Datatilsynet
Att. Kenni Elm Olsen
Carl Jacobsens Vej 35
2500, Valby

Sendt pr. e-mail til dt@datatilsynet.dk

21. december 2020

JOURNALNUMMER 2020-431-0116 - DANSKE BANK A/S

Datatilsynet har ved brev af 3. november 2020 (journalnummer 2020-431-0116) anmodet Danske Bank A/S ("Danske Bank") om at besvare seks spørgsmål vedrørende opbevaring og sletning af personoplysninger.

Danske Bank skal hermed svare på spørgsmålene fra tilsynet.

Vi har for at lette læsningen af dette brev indsat en parentes i hvert afsnit med det tilsvarende nummer på spørgsmålet i brevet fra tilsynet.

Spørgsmålene er blevet besvaret i kronologisk rækkefølge for at give tilsynet et bedre overblik over baggrunden og tidslinjen for Danske Bank's arbejde med opbevaring og sletning. Ved at svare i kronologisk rækkefølge undgås samtidig for mange gentagelser. Spørgsmålene besvares således ikke i nummerorden.

Svarene på tilsynets spørgsmål er uddybet i **Bilag 1-6**, der indeholder beskrivelser og illustrationer, som viser Danske Bank's tilgang til og implementering af opbevaring og sletning i banken. Bilagene vedrører tidsperioden fra 2016 til 1. november 2020.

INDHOLD

1 SPØRGSMÅL (1): HVORNÅR OG HVORDAN DANSKE BANK A/S KONSTATEREDE PROBLEMET MED MANGLENDE SLETNING AF PERSONOPLYSNINGER

1.1 Vores forståelse af spørgsmålet

Danske Bank har ikke haft nogen specifikke "hændelser", som har ført til en undersøgelse med det resultat, at Danske Bank specifikt blev opmærksom på udfordringerne med opbevaring og sletning af personoplysninger.

Det er mere korrekt at se Danske Bank's arbejde med opbevaring og sletning af oplysninger som en løbende opgave. Bankens GDPR Steering Committee (på dansk, "GDPR Styregruppen") beskæftigede sig allerede i oktober 2016 med opbevaring og sletning. Dette arbejde er fortsat frem til i dag og fortsætter, indtil Danske Bank lever op til sine forpligtelser vedrørende opbevaring og sletning.

I det følgende beskriver vi Danske Bank's arbejde i relation til implementering af GDPR.

1.2 Beskrivelse af Danske Bank's implementering af GDPR

Der blev opnået politisk enighed om GDPR i december 2015, og Danske Bank påbegyndte straks herefter arbejdet med at identificere og foretage de nødvendige ændringer som følge heraf. Vi gennemgår i det følgende de største begivenheder i GDPR Programmet i kronologisk rækkefølge. Endvidere giver vi - i svaret på spørgsmål 5 - flere detaljer omkring IT-setuppet og arbejdet med opbevaring og sletning ("Retention and Deletion work stream").

Januar - Maj 2016

Der blev i januar 2016 etableret et projekt i Koncern IT, som indeholdt en række arbejdsspor, med det formål at påbegynde og forankre bankens arbejde med implementering af GDPR.

Da GDPR formelt blev vedtaget af EU-Parlamentet i april 2016, var Danske Bank allerede opmærksom på bankens udfordringer i relation til scope, omfang og finansiering af projektet.

Juni - September 2016

GDPR Programmet blev sat i gang straks efter, at GDPR var blevet vedtaget.

Det blev hurtigt klart for banken, at det var nødvendigt med en overordnet holistisk tilgang til GDPR, idet kravene i GDPR var overlappende, og idet løsningerne var indbyrdes afhængige af hinanden.

GDPR Programmet besluttede samtidig at samle og udvide scopet for de oprindelige arbejdsspor. Det blev prioriteret at foretage en grundig analyse af kravene i GDPR, således at den valgte tilgang kunne dække alle krav og hele Danske Bank koncernen - alle enheder, lande og markedsområder.

Oktober - December 2016

Der blev etableret en governance model for GDPR Programmet.

a) Modellen forankrede det overordnede ansvar for programmet hos den ansvarlige for Personal Banking og koncernens COO.

b) En styregruppe (herefter: "GDPR SteerCo") blev etableret med henblik på at træffe alle endelige beslutninger i GDPR Programmet.

Arbejdet i GDPR Programmet tog form i løbet af 2016. GDPR Programmet blev inddelt i to hovedspor, som blev udført parallelt:

a) Dette hovedspor havde til formål at skabe et overblik, dvs. en kortlægning, over alle forretningsprocesser og interne processer på tværs af Danske Bank koncernen, hvor personoplysninger blev behandlet. Formålet var at skabe et overblik over bankens behandling af personoplysninger samt identificere potentielle områder, hvor banken ikke levede op til reglerne.

b) Dette hovedspor havde til formål at identificere kravene i GDPR, således at der kunne oprettes de nødvendige arbejdsspor, for at kunne vurdere de iboende risici.

Programmet iværksatte en grundig analyse med henblik på at finde en løsningsmodel, som ville kunne tilvejebringe tilstrækkelig dokumentation og et fundament for, at banken i videst muligt omfang kunne efterleve reglerne i GDPR den 25. maj 2018.

Som følge af et meget stort antal IT-systemer - samt en høj grad af kompleksitet og indbyrdes forbindelse mellem systemerne - var det ikke muligt at implementere opbevarings- og slettefunktionaliteter i alle systemer på samme tid. Banken valgte derfor at håndtere kravene til opbevaring og sletning med en faseopdelt tilgang, som desværre ikke kunne færdiggøres inden den 25. maj 2018. Den første fase vedrørte centrale systemer.

Det blev undersøgt, om der var eksterne leverandører, der kunne hjælpe med at løfte opgaven. Mange af de undersøgte løsninger gav udtryk for at kunne afhjælpe udfordringerne ved GDPR. Løsningerne endte dog med at blive forkastet, da størstedelen af løsningerne havde en tilgang, hvor man så på udfordringerne nedefra og op. Dette indebar et fokus på IT-systemer, hvor data udelukkende kunne identificeres, hvis de var i IT-systemer. Det var imidlertid klart for Programmet, at scopet for GDPR var meget bredere end det, og at efterlevelse af GDPR også skulle sikres i forhold til oplysninger, der lå uden for IT-systemer.

På baggrund af ovennævnte blev det klart for Programmet, at man var nødt til at anlægge en oppefra og ned tilgang, hvor der blev fokuseret på forretningsprocesser.

Januar - April 2017

Danske Bank iværksatte en kortlægning af bankens forretningsprocesser for at identificere, hvor personoplysninger blev behandlet.

GDPR SteerCo godkendte brugen af en løsning fra en ekstern leverandør i forbindelse med kortlægningen i Danske Bank koncernen.

Kortlægning af processer

En kortlægning af forretningsprocesser var nødvendig for at skabe et indledende overblik. Forretningsområderne i Danske Bank koncernen blev derfor bedt om at beskrive deres forskellige behandlingsaktiviteter og om at foretage en vurdering af niveauet for efterlevelse af de, dengang, kommende krav i GDPR.

En oppefra og ned tilgang, hvor de overordnede processer blev kortlagt, blev valgt som en effektiv og håndterbar metode, sammenlignet med en nedefra og op tilgang med fokus på IT-systemer. En oppefra og ned tilgang dokumenterer forretningsprocesser i alle forretningsenheder, herunder også hvilke personoplysninger og systemer, der blev anvendt i en given forretningsproces. Den giver et logisk overblik over de kortlagte processer, men viser ikke de fysiske data flows.

En oppefra og ned tilgang blev anset for den rette metode sammenlignet med en nedefra og op tilgang henset til kompleksiteten i Danske Bank og den begrænsede tid, der var til rådighed.

Opgaven i forbindelse med kortlægningen var således at få klarlagt, hvor personoplysninger blev behandlet, og på grundlag heraf at identificere områder med overholdelse såvel som potentiel manglende overholdelse af GDPR.

Inden kortlægningen blev sat i gang i hele koncernen, blev det besluttet at gennemføre et pilotprojekt i området 'Personal Banking'. Området blev udvalgt, fordi stort set alle områdets forretningsprocesser involverer behandling af personoplysninger. Hvis tilgangen fungerede på området for Personal Banking, ville en kortlægning for hele Danske Bank koncernen være næste skridt.

Pilotprojektet inden for 'Personal Banking' var en succes og udgjorde dermed et solidt og dokumenteret grundlag for at igangsætte løsnings-projekter, som nærmere beskrevet nedenfor, i perioden maj 2017 til maj 2018.

Den overordnede indsats vedrørende kortlægningen af forretningsprocesser blev herefter opdelt i to hovedområder:

a) Forretningsenheder: Den primære behandling af forretnings-data, på alle markedsområder, af strukturerede data. GDPR Programmet vurderede, at dette ville dække ~80% af al behandling af personoplysninger.

b) Andre behandlingsaktiviteter: Dette dækkede bl.a. ad hoc-rapportering, testmiljøer, analysemiljøer, selvstændige systemer, interne ikke-kundevendte behandlingsaktiviteter, ustrukturerede persondata på lokale drev, delte drev, SharePoint-sider, mv. Disse behandlingsaktiviteter blev af GDPR Programmet vurderet til at udgøre ~20% af al behandling af personoplysninger.

Tilgangen til kortlægningen i koncernen er nærmere beskrevet i **Bilag 1**.

Opbevaring og sletning af personoplysninger
I forbindelse med, at Danske Bank arbejdede med de dele af GDPR Programmet, der vedrører IT-systemer, blev Danske Bank opmærksom på udfordringerne i forhold til opbevaring og sletning af personoplysninger.

Der blev derfor igangsat et arbejde med at håndtere disse udfordringer som en del af Programmet.

Maj 2017 - Maj 2018
GDPR Programmet nedsatte en arbejdsgruppe, som havde til opgave at kortlægge alle bankens processer. Arbejdsgruppen bestod af omkring 20 medarbejdere, der i forskellige teams gennemførte workshops med alle forretningsenheder i alle lande. Arbejdsgruppen fik kortlagt omkring 3.500 forretningsprocesser, og der blev samlet set brugt mere end 15.000 arbejdstimer på denne øvelse.

Der blev også igangsat et arbejde med henblik på at klarlægge, hvilke kompetencer en virksomhed skal kunne vise, at den besidder, baseret på kravene i GDPR.

På grundlag af dette arbejde fastlagde Danske Bank syv overordnede tiltag i form af arbejdsspor, jf. **Bilag 2**:

(i) Kundevendte dokumenter

(ii) Kundeindsigt og -support

(iii) Oprydning i personoplysninger (opbevaring og sletning)

(iv) Lokale IT-projekter (opbevaring og sletning)

(v) Organisatorisk implementering

(vi) Databehandleraftaler

(vii) Compliance & Governance

Disse syv arbejdsspor dækkede tilsammen omkring 32 projekter. Hvert projekt omfattede underliggende leverancer med det formål at sikre efterlevelse af GDPR inden for det givne område. Blandt de 32 projekter kan følgende særligt fremhæves:

a) Projekt vedrørende opbevaring og sletning. Projektet havde til formål at implementere opbevaringsregler og slettefunktionalitet i IT-systemer, hvor der behandles personoplysninger.

b) Projekt vedrørende oplysningspligt. Der blev i forbindelse med projektet udarbejdet nye privatlivspolitikker, og der blev udsendt 3,6 millioner privatlivspolitiker til kunder.

c) Projekt vedrørende samtykker. Projektet havde til formål at skabe et overblik over, hvor banken brugte samtykke som behandlingshjemmel, og der blev derfor foretaget en screening af alle kundedokumenter og -kontrakter. Samtidig blev der udarbejdet samtykker, der levede op til kravene i GDPR.

d) Projekt vedrørende markedsføring og analyse. Formålet med projektet var at sikre, at banken ikke foretog profilering af kunder i strid med GDPR.

e) Projekt vedrørende indsigt. Indsigtsprojektet havde til formål at sikre, at datasubjekter kunne få indsigt gennem en automatiseret proces, hvor kunden får en rapport med oplysninger fra mere end 300 IT-systemer. Projektet dækkede også kravene i relation til dataportabilitet.

f) Etablering af et GDPR supportteam bestående af 15 personer. Teamet var et uafhængigt supportteam i første forsvarslinje, som håndterede anmodninger fra kunder vedrørende behandling af personoplysninger.

g) Projekt vedrørende ustrukturerede data. Formålet med projektet var at udarbejde og implementere vejledninger, processer og governance vedrørende sletning af ustrukturerede data i emails, excelark, mv.

h) Projekt vedrørende træning af medarbejdere. Med projektet blev der gennemført obligatorisk GDPR-træning af mere end 20.000 medarbejdere på tværs af Danske Bank koncernen. Som en del af træningen var der ligeledes målrettet træning af medarbejdere i særlige funktioner.

i) Intern oplysningskampagne. I marts 2018 blev der lanceret en stor oplysningskampagne for at sikre, at medarbejderne i banken havde tilstrækkelig viden om og kendskab til GDPR. Oplysningskampagnen havde særlig fokus på de vigtigste principper i GDPR, vejledninger om oprydning, rapportering af brud på persondatasikkerheden, og hvordan datasubjekternes rettigheder sikres. Kampagnen blev gentaget i 2019 og 2020.

j) Udarbejdelse af politikker, instruktioner og forretningsgange, herunder gennemgang af eksisterende politikker, instruktioner og forretningsgange.

k) Projektet vedrørende databehandleraftaler. Projektet inkluderede en gennemgang af mere end 5.000 kontrakter med henblik på at klarlægge, om der var behov for ændringer som følge af nye krav med GDPR. Et GDPR-tillæg blev indsat i mere end 350 kontrakter, og underskrevne kopier blev indhentet fra databehandlerne.

l) Projekt vedrørende konsekvensanalyser. Projektet havde blandt andet til formål at implementere en proces, hvormed det bliver sikret, at banken udarbejder de nødvendige risikovurderinger. Herudover blev der udarbejdet skabeloner til konsekvensanalyser og til arbejdet med Privacy by Design og Privacy by Default.

m) Projekt vedrørende brud på persondatasikkerheden. Formålet med projektet var bl.a. at implementere en proces for håndtering af brud på persondatasikkerheden for at sikre, at alle brud bliver underlagt en passende vurdering, og at der er dokumentation for alle underretninger om brud på persondatasikkerheden i Danske Bank.

Den 25. maj 2018 var de fleste projekter gennemført i overensstemmelse med det scope, der var sat for projekterne.

Visse af projekterne vedrørende opbevaring og sletning viste sig dog at være for omfattende og for komplicerede til at nå deres respektive mål til den 25. maj 2018. Danske Bank's svar på spørgsmål 6 nedenfor indeholder en status på projekterne vedrørende opbevaring og sletning pr. 25. maj 2018. Herudover redegøres der for det fortsatte arbejde med projekterne frem til den 1. november 2020.

Bilag 3 indeholder et overblik pr. 30. november 2020 over de overordnede leverancer i projektet vedrørende opbevaring og sletning af personoplysninger.

1.3 **Omfang**

Som nævnt ovenfor omfattede Danske Bank's projekt i forhold til opbevaring og sletning hele Danske Bank koncernen, dvs. alle forretningsenheder, markedsområder og datterselskaber, og var som følge heraf meget stort.

Danske Bank valgte derfor en fasebaseret tilgang for at opdele arbejdet med opbevaring og sletning i håndterbare dele. En løsning, hvor banken sikrede en samlet overholdelse af GDPR på en gang, var ikke mulig på grund af den mængde af ressourcer, som det ville kræve at gennemføre dette. Danske Bank havde også allerede involveret mere end 250 medarbejdere i GDPR Programmet siden maj 2016, og det var derfor hverken realistisk eller effektivt at allokere flere medarbejdere til Programmet.

1.4 **Opsummering**

Som vi har beskrevet ovenfor, er der ikke noget kort og simpelt svar på spørgsmålet "Hvornår og hvordan Danske Bank A/S konstaterede problemet med manglende sletning".

Opbevaring og sletning af personoplysninger var en del af Danske Bank's generelle GDPR Program, og problemerne blev konstateret løbende i forbindelse med arbejdet i Programmet.

2 SPØRGSMÅL (5): OMFANGET AF DANSKE BANK A/S' EGEN UNDERSØGELSE AF FORHOLDET, HERUNDER OM BANKEN ALENE HAR UNDERSØGT EN AFGRÆNSET DEL AF BANKENS FORRETNINGSOMRÅDER I FORHOLD TIL OPBEVARING AF PERSONOPLYSNINGER

2.1 Vores forståelse af spørgsmålet

Med dette spørgsmål antages det, at en "undersøgelse" af forholdet har fundet sted.

Problemerne med opbevaring og sletning af personoplysninger i Danske Bank relater sig, som beskrevet ovenfor, imidlertid ikke til en "hændelse", såsom et brud på persondatasikkerheden, som kan "undersøges" på en afgrænset måde. Problemet er nærmere et IT-problem af en bredere karakter. Som følge heraf er problemet blevet "undersøgt" undervejs i GDPR Programmets arbejde med IT-systemer.

"Undersøgelsen" vedrørte alle forretningsenheder i Danske Bank, se ovenfor.

For at kunne forstå og beskrive Danske Bank's problemer med opbevaring og sletning er det også nødvendigt at forstå opbygningen af Danske Bank's IT-systemer. Nedenfor giver vi derfor en kort beskrivelse af opbygningen af Danske Bank's IT-systemer.

2.2 Introduktion

Danske Bank påbegyndte, som nævnt, bankens GDPR Program i maj 2016. Sigtet med Programmet var, at Danske Bank i maj 2018 skulle være i stand til at efterleve kravene i GDPR, herunder i relation til implementering af effektive funktionaliteter vedrørende opbevaring og sletning i IT-systemer. Arbejdssporene i GDPR Programmet er beskrevet i besvarelsen af spørgsmål 1 ovenfor.

I den oprindelige tidslinje for GDPR Programmet var det forventet, at de fleste af - men ikke alle - initiativerne til at sikre efterlevelse af GDPR, i relation til opbevaring og sletning af personoplysninger, ville være på plads til den 25. maj 2018. Det var endvidere forventet, at det ville være nødvendigt at udvide tidslinjen i forhold til opbygning af "business-as-usual"-aktiviteter på de leverede initiativer.

"Business-as-usual"-aktiviteter blev defineret som en fortsat implementering af et governance framework i forretningsenhederne samt et fokus på organisatorisk implementering med henblik på at bevare og styrke synligheden af og viden om GDPR, og derigennem opnå, at GDPR Programmets initiativer fremover blev en integreret del af hverdagen i Danske Bank.

2.3 Baggrundsinformation om IT-systemer i Danske Bank

Det er nødvendigt at kende det generelle setup for IT-systemer i Danske Bank for at kunne forstå Danske Bank's arbejde med opbevaring og sletning.

Historisk set var alle IT-systemer i banken placeret på en mainframe, hvor der var implementeret opbevarings- og slettefunktionaliteter i relation til kunder og konti. Når en kunde forlod banken, blev kundeoplysningerne slettet på mainframen i overensstemmelse med opbevaringsregler, som var baseret på kommercielle behov og på juridiske krav.

Danske Bank fokuserede indtil 2016 på opbevaring og sletning af oplysninger i systemer på mainframen, og havde alene et begrænset fokus på sletning af oplysninger i lokale systemer.

Behandling af personoplysninger om en kunde kan alene finde sted, hvis banken har oplysninger om kunden i kundesystemet, et centralt system som nærmere beskrevet nedenfor. Alle andre systemer er derfor afhængige af, at kunden er registreret i kundesystemet.

Danske Bank har pr. 1. november 2020 både systemer, som er centrale systemer på en mainframe, og systemer, som er lokale systemer uden for mainframen. Disse systemer dækker alle forretningsenheder i Danske Bank.

IT-setuppet er beskrevet i **Bilag 4**.

De centrale IT-systemer understøtter processerne for transaktioner, kreditter, kort, lån, investeringer, konti og den centrale kundedatabase ("kernekundesystem/KKS").

Som følge heraf indeholder de centrale systemer flest (person)oplysninger både i forhold til mængden af oplysninger og i forhold til antallet af kunder. Dog kan (person)oplysninger om kunder også udelukkende være opbevaret i et lokalt system.

De lokale systemer understøtter specifikke services til kunderne. Der er f.eks. et lokalt system for Mobilbank. De lokale systemer vil, i mange tilfælde, være afhængige af oplysninger, som behandles i ét eller flere centrale systemer. Oplysningerne i de centrale systemer vil dermed i vidt omfang have karakter af "master data".

Danske Bank har to typer af lokale systemer:

a) Lokale systemer, der modtager personoplysninger fra centrale systemer og sender personoplysninger tilbage til de centrale systemer

b) Lokale systemer (decentrale), der er helt uafhængige af de centrale systemer.

Som led i Danske Bank's governance setup er ejere af IT-systemer forpligtede til at:

a) Fastsætte sletteregler for personoplysninger

b) Dokumentere de fastsatte sletteregler i "Retention Rule Tool"

c) Implementere passende procedurer for løbende sletning

d) Designe og implementere kontroller for at sikre, at lokale systemer er dokumenterede, og at der er implementeret sletteregler (Business Risk & Control afdelingen)

2.3.1 Vedrørende a) lokale systemer, der er afhængige af de centrale systemer

Når en person bliver kunde i Danske Bank, bliver kundens personoplysninger opbevaret i et centralt system, samt i et lokalt system med henblik på at kunne tilbyde en specifik service eller et specifikt produkt. Grundet det lokale systems afhængighed af det centrale system, vil personoplysninger blive opbevaret i det centrale system, så længe der behandles personoplysninger om kunden i det lokale system.

Når en kunde ophører med at benytte en Danske Bank service eller et produkt, som er understøttet af et lokalt system, vil det lokale system informere det centrale system om, at datasubjektet ikke længere er aktiv i det pågældende lokale system.

Dette udløser, at det centrale system kontrollerer, om datasubjektet stadig er aktiv i et andet lokalt system, som er afhængig af data fra det centrale system. Hvis dette ikke er tilfældet, bliver personoplysningerne om datasubjektet i det centrale system herefter frigivet til sletning i overensstemmelse med opbevaringsreglerne i det centrale system.

Med andre ord, og som beskrevet ovenfor, så betyder brugen af et centralt system som leverandør af "master data" til lokale systemer, at lokale systemer i praksis også styrer, hvornår "master data" ikke længere er nødvendige for en forretningsproces. Den omstændighed, at centrale systemer ikke har brug for oplysningerne til egne formål, betyder således ikke nødvendigvis, at oplysningerne kan frigives til sletning i de centrale systemer, idet et fortsat behov for oplysningerne i lokale systemer kan begrunde en fortsat opbevaring i det centrale system.

Personoplysninger i de lokale systemer bliver slettet i medfør af specifikke sletteregler for hvert lokalt system.

I afsnit 5.4 beskrives samspillet mellem lokale systemer og centrale systemer i flere detaljer.

2.3.2 Vedrørende b) lokale (decentrale) systemer, der er helt uafhængige af de centrale systemer

Disse lokale systemer er ikke afhængige af personoplysninger fra andre systemer. Personoplysningerne bliver derfor opbevaret i overensstemmelse med de sletteregler, der er fastsat for hvert enkelt lokalt system, og påvirker således ikke opbevaringsperioden for centrale systemer.

I afsnit 5.6 gives flere oplysninger om det udestående arbejde med opbevaring og sletning i lokale systemer.

2.4 **Opsummering**

Vi har ovenfor givet en kort beskrivelse af opbygningen af Danske Bank's IT-systemer. Danske Bank's IT-systemer er, som man kan se, meget store, indbyrdes forbundne og har en kompleks opbygning.

Danske Bank blev opmærksom på udfordringerne i forhold til opbevaring og sletning af personoplysninger under arbejdet med de dele af GDPR Programmet, der relaterer sig til IT-systemerne.

IT-systemerne, der var i scope for Programmet, dækker alle forretningsenheder i Danske Bank.

3 SPØRGSMÅL (2): HVAD DER LIGGER TIL GRUND FOR DEN MANGLENDE SLETNING AF PERSONOPLYSNINGER
SPØRGSMÅL (3): HVORI PROBLEMET BESTÅR

3.1 **Vores forståelse af spørgsmålet**

Forholdets natur taget i betragtning er det vores opfattelse, at årsagen til den manglende sletning af personoplysningerne er den samme som problemet, der forårsager den manglende sletning af personoplysninger.

Vi har derfor valgt at besvare spørgsmål 2 og 3 under ét for at give Datatilsynet et klart og forståeligt svar og for at undgå gentagelser.

Besvarelsen af spørgsmålene er tæt knyttet til beskrivelsen af Danske Bank's GDPR Program og udfordringerne med at færdiggøre de dele af Programmet, som er relateret til opbevaring og sletning, til 25. maj 2018, og som er beskrevet ovenfor.

Spørgsmål 2 og 3 er således i vidt omfang besvaret ovenfor i dette brev. Såvel årsagen som problemet er kort fortalt, at nogle af projekterne vedrørende opbevaring og sletning var for store og for komplekse til at nå deres respektive mål til tiden.

Svaret på spørgsmål 6 indeholder en status over projektet vedrørende opbevaring og sletning pr. 25. maj 2018 samt oplysninger om videreførelse af projektet fra 25. maj 2018 frem til 1. november 2020. I svaret på spørgsmål 6 redegøres der desuden for, hvordan Danske Bank har arbejdet med og vil fortsætte med at arbejde med de opgaver, der udestod pr. 25. maj 2018.

Vi vil for at undgå gentagelser derfor ikke komme med flere bemærkninger i denne del af brevet.

4 SPØRGSMÅL (4): OMFANGET AF PROBLEMET, HERUNDER MÆNGDEN OG KATEGORIEN AF PERSONOPLYSNINGER OG OM PROBLEMET ER ISOLERET TIL DANMARK

4.1 Mængden og kategorierne af personoplysninger

Danske Bank har opbevaret alle typer af personoplysninger, herunder almindelige personoplysninger (artikel 6) og følsomme personoplysninger (artikel 9), i længere tid end nødvendigt.

Der er typisk tale om personoplysninger om:

a) Kunde-ID

b) Kontaktinformation

c) Personnummer

d) Andre kerneoplysninger

e) Produktoplysninger

f) Kontooplysninger

g) Låneoplysninger

h) Kreditkortoplysninger

i) Transaktionsoplysninger

4.2 **Omfanget af problemet**

I brede termer kan de personoplysninger, som Danske Bank behandler om sine kunder pr. 1. november 2020, inddeles i tre kategorier:

a) Personoplysninger i systemer, der var omfattet af de nødvendige opbevaringsregler/sletteregler forud for februar 2019. Sletning af disse oplysninger blev dog sat i bero i februar 2019, se afsnit 6. Oplysninger omfattet af a) blev således slettet på almindelig vis forud for februar 2019, og sletningen vil blive genoptaget, når det er muligt.

   Det bemærkes, at Danske Bank, siden sletning blev sat i bero i februar 2019, løbende har gennemgået sine systemer og data for at sikre, at opbevaringen er nødvendig og proportional. Banken har endvidere genoptaget sletning, hvor dette har været muligt. På denne baggrund finder Danske Bank, at banken lever op til sine forpligtelser i relation til sletning af oplysninger omfattet af punkt a).

b) Personoplysninger i systemer, der ikke var omfattet af de tilsigtede opbevaringsregler/sletteregler forud for februar 2019. Sletning af disse oplysninger blev fra februar 2019 sat i bero, se afsnit 6. Danske Bank har imidlertid i perioden siden februar 2019 fastsat og implementeret de nødvendige opbevaringsregler/sletteregler, der pr. 1. november 2020 gør Danske Bank i stand til at aktivere sletning, når det er muligt.

   Det bemærkes, at Danske Bank, siden sletning blev sat i bero i februar 2019 løbende gennemgået sine systemer og data for at sikre, at opbevaringen er nødvendig og proportional. Banken har foretaget sletning, hvor dette har været muligt. Danske Bank finder derfor, at banken pr. 1. november 2020 lever op til sine forpligtelser i relation til oplysninger omfattet af punkt b).

c) Personoplysninger, der er omfattet af det ikke færdiggjorte arbejde i forhold til opbevaring og sletning, se endvidere afsnit 5.6. Det er i forhold til disse områder/projekter, at Danske Bank ikke lever op til GDPR's krav i relation til opbevaring og sletning af personoplysninger. Det er ikke muligt at give et estimat for, hvor mange personoplysninger, der skulle have været slettet, herunder i hvilket omfang personoplysningerne kunne have været blevet slettet, se afsnit 6.

4.3 **Er problemet isoleret til Danmark?**

Problemet er ikke isoleret til Danmark. Inden for Danske Bank A/S, som har hovedkvarter i Danmark, er der juridiske filialer etableret i følgende EU/EØS lande: Sverige, Norge, Finland, Letland, Litauen, Polen, Tyskland, Irland og Storbritannien. Danske Bank havde tidligere en filial i Estland, som nu er blevet lukket.

Hver af filialerne har kunder, der er indbyggere i de pågældende lande.

5 SPØRGSMÅL (6): HVAD DANSKE BANK A/S HAR FORETAGET SIG – OG AGTER AT FORETAGE SIG – FOR AT RETTE OP PÅ PROBLEMET

5.1 **Vores forståelse af spørgsmålet**

Forholdet er, som beskrevet ovenfor, tæt knyttet til Danske Bank's GDPR Program. Afhjælpningen af problemet med opbevaring og sletning af personoplysninger har været og vil fortsat blive håndteret som led i Programmet.

Vi vil derfor i det følgende kort beskrive den del af GDPR Programmet, som er gennemført efter 25. maj 2018, og som relaterer sig til opbevaring og sletning af personoplysninger.

5.2 Introduktion

Spørgsmålet vil blive besvaret i fire dele:

(i) Status i forhold til afsluttet arbejde med opbevaring og sletning pr. 25. maj 2018

(ii) Tidslinje for Danske Bank's arbejde med opbevaring og sletning fra 25. maj 2018 frem 1. november 2020

(iii) Status i forhold til afsluttet arbejde med opbevaring og sletning pr. 1. november 2020

(iv) Danske Bank's planer i forhold til at afslutte det udestående arbejde med opbevaring og sletning

I **Bilag 5** har vi indsat illustrationer og beskrivelser af princippet for opbevaring og sletning i centrale systemer og lokale systemer.

5.3 (i) Status i forhold til afsluttet arbejde med opbevaring og sletning pr. 25. maj 2018

Danske Bank havde foretaget følgende pr. 25. maj 2018:

a) Indført regler om opbevaring af personoplysninger i de centrale kundesystemer i Danske Bank (212 ud af 251 opbevaringsregler). "Opbevaringsregler" betyder i denne sammenhæng kriterier for opbevaring af personoplysninger - når opbevaring ikke længere er berettiget efter de fastsatte kriterier, kan oplysningerne frigives til sletning. Tallene viser, hvor mange regler om opbevaring, der faktisk var implementeret, ud af hvor mange regler om opbevaring, der skulle have været implementeret, pr. 25. maj 2018. Det bemærkes, at de sidste regler om opbevaring blev implementeret i Q4 2019, som beskrevet yderligere nedenfor.

b) Indført regler om opbevaring af personoplysninger i lokale systemer relateret til Future Financing, Cards, Payment Solutions og andre lokale systemer.

c) Foretaget oprydning/sletning i størstedelen af HR-oplysninger, herunder implementering af opbevarings- og sletteregler.

d) Foretaget oprydning/sletning i kunde- og produktoplysninger i visse lokale IT-systemer

e) "Customer Data Retention Rule Tool version 1" var på plads i midten af juni 2018, men meget tæt på at være færdig i maj 2018. Dette system bruges til at administrere regler om opbevaring af personoplysninger og anvendes på tværs af IT-systemer i Danske Bank.

5.4 (ii) Tidslinje for Danske Bank's arbejde med opbevaring og sletning fra 25. maj 2018 frem til 1. november 2020

Juni 2018 - Marts 2019
Danske Bank fortsatte arbejdet, efter at GDPR fandt anvendelse.

Den næste fase af projektet vedrørende opbevaring og sletning blev lanceret med fokus på lokal opbevaring, fysiske arkiver og data warehouse.

Nye vejledninger fra Datatilsynet nødvendiggjorde også, at nye projekter blev iværksat, for eksempel i forhold til kryptering af fortrolige og følsomme personoplysninger ved af transmission over internettet.

I erkendelse af at det ville kræve en betydelig og løbende indsats at vedblive med at efterleve reglerne i GDPR, skiftede GDPR Programmet samtidig fokus med henblik på sikring heraf, ligesom overgangen fra Programmet til business-as-usual blev planlagt.

Et master governance dokument, hvori GDPR-ansvaret for ejerne i forretningsenhederne blev beskrevet, blev introduceret. Dokumentet forbandt de kortlagte GDPR-krav med relevante ansvarsområder i alle enheder.

Governance var, som nævnt, forankret i forretningsprocesserne. Det blev dog konstateret, at de processer, der blev kortlagt i den tidlige fase af Programmet, ikke var blevet kortlagt i en grad, hvor forretningen kunne tage over. Dette førte til en fornyet gennemgang af alle de processer, som allerede var kortlagt, samt til identificering af nye processer, som ligeledes skulle kortlægges.

Danske Bank indså også i efteråret 2018, at det for at opnå overholdelse af GDPR var nødvendigt at igangsætte et separat projekt i forhold til optagelse af samtaler. Dette projekt omfattede blandt andet implementering af opbevarings- og slettefunktionaliteter.

April - Oktober 2019
I denne periode fastsatte Danske Bank procedurer for udarbejdelse af risikovurderinger og fastsættelse af kontroller for IT-systemejerne.

Konsolidering af eksisterende data warehouses var påbegyndt, og det blev i den sammenhæng besluttet at fokusere på oprydning og anonymiseringsprincipper for det fremtidige, konsoliderede data warehouse.

Arbejdet skred også frem inden for sporene vedrørende lokal opbevaring, fysiske arkiver og optagelse af samtaler.

Den udestående oprydning for lokale IT-projekter i Wealth Management, Asset Finance og HR-systemer blev færdiggjort i Q2 2019.

I august 2019 blev der etableret et Group Data Office. Denne enhed fik til opgave at koordinere udviklingen af et stærkere grundlag for data management inden for bankens forretningsområder.

Dette var, og er fortsat, fokuseret omkring en række integrerede arbejdsspor, som tilsammen danner dette nye grundlag:

a) Koncerndata strategi ("Group Data Strategy"). En aftale om fælles måder at arbejde på og fokus på at adressere bankens udfordringer og ambitioner.

b) Datakendskab ("Data Awareness"). Initiativer på tværs af koncernen i relation til kommunikation og træning målrettet at bygge en datakultur og en fælles måde at arbejde på.

c) Instruktion for styring af koncerndata ("Group Data Management Instruction"). Instruktionen definerer principperne for dataejerskab, datakvalitet og dataarkitektur i banken.

d) Data governance ("Data Governance"). Registrering af dataejer, data steward, ordforklaringer, definitioner og standarder for data.

e) Dataarkitektur ("Data Architecture"). Registrering af flowet af data på tværs af forretningsområder og IT-systemer.

f) Datakvalitet ("Data Quality"). Opstilling af standarder for måling af datakvalitet, centralisering af rapportering af datakvalitet, og centralisering af registrering af og styring af problemer med data.

Data Protection Compliance teamet identificerede, at Danske Bank manglede et informationsstyrings-setup og et data governance framework, der går på tværs af koncernen. Teamet flagede i observationer i 2018 (som blev konsolideret til én observation i oktober 2019), de risici - i forhold til manglende efterlevelse af GDPR - der kan være forbundet med ikke at have dette på plads. Observationen førte til, at banken etablerede Group Data Office, som pt. er i gang med at udvikle en koncernfunktion for Group Information Records Management og et framework, som vil hjælpe med at sikre banken en effektiv og systematisk kontrol med data samt afhjælpe identificerede problemer med datakvalitet og opbevaring og sletning. Designet af den operative model er sat til at være på plads i slutningen af 2020, og implementering af et funktionelt setup begynder i 2021. Se afsnit 5.6 nedenfor for flere oplysninger.

<u>November - December 2019</u>
GDPR Programmet blev instrueret i at fokusere på overgangen til business-as-usual. Et begrænset antal projekter fortsatte dog ind i 2020.

Det væsentligste videreførte projekt vedrørte implementering af opbevarings- og slettefunktionaliteter.

Arbejdet med opbevaring og sletning i centrale systemer blev færdiggjort i Q4 2019. Danske Bank etablerede en proces for opbevaring af centrale kundeoplysninger, også kendt som "Customer Clean-up", som også er beskrevet og illustreret i **Bilag 5**.

Processen kan beskrives som følgende:

a) Oprydning af kunder udføres automatisk hver måned

b) Setuppet indeholder +250 opbevaringsregler, også betegnet som "clean-up members"

c) Hver opbevaringsregel er definitionen på en legitim, forretningsmæssig begrundelse for at bevare kunder

d) Hver opbevaringsregel bruger en SQL til at udvælge en liste over kunde-ID'er fra et produktsystems lokale tabel(ler)

e) Aggregeringen af alle lokalt generede lister med kunde-ID'er udgør de centrale opbevaringsmålgrupper ("Central Retention Targets")

f) Kunde-ID'er, som ikke længere er nødvendige for lokale systemer, er slettekandidater.

Danske Bank fortsatte med at implementere funktionalitet i forhold til opbevaring og sletning i lokale systemer, Data Warehouse og systemer til opbevaring af optagede samtaler, men arbejdet var endnu ikke færdiggjort.

Der blev fastsat sletteprincipper for personoplysninger i fysiske arkiver.

Aktiviteter med det formål at rydde op i ustrukturerede data blev færdiggjort på tværs af koncernen i Q4 2019.

Det sidste projekt, der blev startet og finansieret af GDPR Programmet, var et projekt omkring brugen af personoplysninger i testmiljøer. Der blev foretaget vurderinger af den daværende behandling af oplysninger i testmiljøer, og eksisterende forretningsgange og vejledninger blev opdateret. Danske Bank analyserede endvidere behovet for brug af værktøjer til understøttelse af maskering, scanning og automatiseret kontrol. Målet var et sikre efterlevelse af GDPR ved at benytte anonymiserede data i vores testmiljøer og samtidig sikre rettidig oprydning, hvis produktionsdata var nødvendige i forbindelse med problemsøgning.

Januar - November 2020
Da Programmet var ved at trappe ned, blev alle udviklingsområder i IT instrueret i at fortsætte deres arbejde og bruge det afsatte budget for 2020.

Projektet med fysiske arkiver blev afsluttet i Q1 2020. Projektet gennemgik og opdaterede regler for opbevaring af dokumenter håndteret af eksterne samarbejdspartnere og leverede GDPR-vejledninger til oprydning i interne, lokale fysiske arkiver. Vejledningerne indeholder overordnede instruktioner om, hvordan fysiske arkiver skal håndteres, hvordan regler for opbevaring fastsættes, og hvordan oprydning foretages.

Danske Bank fortsatte i løbet af denne periode sit arbejde med implementering af funktionalitet til håndtering af opbevaring og sletning i lokale systemer, Data Warehouse, testmiljøer og systemer indeholdende optagede samtaler.

Programmet fortsatte med et reduceret antal medarbejdere med fokus på overgangen til business-as-usual.

5.5 (iii) Status for færdiggjort arbejde med opbevaring og sletning per 1. november 2020

En oversigt over projekter i GDPR Programmet, som involverer opbevarings- og sletteaktiviteter, er vedlagt som **Bilag 6**. Dette bilag viser status pr. 1. november 2020 og hovedmålene for hvert projekt.

Følgende projekter i Danske Bank er blevet færdiggjort pr. 1. november 2020:

a) Opbevaring af kundeoplysninger centralt (færdiggjort Q4 2019)

b) HR (færdiggjort Q2 2019)

c) Wealth Management (færdiggjort Q2 2019)

d) Ustrukturerede data (færdiggjort Q4 2019)

e) Fysiske arkiver (færdiggjort Q1 2020)

Bilag 3 viser en mere detaljeret oversigt over de overordnede leverancer i disse projekter vedrørende opbevaring og sletning siden 2016.

5.6 (iv) Danske Bank's planer for at færdiggøre det udestående arbejde med opbevaring og sletning

Bilag 6 viser de ikke-færdiggjorte projekter. Det er i forhold til disse områder/projekter, at Danske Bank ikke lever op til kravene i GDPR om opbevaring og sletning.

Projekterne, hvor der endnu ikke er implementeret regler/funktionalitet for opbevaring og sletning, er:

a) Opbevaring af kundeoplysninger i lokale systemer (forventet færdiggørelse Q4 2021)
   - Status: Danske Bank er i øjeblikket i gang med at kortlægge alle lokale systemer for (i) at kunne identificere, hvilke systemer der endnu ikke har fået implementeret regler om opbevaring og sletning, og (ii) for at kunne udarbejde en plan sammen med IT-systemejerne for implementering af regler for opbevaring og sletning.

b) Data Warehouse (forventet færdiggørelse Q4 2021)
   - Status: Værktøjer til anonymisering er blevet implementeret for visse dele af oplysningerne i Data Warehouse. Danske Bank arbejder i øjeblikket med implementering af anonymiseringsværktøjer for de resterende dele af oplysningerne i Data Warehouse.

c) Testmiljøer (forventet færdiggørelse Q2 2021)
   - Status: Danske Bank har anvendt produktionsdata i testmiljøer. Formålet med denne anvendelse af produktionsdata er at muliggøre testning og validering af forretningsløsninger forud for implementering i produktionsmiljøet. Dette sikrer ordentlig kvalitet i de implementerede løsninger. Der er i øjeblikket i visse tilfælde ikke andre muligheder for at teste systemer tilstrækkeligt, men best practice er at minimere, at det sker. Danske Bank arbejder på at etablere automatiserede procedurer for oprydning, samt på at udvikle et forbedret, centralt værktøj for maskering af oplysninger. Planen er at genoverveje og optimere den måde, hvorpå der på nuværende tidspunkt foretages maskering af oplysninger, samt etablere ejerskab i forhold til oplysninger, kontroller, godkendelser, og adgangskontrol. Der bliver tillige foretaget interne vurderinger af niveauet for efterlevelse af GDPR i forhold til testdata, governance og kontroller i testmiljøerne. Danske Bank har i den forbindelse identificeret tilknyttede problemstillinger udover opbevaring og sletning, hvor GDPR ikke overholdes.

d) Optagelser af samtaler (forventet færdiggørelse Q1 2021)
   - Status: Danske Bank har af en ekstern leverandør købt en løsning, der kan supplere det eksisterende system til optagelse af samtaler. Denne supplerende løsning understøtter automatisk sletning. Løsningen er blevet succesfuldt installeret i Q4 2020. Regler om opbevaring og sletning er under udarbejdelse, og vil blive lagt ind i systemet for at muliggøre sletning. Projektet vil herefter være afsluttet.

"Forventet færdiggørelse" betyder, at der er implementeret funktionaliteter i de(t) relevante system(er), og at funktionaliteten er klar til at blive aktiveret.

Som nævnt ovenfor i afsnit 5.4 identificerede Data Protection Compliance teamet, at der mangler et informationsstyrings-setup og et data governance framework, der går på tværs af koncernen. I den forbindelse

flagede teamet en observation, der fremhævede de risici - i forhold til manglende efterlevelse af GDPR - der kan være forbundet hermed.

Dette førte til etablering af Group Data Office, som i øjeblikket er i gang med at udvikle en koncernfunktion for informationsstyring og et framework, som vil hjælpe med at sikre effektiv og systematisk kontrol med data og afhjælpe identificerede problemer med datakvalitet og opbevaring og sletning. Designet af den operative model er planlagt til at være færdig i slutningen af 2020, og implementering af et funktionelt setup begynder i 2021.

Group Data Office, som ledes af en Chief Data Officer, skal blandt andet være

- overordnet ansvarlig for at definere og vedligeholde datastrategien, som sætter retningen for, hvordan data bliver håndteret og set.

- ansvarlig for at sikre, at enhver person, der er tildelt ejerskab eller ansvar i relation til data management governance frameworket, trænes tilstrækkeligt og støttes for at sikre, at de kan opfylde deres roller effektivt.

- ansvarlig for overvågningen af forretningens compliance med data management framework standarderne og data management instruktionen.

- overordnet ansvarlig for at definere og vedligeholde en proces for at identificere forretningstermer og de underliggende data inden for den definerede dataklassemodel.

- ansvarlig for at sikre implementering af et IT-system til vedligeholdelse af en forretningsterminologi og dens underliggende dataattributter, og for at fastsætte minimumskrav for informationen, som skal være tilgængelig i et centralt informations governance værktøj.

- overordnet ansvarlig for at udarbejde vejledninger til etablering af kvalitets KPI mål og tærskler og rapportering af hvert Critical Data Element.

- ansvarlig for at facilitere rapportering på problemstatus.

5.7 **Opsummering**

Vi har i svaret på dette spørgsmål beskrevet den del af GDPR Programmet, som er relateret til opbevaring og sletning af personoplysninger, og som er udført, eller som skal udføres, efter 25. maj 2018.

Danske Bank har, som det fremgår af afsnit 5.6, næsten afsluttet de opgaver, der var udestående pr. 25. maj 2018, og forventer at være i stand til at afslutte de opgaver, der er udestående pr. 1. november 2020.

Danske Bank har endvidere etableret et Group Data Office, som skal udvikle en koncernfunktion for informationsstyring og et framework, og som skal medvirke til at sikre en effektiv og systematisk kontrol med data og afhjælpe identificerede problemer med datakvalitet og opbevaring og sletning.

6 BEVARELSE AF DATA I RELATION TIL DEN NON-RESIDENT PORTEFØLJEUNDERSØGELSE

Danske Bank er i løbende dialog med myndigheder omkring den ophørte, non-resident portefølje i bankens estiske filial, som var aktiv mellem 2007 og 2015. Dette inkluderer strafferetlige og regulatoriske undersøgelser foretaget af myndigheder i Estland, Danmark, Frankrig og USA ("Undersøgelserne").

Danske Bank er endvidere involveret i civile retssager i Danmark og USA angående den estiske sag ("Retssagerne").

Som del af Undersøgelserne og Retssagerne har Danske Bank været og fortsætter med at være undergivet juridiske forpligtelser til og har endvidere legitime interesser i at opbevare personoplysninger i struktureret og ustruktureret format.

Danske Bank har taget skridt til at bevare data, der er nødvendige og proportionale for Undersøgelserne og Retssagerne for at kunne forfølge en række kritiske interesser, herunder interesser i forhold til at sikre, at banken grundigt kan undersøge påstandene, samarbejde med regulatoriske myndigheder og retshåndhævende myndigheder, og kan forsvare sig mod potentielle civile og strafferetlige skridt.

Hvis Danske Bank ikke havde taget de pågældende skridt til opbevaring af oplysninger, ville der have været væsentlig materiel risiko for, at materiale, der potentielt kunne have været relevant, ville blive uopretteligt slettet. Nogle af de konsekvenser, som Danske Bank kunne blive mødt med, hvis potentielt relevant materiale ikke blev bevaret, inkluderer, men er ikke begrænset til, (i) manglende evne til fuldt ud at samarbejde med undersøgende myndigheder, (ii) potentiel strafferetlig forfølgelse på grund af destruktion af bevismateriale, og/eller (iii) manglende evne til at kunne forsvare sig mod civile og strafferetlige skridt mod Danske Bank og dets nuværende og tidligere ansatte.

Opbevaringen har ikke påvirket Danske Bank's arbejde med at udarbejde tekniske løsninger, mv., som kan muliggøre opbevaring og sletning i overensstemmelse med GDPR, men har påvirket timingen for implementering og aktivering af disse tekniske løsninger for visse systemer.

Danske Bank fortsætter med at gennemgå bankens systemer og data med henblik på at sikre, at bankens opbevaring af oplysninger er nødvendig og proportional. Danske Bank har gennem hele perioden, på grund af undersøgelsens fremskridt og for at sikre løbende overholdelse af sine forpligtelser i medfør af GDPR, genbesøgt de trufne foranstaltninger til bevarelse af data og genindført GDPR oprydningsprocesser, hvor det har været muligt, for at sikre, at den fortsatte opbevaring af oplysninger er nødvendig og proportional.

- 0 -

Vi foreslår at holde et møde, hvor Danske Bank, sammen med bankens juridiske rådgiver Plesner, yderligere kan uddybe bankens arbejde med opbevaring og sletning af data over for Datatilsynet.

Med venlig hilsen

[Sendt elektronisk og derfor ikke underskrevet]
Bo Svejstrup

7 BILAG

1) Beskrivelse af de koncernens løsningsprojekter

2) Oversigt over arbejdssporene i GDPR Programmet

3) Danske Bank koncernens overordnede leverancer i projekter vedrørende opbevaring og sletning siden 2016.

4) Illustration af opbygningen af Danske Bank's IT-systemer

5) Illustrationer og beskrivelser af princippet for opbevaring og sletning i centrale systemer og lokale systemer

6) Oversigt over færdiggjorte og ikke-færdiggjorte projekter, som involverer opbevarings- og sletteaktiviteter

Danske Bank

BILAG 1

GDPR Programme components

The three GDPR Programme Pillars

1. Group wide data mapping

The data mapping has been carried out on a risk based approach, where the sequence of each business entity is decided by their amount of personal data and level of complexity.

The Group wide data mapping is conducted by each business unit with the assistance of both GDP and NNIT Consultants.

The latter has facilitated the data mapping workshops and collected the GDPR data in a GDPR Tool.

2. Group wide Solution Projects

The Group wide Solution Projects are approved by Danske Bank GDPR Steering Committee.

Once a project manager has been allocated she co-creates a project charter, which is to be approved by the Project Steerco, on which the GDPR Programme is always represented.

3. Business unit level projects

The Group wide Solution Projects are designed to cover the entire Group. This is not feasible in every case, because some business entities run on separate IT platforms, demanding local GDPR Projects.

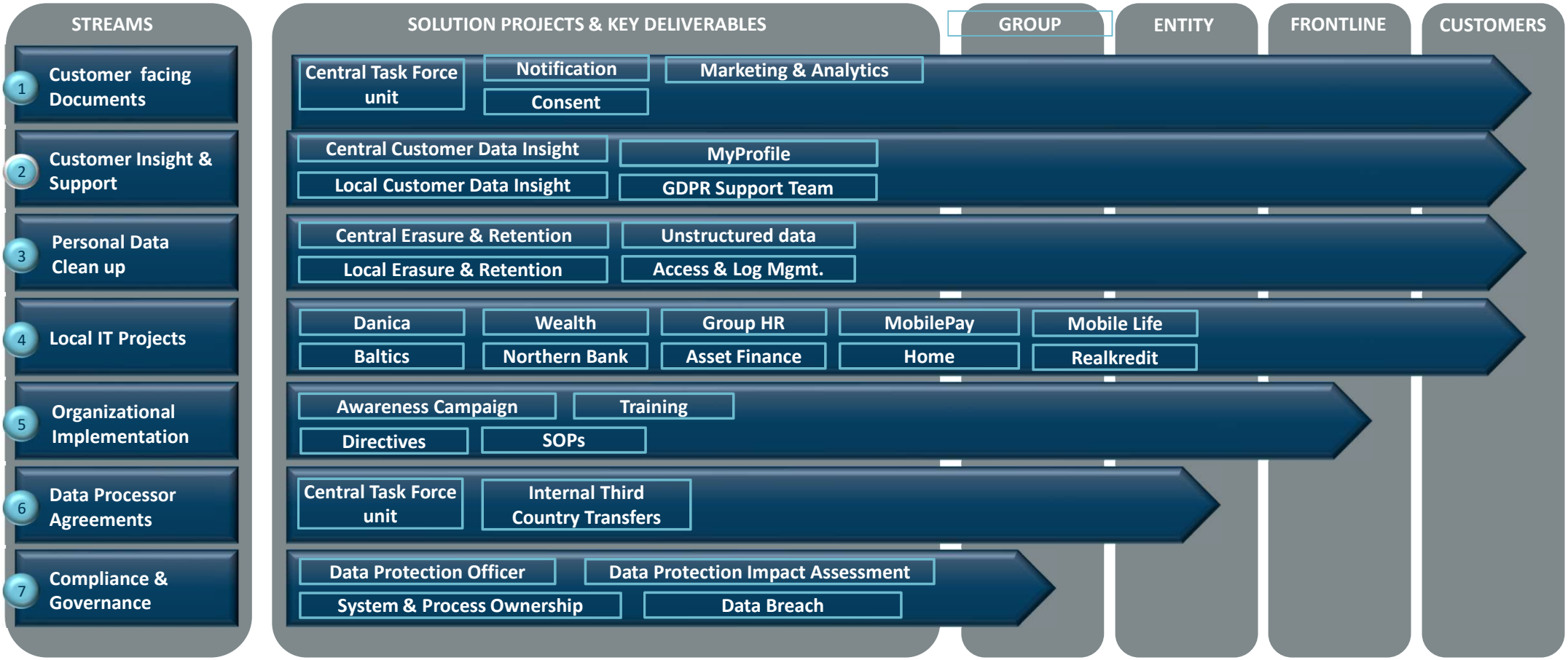
These will also be monitored by the GDPR Programme to ensure that the entire Group reaches the desired compliance levels.

Created: 16.12.2020

Danske Bank

BILAG 2

Overview of Work Streams and Solution Projects



Created: 27.11.2020

Danske Bank Group's deliveries in Erasure & Retention Projects Since 2016

BILAG 3

High-level Deliveries up until November 30th, 2020

- Applied retention rules to the central customer systems in Danske Bank
- Applied retention rules to local systems related to Future Financing, Cards, Payments Solutions and other local systems
- Clean-up most important HR data
- Clean-up in local customer and product data in some local IT systems
- Customer data Retention Rule Tool v 1 in place by mid June 2018, which is a system documenting each retention rule, where it is applied, etc.
- Activities to clean-up unstructured data throughout the Group (incl. training of employees)
- Clean-up in: Local IT systems in Wealth Management, Asset Finance etc.
- Completion of remaining clean-up for local IT
- Projects in Wealth Management, Asset Finance, HR systems etc.
- Local retention in product areas on central platform
- Anonymization tools have been implemented for some parts of the data in the Data Warehouse

Future Deliveries

- **Local retention –** Establishment of retention rules in remaining product areas on central platform
- **Data Warehouse -** Implementing anonymization tools on the remaining part of the data in the Data Warehouse.
- **Test & Syst. environments** – Retention & clean-up procedures
- **Voice recordings -** Retention rules are in the pipeline to be set up in the system to enable deletion which will complete the project

.

Created: 18.12.2020

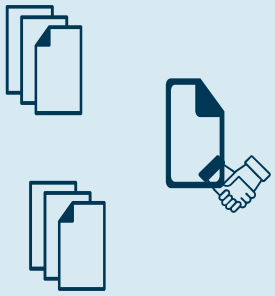
Danske Bank

High level overview – data and systems

BILAG 4

Unstructured data*
Manual clean-up, assessed by employees

Physical data

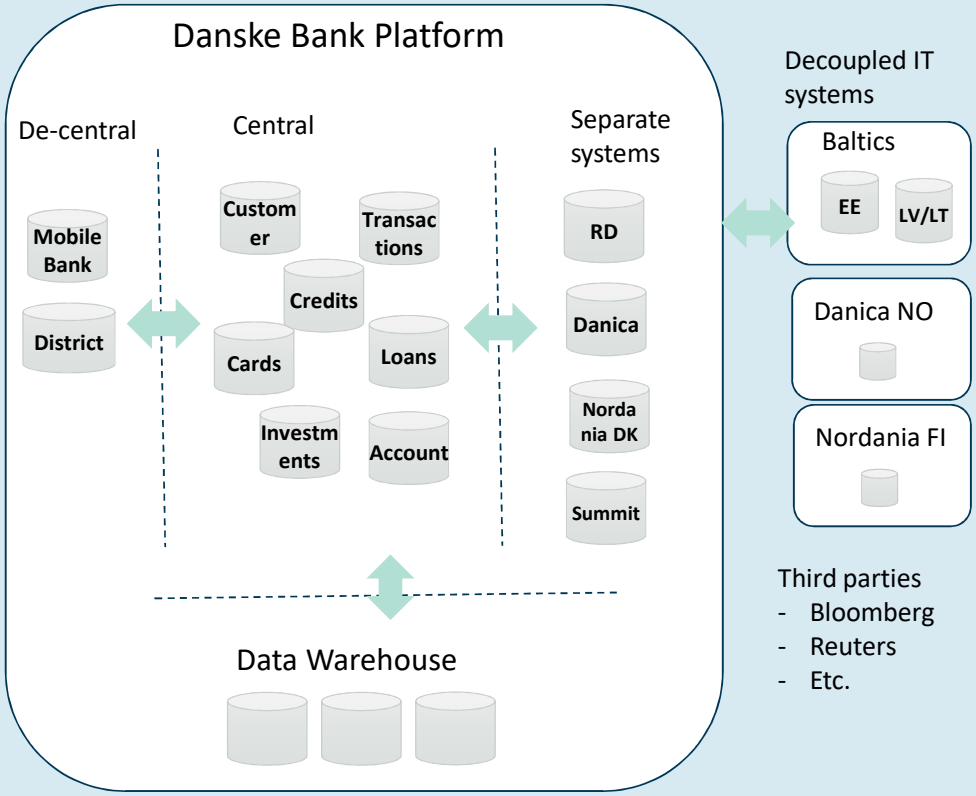


Examples: Signed agreements, print-out, microfiche

Electronical data

Examples: Outlook mail, I-drives, Sharepoint and confluence sites, USB keys

Structured data*
Automated clean-up, assessed by computer logic



*The systems shown are only examples

Created: May 2019 - presented to Group legal representatives to explain data definitions and Erasure scope

Danske Bank

BILAG 5

Customer Data central & local retention – done for Danske Bank central platform

Project was initiated May 2017, to assure that the existing clean-up functionality was updated and scope of clean-up extended to the whole Danske Bank central platform. Priority 1 central retention was done before 25 May 2018, priority 2 central retention before EOY 2018. Afterwards, the project used a phase-based approach to prioritize local retention, as it was realised that all scope could not be achieved at once.

Principle applied to clean-up of Danske Bank central platform

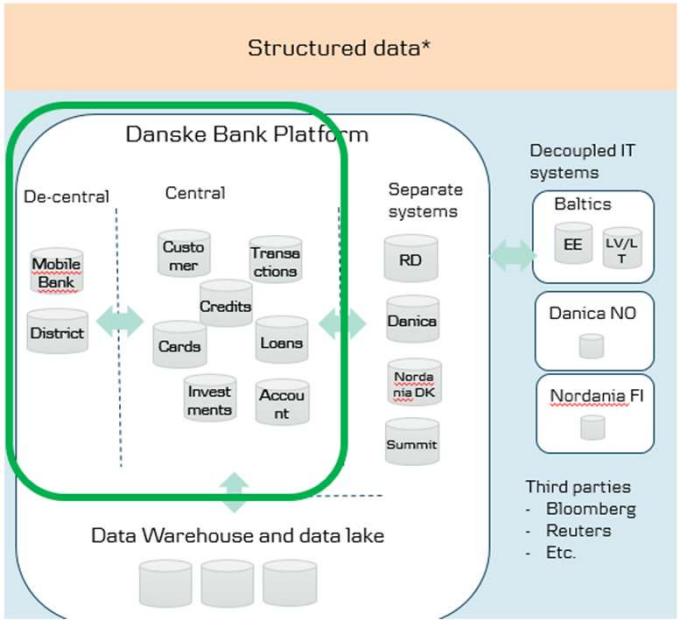
Central retention

Retention rules which directly impact clean-up of a customer. This also includes rules impacting customers who are both customers in Danske Bank and other legal entities. Meaning RD, Danica etc. have central retention rules impacting the Danske Bank central platform.

Local retention

Clean up in local databases and systems, on the Danske Bank central platform, which do not hold master copies of customer data.

Focus of project



*The systems shown are only examples

Created: 25.11.2020

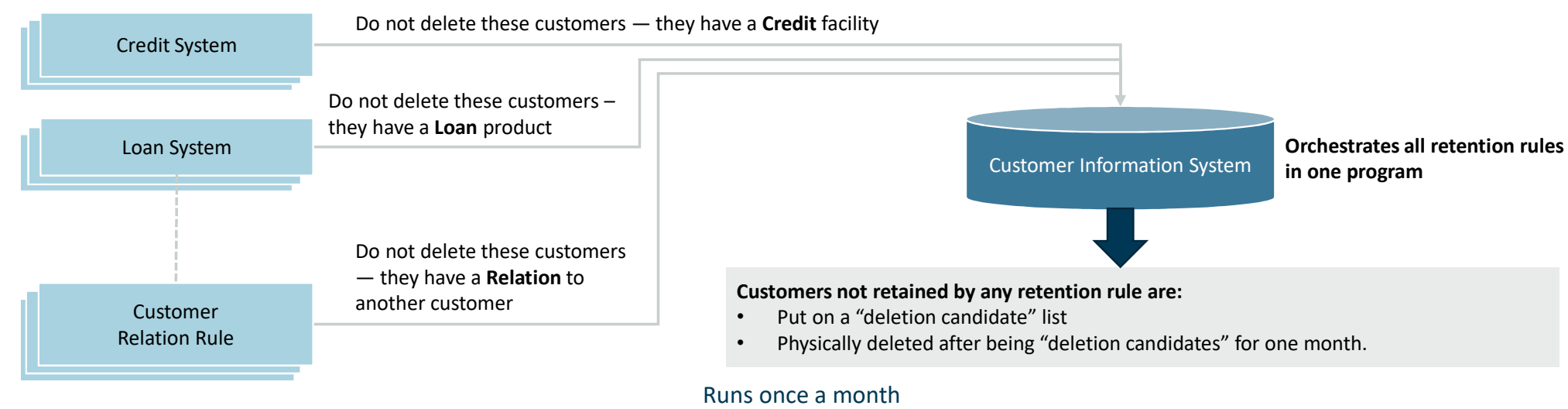
Danske Bank

BILAG 5

The central customer data retention process today, a.k.a. “Customer Clean-up”

- Clean-up of customers is performed automatically every month.
- The setup consists of +250 retention rules, also referred to as *clean-up members*.
- Each retention rule is the definition of a legitimate business reason to keep customers.
- Each retention rule uses an SQL to select a list of customer IDs from a Product System’s local table(s).
- The aggregation of all locally generated lists of customer IDs make up the *Central Retention Targets*.
- Customer IDs ”wanted” by none of the areas are deletion candidates.

Central Customer Retention Process (example)



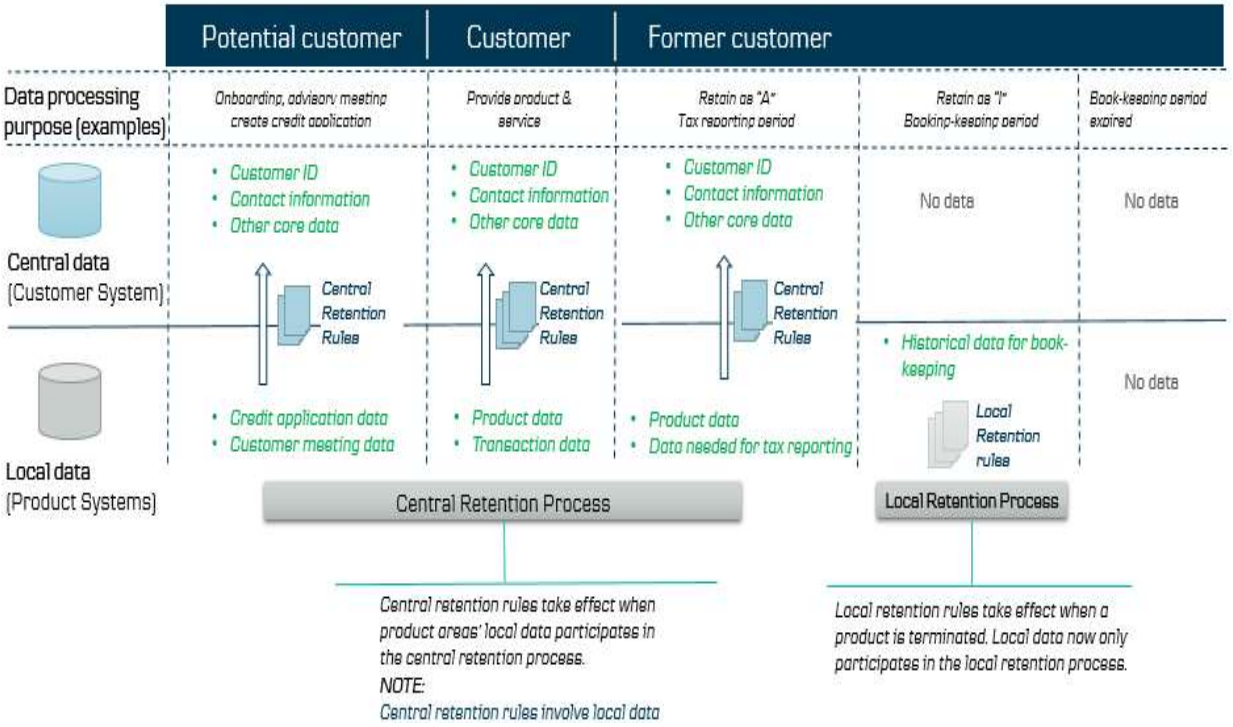
PUB/SUB setup implemented during 2019, and used by some areas for local retention

Created: Fall 2017, to explain principle for central retention. Presented in Business unit intro meetings January and February 2018
Change 25.11.2020: “+200 retention rules” changed to “+250 retention rules”, PUB/SUB status changed from planned to implemented. PUB/SUB is the principle for publishing and subscribing to system events.

Local retention

BILAG 5

Local retention



Clean up in local databases and systems,
which do not hold master copies of customer data.

There is no single way of doing this, this is based on the data and systems.

Created: 25.11.2020 to explain principle for central and local retention

Danske Bank

BILAG 5

Deletion by default – automatic clean-up – customers - example

Customer data can only be deleted when there is no related product data

	Potential customer	Customer			Former customer	
		 *Account, Loan, Credit card*	*Customer has paid back the loan after 5 years*	 *Account, Credit card*	*Customer leaves the bank after 16 years*	
Data processing purpose (examples)	*Onboarding, advisory meeting create credit application*	*Provide product & service*			*Retain for Tax reporting*	*Retain Booking-keeping period* / *Minimum data retention period expired*

 **Data kept for this customer**	• Customer ID
	• Contact information
	• Other core data
	• Credit appl. data
	• Customer meeting data
		• Customer ID
		• Contact information
		• Other core data
		• Product data
		  • Account
		  • Loan
		  • Credit Card
		• Transaction data
			• Customer ID
			• Contact information
			• Other core data
			• Product data
			  • Savings Account
			  • ~~Loan~~ (inactive)
			  • Credit Card
			• Transaction data
				• Customer ID
				• Contact information
				• Other core data
				• Product data
				  • Savings Account
				  • Credit Card
				• Transaction data
					Historical data for tax reporting, book-keeping, CIFI	Historical data for book-keeping / No data

Retention rules for keeping customer data 	*Keep data, this is a potential customer and there is a potential related product. If customer is not returning delete data after 6 months*	*Keep customer data, there is related product data (Account, loan, Credit Card)*	*Keep customer data, there is related product data (Account, Loan, Credit Card)*	*Keep customer data, there is related product data (Account, Credit Card)*	*Keep customer data, there is related product data (Account, Credit Card), which still has a legal warrant*	*No legal warrant to keep customer data customer data deleted*
Retention rules for keeping product data 			*Loan is paid out, marked inactive. No changes to account and credit card.*	*Loan data deleted after 10 years (no legal warrant) No changes to account and credit card.*	*Account and credit card marked inactive*	*No legal warrant to keep product data, product data deleted*

Created: February 2018, to explain principle for central and local retention to local legal representatives

Danske Bank

Overview of projects which included erasure activities

BILAG 6

Project	Key objective	Status
Structured data		
Customer Data central retention	Assure update of existing and determination of new retention rules, further assure cleanup of data on Danske Banks central platform, using principles of central retention.	Completed Q4 2019
Customer Data local retention	Assure update of existing and determination of new retention rules, further assure cleanup of data on Danske Banks central platform, using principles of local retention.	Expected to complete Q4 2021
HR	Assure determination of retention rules and clean-up of HR data for both Danske Bank central and country local IT platforms.	Completed Q2 2019
Wealth Management	Assure determination of retention rules and clean-up of Data local to the Wealth Management organisations IT platform.	Completed Q2 2019
Data Warehouse	Assure that source system retention rules are reflected on our data warehouse platform, meaning that data is deleted or anonymized when no longer retained in the source system.	Expected to complete Q4 2021
Test environments	Assure GDPR compliance by using anonymized data in our test environments and timely data clean-up if prod data is needed for problem testing.	Expected to complete Q2 2021
Unstructured data		
Unstructured Data	Assure group wide awareness of clean-up responsibilities attached to employees and managers clean-up of personal data (mail box's, H-drives, desks etc.)	Completed Q4 2019
Physical Archives	Assure determination of retention rules and clean-up of documents, microfiche etc, in all Danske Bank central and local archives.	Completed Q1 2020
Voice recordings	Assure determination of retention rules and clean-up in voice recordings in our group voice recording platform.	Expected to complete Q1 2021