejledning til anmeldelse til tilsynsmyndigheden ved brud på persondatasikkerheden

I henhold til Databeskyttelsesforordningens artikel 33 anmeldelses nedenstående til Datatilsynet:

- En beskrivelse af 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
- Navn og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
- En beskrivelse af de sandsynlige konsekvenser af bruddet på persondatasikkerheden
- En beskrivelse af de foranstaltninger, som Københavns Kommune har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

Anmeldelse sker gennem virk.dk på den netop offentliggjorte portal:

https://indberet.virk.dk/myndigheder/stat/ERST/Indberetning_af_brud_paa_sikkerhed

Koncern IT udarbejder og udsender en supplerende vejledning til anmeldelsen.

Bilag 6: Skabelon til underretning til den registrerede ved brud på persondatasikkerheden

I henhold til Databeskyttelsesforordningens artikel 34 anmeldelses nedenstående til dig som registreret:

En beskrivelse af karakteren af bruddet på persondatasikkerheden i et klart og forståeligt sprog

[Indsæt en beskrivelse af karakteren af bruddet på persondatasikkerheden i et klart og forståeligt sprog:]

Navn og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes

[Indsæt navn og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes:]

En beskrivelse af de sandsynlige konsekvenser af bruddet på persondatasikkerheden

[Indsæt en beskrivelse af de sandsynlige konsekvenser af bruddet på persondatasikkerheden:]

En beskrivelse af de foranstaltninger, som Københavns Kommune har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

[Indsæt en beskrivelse af de foranstaltninger, som Københavns Kommune har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger:]

Bilag 7: Standardvejledninger til Borgeren om afhjælpning af konsekvenserne for Sikkerhedsbruddet

Standardvejledninger til Borgeren om afhjælpning af konsekvenserne for Sikkerhedsbruddet

I forbindelse med underretning til Borgerne, skal kommunen samtidig orientere om, hvordan Sikkerhedsbruddets potentielle risici kan minimeres.

En sådan underretning skal altid være tilpasset, men det kan alligevel forventes, at der vil opstå typetilfælde, hvortil der kan forberedes standardtekster. Sådanne tekster kan fx være:

NemID:

"Oplysninger om dit NemID er kommet til uvedkommendes kendskab, og du bør straks spærre dit nøglekort. Du spærrer dit nøglekort ved at logge på med dit NemID og adgangskode. Der sendes ikke automatisk et nyt nøglekort. For at bestille et nyt nøglekort online skal du legitimere dig med dit danske pas eller kørekort."

CPR.nr:

"Oplysninger om dit CPR.nr. er kommet til uvedkommendes kendskab, og du bør straks kontakte den sælger, virksomhed eller offentlige myndighed, som du har mistanke til, kan misbruge dit CPR.nr. Her skal du oplyse, at din identitet er blevet misbrugt, og at du derfor ikke anser dig for bundet af aftalen eller forholdet. Du kan i særlige tilfælde få et nyt personnummer, såfremt det er blevet misbrugt".