The Data Protection Agency
Att. Kenni Elm Olsen
Carl Jacobsens Vej 35
2500, Valby

Sent by e-mail to dt@datatilsynet.dk

21 December 2020

CASE NO. 2020-431-0116 - DANSKE BANK A/S

The Danish Data Protection Agency (the "Agency") has by letter of 3 November 2020 (case no. 2020-431-0116) requested Danske Bank A/S ("Danske Bank") to answer six questions regarding retention and deletion of personal data.

Danske Bank shall hereby provide answers to the questions from the Agency.

In order to ease the reading of this letter, we have for each item added a parenthesis with the corresponding number of the question in the letter from the Agency.

The questions have been answered in a chronological order to provide the Agency with a better overview of the background and timeline of Danske Bank's work on retention and deletion. By answering in a chronological order, too many repetitions are also avoided. This means that the answers are not provided numerically.

The answers to the Agency's questions are further detailed in **Exhibit 1-6** containing descriptions and illustrations of the approach and implementations in Danske Bank related to retention and deletion. The exhibits cover the time period from 2016 to 1 November 2020.

CONTENTS

1 QUESTION (1): WHEN AND HOW DID DANSKE BANK A/S DISCOVER THE PROBLEM WITH THE NON-DELETION OF PERSONAL DATA?

1.1 Our understanding of the question

Danske Bank has not had any specific "incidents" leading to an investigation resulting in Danske Bank becoming specifically aware of the challenges with retention and deletion of personal data.

It is more correct to say that the work with retention and deletion of data in Danske Bank is an ongoing task. The Bank's GDPR Steering Committee was already dealing with retention and deletion in October 2016. This work has continued up till today and continues until Danske Bank is compliant with applicable retention and deletion obligations.

In the following, we provide a description of Danske Bank's work related to implementation of the GDPR.

1.2 Description of Danske Bank's GDPR implementation

There was political agreement regarding the GDPR in December 2015, and Danske Bank immediately began work on identifying and making the changes necessary to comply with it. In the following we provide a timeline of the major events of the GDPR Programme. Further, in the answer to question 5, we provide more details about the IT setup and the Retention and Deletion work stream.

January - May 2016

A project, including a number of initial work streams, was established in Group IT in January 2016 in order to initiate and anchor the implementation work surrounding the GDPR.

Awareness of the challenges in terms of scope, extent and funding was materializing as GDPR was formally adopted by the European Parliament in April 2016.

June - September 2016

The GDPR Programme was initiated immediately after the GDPR was adopted.

It became clear that a holistic, overall approach to the GDPR was necessary as the requirements were overlapping and solutions were depending on each other.

The GDPR Programme decided to incorporate and expand the scope of the initial workstreams. It was prioritised to conduct a thorough analysis of the requirements to decide on an approach that would cover all GDPR requirements and the entire Danske Bank group – all units, countries and market areas.

October - December 2016

A governance model was established for the GDPR Programme.

a) The model anchored the overall responsibility with the head of Personal Banking and the group COO.

b) A steering committee (the "GDPR SteerCo") was established to make all final decisions for the GDPR Programme.

During the course of 2016, the approach of the GDPR Programme in Danske Bank was taking shape. The approach to building the GDPR Programme was divided into two main tracks which were performed in parallel:

a) Preparing an overview, i.e. a mapping, of the business and internal processes across the Danske Bank group where personal data was processed with an intention to achieve visibility about the personal data processed and identify areas of potential non-compliance.

b) Identifying the GDPR requirements and work streams needed for the Danske Bank group, with an intention to assess the inherent risks.

The Programme initiated a thorough analysis to identify an approach that could provide solid documentation and a foundation to become as compliant as possible by 25 May 2018.

Due to the large number of IT-systems and the high complexity and inter-connectedness between the systems, it was not possible to build retention and deletion functionality in all systems at the same time. Therefore, the requirements on retention and deletion were handled in a phase-based approach, that unfortunately could not be finalized by May 2018. The first phase concerned central systems.

It was pursued whether external supplier solutions could help solve the tasks. Many solutions claiming that they would solve GDPR were rejected as the majority of these took a Bottom-Up approach identifying data as only being present in IT-systems, hence focusing on IT-systems. It became clear to the Programme that the GDPR scope was much bigger than that because compliance with the GDPR also had to be ensured outside IT-systems.

The concept of a Top-Down approach, focusing on business processes, was becoming the only possible way to possibly cover all GDPR requirements.

January - April 2017

Danske Bank initiated the mapping of its business processes to identify where personal data was processed.

GDPR SteerCo approved the use of a process mapping solution provided by an external vendor for Danske Bank Group.

Mapping of processes

A business process mapping was necessary in order to create an initial overview. Business areas in the Danske Bank Group were asked to describe the various processing activities and to assess the level of compliance with the then to-be requirements under the GDPR.

A Top-Down approach, where the overall processes were mapped, was chosen as an efficient and manageable option compared to a Bottom-Up approach, which focuses on IT-systems. The Top-Down approach documents business processes in business units, including data and systems used in the business processes. It reflects a logical overview of the mapped processes but does not show the physical data flows.

A Top-Down approach was assumed to be the right method compared to Bottom-Up given the complexity of Danske Bank and the limited time available.

By mapping business processes, the task was to identify where personal data was processed and through this identification to document areas of compliance, and potential non-compliance, with the GDPR.

Before applying the approach to the whole group, it was decided to launch a pilot with Personal Banking. This area was chosen because nearly all of its business processes involve personal data. If the expected result was achieved from this pilot, process mapping for the entire Danske Bank Group was next step.

The pilot with Personal Banking proved to be successful and a solid and documented foundation for launching solution projects, as further described below, in the time period from May 2017 - May 2018.

The overall approach in relation to the mapping of processes was then divided into two main focus areas:

a) Business Units: Primary business data processing, in all market areas, as structured data. This accounted for ~80% of all personal data processing as assessed by the GDPR Programme.

b) Other data processing: Such as ad hoc reporting, test environments, analysis environments, stand-alone systems, internal non-customer-faced data processing, unstructured personal data in local drives, shared drives, SharePoint sites etc. This accounted for ~20% of all personal data processing as assessed by the GDPR Programme.

The group-wide data mapping approach is described in **Exhibit 1**.

Retention and deletion of personal data
While working on the parts of the GDPR Programme that relates to IT-systems, Danske Bank learned of the challenges with retention and deletion of personal data.

Work was undertaken to deal with these challenges as part of the Programme.

May 2017 - May 2018
The GDPR Programme established a process mapping workforce allocating around 20 employees in different teams to conduct workshops with all business units in all countries. Around 3,500 business processes were mapped, and more than 15,000 hours were spent on this exercise.

An exercise was initiated to identify the capabilities that a company must be able to demonstrate based on the GDPR requirements.

As a result of the gap analysis and identified capabilities, seven high-level actions defined as work streams were introduced, cf. **Exhibit 2**:

(i) Customer facing documents

(ii) Customer Insight & Support

(iii) Personal Data Clean up (Retention and Deletion)

(iv) Local IT Projects (Retention and Deletion)

(v) Organizational Implementation

(vi) Data Processor Agreements

(vii) Compliance & Governance

These seven work streams covered a total of approximately 32 overall solution projects. Each project included underlying deliverables for ensuring compliance within the area in scope of that project. These solution projects and deliverables included the following highlights from the projects:

a) The Retention and Deletion Project, which implemented retention rules and deletion functionalities in IT-systems processing personal data.

b) The Notification Project, where 3.6 million privacy notices were provided for customers, and privacy notices for new customers were drafted.

c) The Consent Project, where an overview of relevant consents ensuring GDPR compliance was created, and screening of all customer documents and contracts was carried out to ensure that there were no hidden consents.

d) The Marketing & Analytics Project aimed at ensuring that no GDPR non-compliant profiling was made.

e) The Insight Project, which aimed at ensuring that data subjects could get insight through an automated process providing the customer with a report of data from more than 300 IT-systems. This also covered data portability requirements.

f) The establishment of a GDPR support team consisting of 15 people, which was an independent, first line support team to handle customer requests related to processing of personal data.

g) The Unstructured Data Project, which implemented guidelines, processes and governance around deletion of unstructured data in emails, excel sheets, etc.

h) The Training Project, which established mandatory GDPR training for more than 20,000 employees across the Danske Bank Group with dedicated training for specialized functions.

i) A large awareness campaign was launched in March 2018 to ensure knowledge and awareness about GDPR, particularly on key principles of GDPR, clean-up guidelines, data breach reporting, how to ensure data subjects' rights etc. The campaign has been repeated in 2019 and 2020.

j) The drafting of directives, instructions and Standard Operating Procedures, including review of existing directives, instructions and Standard Operating Procedures.

k) The project on data processing agreements, which included review of more than 5,000 contracts to identify contracts subject to change due to GDPR requirements. A GDPR addendum was added to more than 350 contracts and signed copies were collected from vendors on the same.

l) The project on data protection impact assessments, which included implementation of a process for identification of necessary risk assessments, drafting of a DPIA-template and a Privacy by Design and Privacy by Default template.

m) The Data Breach Project, which included implementation of a process for handling personal data breaches to ensure proper assessment and documentation of all reported breaches within Danske Bank.

By 25 May 2018, most of the projects had achieved what was in scope for each project.

Some of the solution projects regarding retention and deletion were, however, too large and complex to reach their respective targets by 25 May 2018. The answer to question 6 contains a status for Retention and Deletion Project as of 25 May 2018 and the information about the continuation of this project from 25 May 2018 through 1 November 2020.

Exhibit 3 provides an overview of the high-level deliveries on the retention and deletion projects as of 30 November 2020.

1.3 Extent

As mentioned above, Danske Bank's work as part of the GDPR Programme on tasks regarding retention and deletion covered the whole Danske Bank Group, i.e. all business units, market areas, subsidiaries, and was accordingly very large.

Danske Bank therefore chose a phase-based approach to handle the work on retention and deletion in manageable portions. A one-off solution to ensure compliance with the GDPR was not possible due to the amount of resources it would take to execute this. Danske Bank had involved more than 250 employees in the GDPR Programme since May 2016, and it was not realistic nor efficient to allocate more employees.

1.4 Summary

As we have described above, there is no short and simple answer to the question "When and how did Danske Bank A/S discover the problem with the non-deletion of personal data?"

Retention and deletion of personal data was a part of Danske Bank's ordinary GDPR Programme, and the problems were discovered in the course of the Programme.

2 QUESTION (5): THE SCOPE OF DANSKE BANK A/S' OWN INVESTIGATION OF THE MATTER, INCLUDING WHETHER THE BANK INVESTIGATED ONLY A LIMITED PART OF ITS BUSINESS UNITS IN RELATION TO THE STORING OF PERSONAL DATA.

2.1 Our understanding of the question

This question presumes that an "investigation" of the matter has been performed.

As described above, the problem with retention and deletion of personal data in Danske Bank does not relate to an "incident", such as a data breach incident, which can be "investigated" in a delimited way, but rather to an IT-issue of a broader nature. The problem was therefore "investigated" in the course of the work on the IT-systems as part of the GDPR Programme.

The "investigation" concerned all business units within Danske Bank, see above.

In the following, we will give a brief description of the structure of Danske Bank's IT-systems, since in order to understand and describe the problem, one must understand the structure of Danske Bank's IT-systems.

2.2 Introduction

As mentioned, Danske Bank initiated the GDPR Programme in May 2016. The Programme aimed at making Danske Bank compliant with the GDPR by May 2018, including implementation of effective functionalities for retention and deletion in IT-systems. The work streams in the GDPR Programme is described in question 1 above.

The initial Programme timeline implied that by 25 May 2018 most - but not all - of the initiatives to ensure compliance with GDPR in terms of retention and deletion of personal data would be in place. Further, a potential stretch was anticipated for building Business-As-Usual activities on the delivered initiatives.

The Business-As-Usual activities were defined as a continued implementation of a governance framework in the Business Units and a focus on organizational implementation in order to maintain and enforce visibility and knowledge of GDPR, which would lead to business as usual.

2.3 Background information on IT-systems in Danske Bank

In order to understand Danske Bank's work on retention and deletion, it is necessary to explain the general set-up of IT-systems in Danske Bank.

Historically, all IT-systems were on the mainframe and had customer and account retention and deletion functionality implemented. When customers left the bank, customer information was deleted on the mainframe in accordance with retention rules, which were based on commercial needs and on legal requirements.

Until 2016 Danske Bank focused on retention and deletion of data in systems on the mainframe, and had only a limited focus on deletion of data in local systems.

As all systems are dependent on the customer being registered in the customer system, which is a central system as further described below, no processing of personal data in other systems can take place without having personal data about the customer in the customer system.

As of 1 November 2020, Danske Bank has systems which are central systems on a mainframe, and systems which are local systems outside the mainframe. These systems cover all business units within Danske Bank.

The IT setup is shown in **Exhibit 4**.

The central systems support the processes for transactions, credits, cards, loans, investments, accounts and the central customer database ("kernekundesystem/KKS").

Accordingly, the central systems contain the most (personal) data both in terms of the amount of data and number of customers. However, (personal) data about customers may also be stored solely in a local system.

The local systems support specific services offered to customers, e.g. there is a local system for the Mobile Bank. In many cases, the local systems will be dependent on data processed in one or more central systems. Said data in the central systems will hence to a large degree have a nature of "master data".

There are two types of local systems:

a) Local systems which receive personal data from the central systems and sends personal data back to the central systems

b) Local systems (de-central) which are entirely separated from the central systems.

According to Danske Bank's governance setup, owners of IT-systems are obligated to:

a) Define retention periods for the personal data

b) Document the Retention Rules in the Retention Rule Tool

c) Implement the appropriate clean up procedures

d) Design and implement controls for making sure local systems are documented and retention rules are assigned (Business Risk & Control department)

2.3.1 Regarding a) local systems dependant on the central systems

Personal data is stored in a central system when the data subject becomes a customer in Danske Bank, and in a local system used for a further, specific service or product offered to the customer. Given the dependence by the local system of personal data in the central system, personal data will be stored in the central system as long as the local system processes personal data about the customer.

When a customer leaves a Danske Bank service or product supported by a local system, the local system will inform the central system that the data subject is no longer active in that local system.

This triggers the central system to check whether the data subject is still active in another local system, which is dependent on data from the central system. If not, the personal data in the central system about the data subject will then be eligible for deletion in accordance with the retention rules for the central system.

In other words, and as mentioned above, the use of a central system as a provider of "master data" to local systems means that the local systems in practice also govern when the "master data" is deemed to no longer be necessary for a business process. The fact that the central system does not need the data for its own purposes does not necessarily mean that the data is eligible for deletion in accordance with the retention rules, since the needs of local systems may warrant the continued retention in the central system.

Personal data in the local systems will be deleted pursuant to the specific retention rules for each local system.

See item 5.4 for more information about the relationship between these local systems and central systems.

2.3.2 Regarding b) local (de-central) systems which are entirely separated from the central systems

These local systems are not dependent on personal data from other systems. Personal data will be retained pursuant to the retention rules for each local system, and does not influence the retention period in central systems.

See item 5.6 for more information about the remaining work on retention and deletion in local systems.

2.4 **Summary**

In the above, we have provided a brief description of the structure of Danske Bank's IT-systems. As one can see, Danske Bank's IT-systems are very large, inter-dependent and have a complex structure.

Danske Bank learned of the challenges with retention and deletion of personal data while it was working on the parts of the GDPR Programme that relates to the IT-systems.

The IT-systems in scope for the Programme cover all business units within Danske Bank.

3 QUESTION (2): WHAT IS THE REASON BEHIND THE NON-DELETION OF PERSONAL DATA?
QUESTION (3): WHAT IS THE PROBLEM?

3.1 Our understanding of the question

Given the nature of the issue, we find that the reason behind the non-deletion of the personal data is the same as the problem causing the issue with non-deletion of personal data. In order to provide the Data Protection Agency with a clear and understandable answer, and to avoid overlaps, we have decided to combine questions 2 and 3.

The answers to these questions are closely related to the description of Danske Bank's GDPR Programme and the challenges in finalising the parts of the Programme relating to retention and deletion by 25 May 2018, and which are described above.

For this reason, these questions are to a large degree answered in the above parts of this letter. In short, the reason as well as the problem are that some of the solution projects regarding retention and deletion were too large and complex to reach their respective targets on time.

The answer to question 6 contains a status for Retention and Deletion Project as of 25 May 2018 and information about the continuation of this project from 25 May 2018 through 1 November 2020. Further, in the answers to question 6, we explain how Danske Bank has been and will continue to be working with the tasks that were outstanding as of 25 May 2018.

In order to avoid overlaps, we will therefore not provide further comments in this part of the letter.

4 QUESTION (4): THE EXTENT OF THE PROBLEM, INCLUDING THE AMOUNT AND CATEGORY OF PERSONAL DATA, AND WHETHER THE PROBLEM IS ISOLATED TO DENMARK.

4.1 Amount and category of personal data

Danske Bank has retained all types of personal data, including ordinary (article 6) and special categories (article 9) of personal data, for longer than necessary.

The personal data typically relates to:

a) Customer ID

b) Contact information

c) National identification number

d) Other core data

e) Product data

f) Account data

g) Loan data

h) Credit Card data

i) Transaction data

4.2 Extent of the problem

In broad terms, the personal data on customers which Danske Bank retains as of 1 November 2020 can be divided into three categories:

a) Personal data in systems which were made subject to the necessary retention/deletion rules prior to February 2019. The deletion of this data was, however, put on hold in February 2019, see item 6. Accordingly, data covered by this point a) was duly deleted on a regular basis prior to February 2019, and the deletion jobs will be resumed once possible.

   Note that since the deletion was put on hold in February 2019, Danske Bank has continuously reviewed its data systems and types to ensure its retention is necessary and proportionate, and re-instituted GDPR clean-up processes where possible. Danske Bank therefore finds that it complies with its obligations in regards to data covered by this point a).

b) Personal data in systems which were not made subject to the intended retention/deletion rules prior to February 2019. From February 2019 onwards deletion of this data was put on hold, see item 6, but Danske Bank has during this time period developed and implemented the necessary retention/deletion rules that as of 1 November 2020 enables Danske Bank to activate the deletion jobs once possible.

   Note that since the deletion was put on hold in February 2019, Danske Bank has continuously reviewed its data systems and types to ensure its retention is necessary and proportionate, and instituted GDPR clean-up processes where possible. Danske Bank therefore finds that as of 1 November 2020 it complies with its obligations in regards to data covered by this point b).

c) Personal data which is covered by the remaining work on retention and deletion, see item 5.6. These are the areas/projects that contain the non-compliance regarding retention and deletion. It is not possible to estimate the amount of personal data that should have been deleted, including to what extent the personal data could have been deleted, see item 6.

4.3 Is the problem isolated to Denmark?

The problem is not isolated to Denmark. Within the legal entity Danske Bank A/S, which is headquartered in Denmark, there are legal branches established in the following EU/EEA countries: Sweden, Norway, Finland, Latvia, Lithuania, Poland, Germany, Ireland and United Kingdom. Danske Bank previously had a branch in Estonia, which has now been liquidated.

Each of the branches will have customers that are residents of the pertinent countries.

5 QUESTION (6): WHAT HAS DANSKE BANK A/S DONE – AND WHAT DOES THE BANK INTEND TO DO – TO PUT THE MATTER RIGHT?

5.1 Our understanding of the question

As described above, the matter is closely related to Danske Bank's GDPR Programme. The remediation of the problem with retention and deletion of personal data has been and will continue to be handled as part of the Programme.

In the following, we therefore provide a description of the part of the GDPR Programme performed after 25 May 2018 related to retention and deletion of personal data.

5.2 Introduction

This question will be answered in four parts:

(i) Status on completed work on retention and deletion by 25 May 2018

(ii) Timeline for Danske Bank's work on retention and deletion from 25 May 2018 through 1 November 2020

(iii) Status on completed work on retention and deletion by 1 November 2020

(iv) Danske Bank's plans for completing the remaining work on retention and deletion

In **Exhibit 5** we provide illustrations and descriptions of the principle of retention and deletion in central systems and local systems.

5.3 (i) Status on completed work on retention and deletion by 25 May 2018

Danske Bank had implemented the following deliveries by 25 May 2018:

a) Applied retention rules to the Central customer systems in Danske Bank (212 of 251 retention rules). "Retention rules" means criteria for retention of personal data - once there is no longer a justification for retention in the rule, the personal data is eligible for deletion. The numbers show how many retention rules which were actually implemented out of how many retention rules that should have been implemented by 25 May 2018. It is noted that the remaining retention rules in central systems were implemented as per Q4 2019 as described further below.

b) Applied retention rules to local systems related to Future Financing, Cards, Payments Solutions and other local systems

c) Clean-up/deletion of majority of HR data, including implementation of retention and deletion rules

d) Clean-up/deletion in customer and product data in some local IT-systems

e) Customer Data Retention Rule Tool version 1 in place by mid June 2018, but very close to being completed by May 2018. This system is used to keep track of the retention rules applied throughout IT-systems in Danske Bank.

5.4 (ii) Timeline for Danske Bank's work on retention and deletion from 25 May 2018 through 1 November 2020

June 2018 - March 2019

Danske Bank continued the work after the GDPR entered into force.

The next phase of the Retention and Deletion Project was launched with a focus on local retention, physical archives and Data Warehouse.

New guidelines from the Danish Data Protection Agency also required new solution projects to be initiated, for example on encryption for transmission of confidential and sensitive personal data over the internet.

In addition, the GDPR Programme changed its focus, considering that staying compliant with GDPR requirements also presumed a significant, ongoing effort, and transition from Programme to Business-As-Usual was planned.

A master governance document was introduced outlining GDPR responsibilities for the owners in Business Units. The document connected the identified GDPR requirements to areas of responsibility for all units.

Governance was, as mentioned, anchored in the business processes. It was recognized that the processes mapped in the early phase of the Programme were not mapped to a degree where the business could take over. This led to a review of all processes already mapped and identification of new processes that had to be mapped.

During the fall of 2018, Danske Bank also realised that a separate project on voice recordings, which included implementation of retention and deletion functionality, was needed to ensure GDPR compliance.

April - October 2019

During this time period, Danske Bank established risk assessment procedures and controls for IT-system owners.

Consolidation of existing Data Warehouses had started, and it was decided to focus on clean-up and anonymization principles for the future consolidated Data Warehouse.

Work was also progressing within the streams on local retention, physical archives and voice recordings.

Further, the remaining clean-up for local IT projects in Wealth Management, Asset Finance and HR systems was completed in Q2 2019.

On data governance, a Group Data Office was established in August 2019 to co-ordinate the creation of a stronger data management foundation with the business areas of the Bank.

This was, and currently is, focused on a series of integrated workstreams that together implement this new foundation:

a) Group Data Strategy. The agreement of common ways of working and focus for addressing data challenges and ambitions of the Bank.

b) Data Awareness. The Group-wide communication and training initiatives aimed at building up data culture and common ways of working.

c) Group Data Management Instruction. The instruction that defines principles for data ownership, data quality and data architecture in the Bank.

d) Data Governance. The service that records data owner, data steward, business glossary, definitions and standards for data.

e) Data Architecture. The service that records the flow of data across business areas and IT systems.

f) Data Quality. The services that standardises the measurement of data quality, centralises the reporting of data quality results, and centralises the recording and management of data issues.

The Data Protection Compliance team identified the lack of a group-wide information records management and limited data governance framework and raised observations in 2018 (consolidated into a single observation in October 2019) that highlighted the associated risks of being GDPR non-compliant. This led to the establishment of the Group Data Office, which is currently working on developing a Group Information Records Management function and a framework that will help ensure efficient and systemic control of data and resolve identified issues on data quality and retention and deletion. The operating model design is due to be completed by end 2020, with implementation of the functional set-up commencing in 2021. See below, item 5.6, for more information.

November - December 2019

The GDPR Programme was instructed to focus on transition to Business-As-Usual. However, a limited number of projects continued into 2020.

The main continued project concerned implementation of retention and deletion functionality.

The work on central retention was completed in Q4 2019. Danske Bank set up a central customer data retention process, also known as "Customer Clean-up", which is also described and illustrated in **Exhibit 5**, page 1 and 2.

The process can be explained as:

a) Clean-up of customers is performed automatically every month

b) The setup consists of +250 retention rules, also referred to as clean-up members

c) Each retention rule is the definition of a legitimate business reason to keep customers

d) Each retention rule uses an SQL to select a list of customer IDs from a Product System's local table(s)

e) The aggregation of all locally generated lists of customer IDs make up the Central Retention Targets

f) Customer IDs no longer needed by local systems are deletion candidates.

Danske Bank continued to implement retention and deletion functionality in local systems, Data Warehouse and voice recording systems, but the work was not yet completed.

Deletion principles were set up for physical archives.

Activities to clean-up unstructured data throughout the Group was completed in Q4 2019.

The last project to be started and funded by the GDPR Programme was scoped around the use of personal data in the test environments. Assessments of current situation with test environments were carried out and existing business procedures and guidelines were updated. Further, Danske Bank analysed the need for supporting tools for masking, scanning and automated control. The aim was to ensure compliance by using anonymized data in our test environments and timely data clean-up if production data is needed for problem testing.

January - November 2020
As the Programme was ramping down, all development areas in IT were instructed to continue their development utilizing the dedicated budget for 2020.

The project on physical archives was completed in Q1 2020. The project reviewed and updated retention rules for documents handled by external partners and delivered GDPR guidelines for clean-up in internal local physical archives. The guidelines are a high-level instruction on handling of physical archives, how to establish retention rules and how to conduct clean-up.

During this time period, Danske Bank continued its work with implementation of retention and deletion functionality in local systems, Data Warehouse, test environments and voice recording systems.

The Programme continued with a reduced number of employees with a focus on transition to Business-As-Usual.

5.5 (iii) Status on completed work on retention and deletion by 1 November 2020

An overview of projects in the GDPR Programme which include retention and deletion activities is enclosed as **Exhibit 6**. This exhibit shows the status as of 1 November 2020 and key objectives for each project.

The following projects in Danske Bank have been completed by 1 November 2020:

a) Customer Data central retention (completed Q4 2019)

b) HR (completed Q2 2019)

c) Wealth Management (completed Q2 2019)

d) Unstructured Data (completed Q4 2019)

e) Physical Archives (completed Q1 2020)

Exhibit 3 shows a more detailed overview of the high-level deliveries in these retention and erasure projects since 2016.

5.6 (iv) Danske Bank's plans for completing the remaining work on retention and deletion

Exhibit 6 shows the non-completed projects. These are the areas/projects that contain the non-compliance regarding retention and deletion.

The projects which have not yet implemented retention and deletion rules/functionality are:

a) Customer Data local retention (expected to complete Q4 2021)
   - Status: Danske Bank is currently mapping local systems to determine (i) which systems do currently not have retention/deletion rules implemented, and (ii) making a plan with the IT-system owners for implementation of retention/deletion rules.

b) Data Warehouse (expected to complete Q4 2021)
   - Status: Anonymization tools have been implemented for some parts of the data in the Data Warehouse. Danske Bank is currently working on implementing anonymization tools on the remaining part of the data in the Data Warehouse.

c) Test environments (expected to complete Q2 2021)
   - Status: Danske Bank has been using production data in test environments. The purpose of this use of production data is to allow testing and validation of business solutions prior to implementation into the production environment. This ensures proper quality of the implemented solutions. It is sometimes the case that there is no other way to properly test systems presently, but best practice is to minimise when this occurs. Danske Bank is working on establishing automated clean-up procedures, and an improved central tool for masking of data. The plan is to reconsider and optimize the current way of masking data, and establish ownership for data, controls, approvals, and access control. Further, internal assessments on the level of compliance regarding test data, governance, and controls in test environments is being conducted. In this context, Danske Bank has identified other associated areas of non-compliance with the GDPR than retention and deletion.

d) Voice recordings (expected to complete Q1 2021)
   - Status: Danske Bank has bought an additional vendor solution on top of the existing voice recording system which enables automatic deletion. The solution has been successfully installed in Q4 2020. Retention rules are in the pipeline to be set up in the system to enable deletion which will complete the project.

"Expected to complete" means that the functionality is implemented in the relevant system(s) and is ready for activation.

As mentioned above, item 5.4, in 2018 the Data Protection Compliance team identified the lack of a group-wide information records management and limited data governance framework and raised an observation that highlighted the associated risks of being GDPR non-compliant.

This led to the establishment of the Group Data Office, which is currently working on developing a Group Information Records Management function and a framework that will help ensure efficient and systemic control of data and resolve identified issues on data quality and retention and deletion. The operating model design is due to be completed by end 2020, with implementation of the functional set-up commencing in 2021.

The Group Data Office, led by the Chief Data Officer, shall amongst others be

- accountable for defining and maintaining the Data Strategy that sets the direction for how data is managed and viewed.

- responsible for ensuring that any individuals that are assigned ownership or responsibilities relating to the Data Management Governance Framework should be adequately trained and supported to ensure they can fulfil their roles effectively.

- responsible for monitoring the business compliance to the Data Management Framework standards and Data Management Instruction.

- accountable for defining and maintaining a process for identifying Business Terms and the underlying data held within the defined Data Class Model.

- responsible for ensuring the implementation of an IT system for maintaining a Business Term and its underlying data attributes, and for setting minimum requirements for the information, which must be available in a central Information Governance Tool.

- accountable for setting the guidelines for establishing the quality KPI targets and thresholds and reporting for each Critical Data Element.

- responsible for facilitating reporting on issue status.

5.7 Summary

In the answer to this question, we have described the part of the GDPR implementation programme performed or to be performed after 25 May 2018 related to retention and deletion of personal data.

As it appears in item 5.6, Danske Bank has almost completed the tasks that were outstanding as of 25 May 2018 and expects to be able to complete the tasks that are outstanding as of 1 November 2020.

Further, Danske Bank has established a Group Data Office, which shall develop a Group Information Records Management function and a framework that will help ensure efficient and systemic control of data and resolve identified issues on data quality and retention and deletion.

6 DATA PRESERVATION IN RELATION TO THE NON-RESIDENT PORTFOLIO INVESTIGATION

Danske Bank remains in dialogue with various authorities regarding the terminated non-resident portfolio at the Bank's Estonian branch, which was active between 2007 and 2015. This includes criminal and regulatory investigations by authorities in Estonia, Denmark, France and the United States (the "Investigations").

Further, Danske Bank is involved in civil litigation in Denmark and the United States pertaining to the Estonia matter (the "Litigations").

As part of the Investigations and Litigations, Danske Bank has been and continues to be subject to legal obligations and further has legitimate interests to preserve personal data in structured and unstructured form.

Danske Bank has taken steps to preserve data necessary and proportionate to the Investigations and Litigations in order to pursue a range of critical interests, including ensuring it can thoroughly investigate the allegations, cooperate with regulatory bodies and enforcement agencies, and adequately defend potential civil and criminal actions.

If preservation steps had not been taken, there would have been a substantial material risk that evidence that was potentially relevant would be irretrievably destroyed. Some of the consequences Danske Bank could

face if potentially relevant evidence is not preserved, include, but are not limited to, (i) the inability to cooperate fully with investigating authorities, (ii) potential criminal prosecution owing to the destruction of evidence, and/or (iii) the inability to adequately defend civil and criminal actions against Danske Bank and its current and former employees.

The preservation has not affected Danske Bank's work on technical solutions etc. to enable retention and deletion as required under the GDPR, but it has affected the timing of the implementation and activation of said solutions for certain systems.

Danske Bank continues to review its data systems and types to ensure its retention is necessary and proportionate. Over this period of time, due to the progress of the investigation and to ensure ongoing compliance with GDPR obligations, Danske Bank has revisited the steps taken to preserve data and re-instituted GDPR clean-up processes where possible to ensure that the continued preservation is necessary and proportionate.

- 0 -

We propose to have a meeting between the Agency and Danske Bank, including Plesner as Danske Bank's legal counsel, where Danske Bank's work on retention and deletion can be further elaborated.

Yours sincerely

[Sent electronically and therefore not signed]
Bo Svejstrup

7 EXHIBITS

1) Description of the group-wide solution projects.

2) Overview of the work streams.

3) Danske Bank Group's high-level deliveries in Erasure & Retention Projects Since 2016

4) Illustration of the IT set-up.

5) Illustrations and descriptions of the principle of retention and deletion in central systems and local systems.

6) Overview of completed and non-completed projects which include retention and deletion activities.

Danske Bank

EXHIBIT 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.

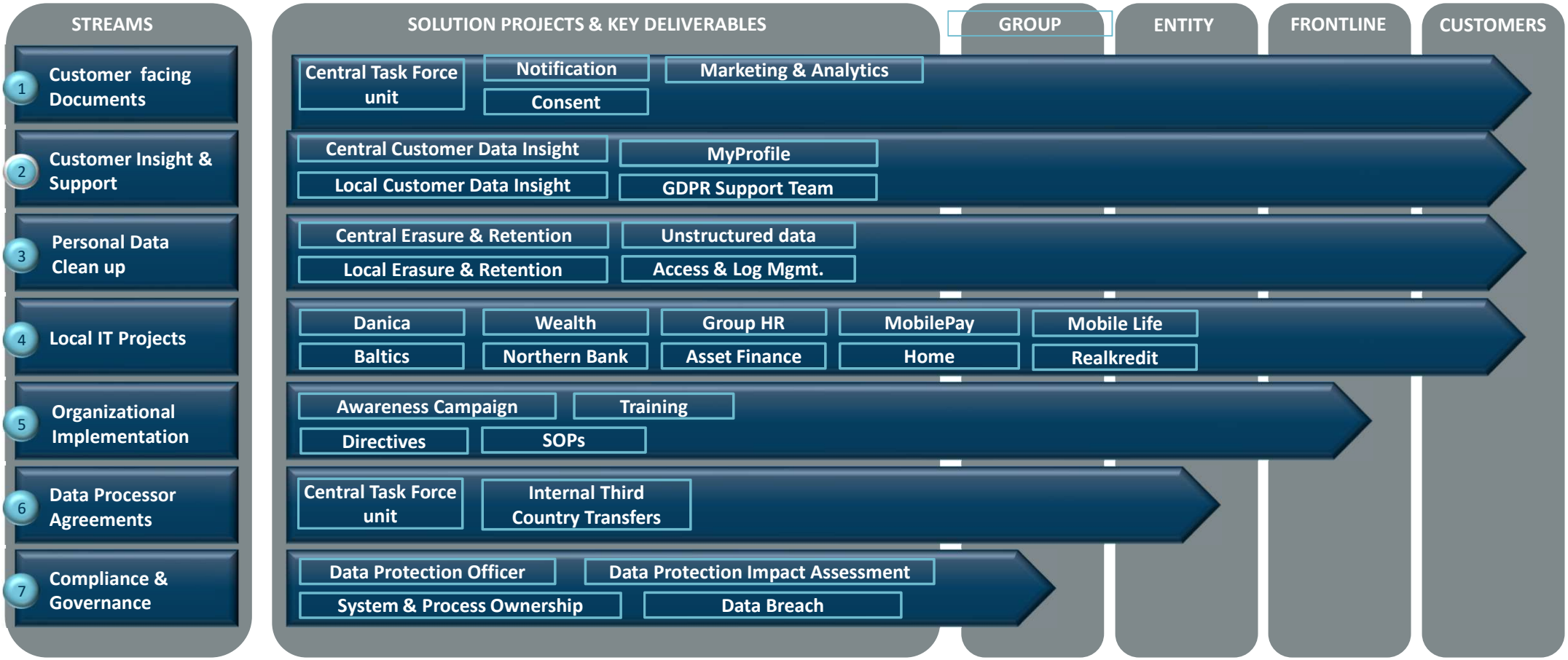
These will also be monitored by the GDPR Programme to ensure that the entire Group reaches the desired compliance levels.

Created: 16.12.2020

Danske Bank

EXHIBIT 2

Overview of Work Streams and Solution Projects



Created: 27.11.2020

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

EXHIBIT 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

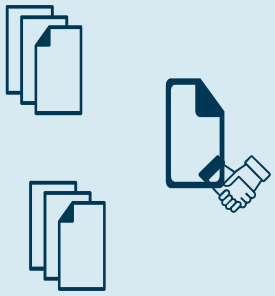
Danske Bank

EXHIBIT 4

High level overview – data and systems

Unstructured data*
Manual clean-up, assessed by employees

Physical data

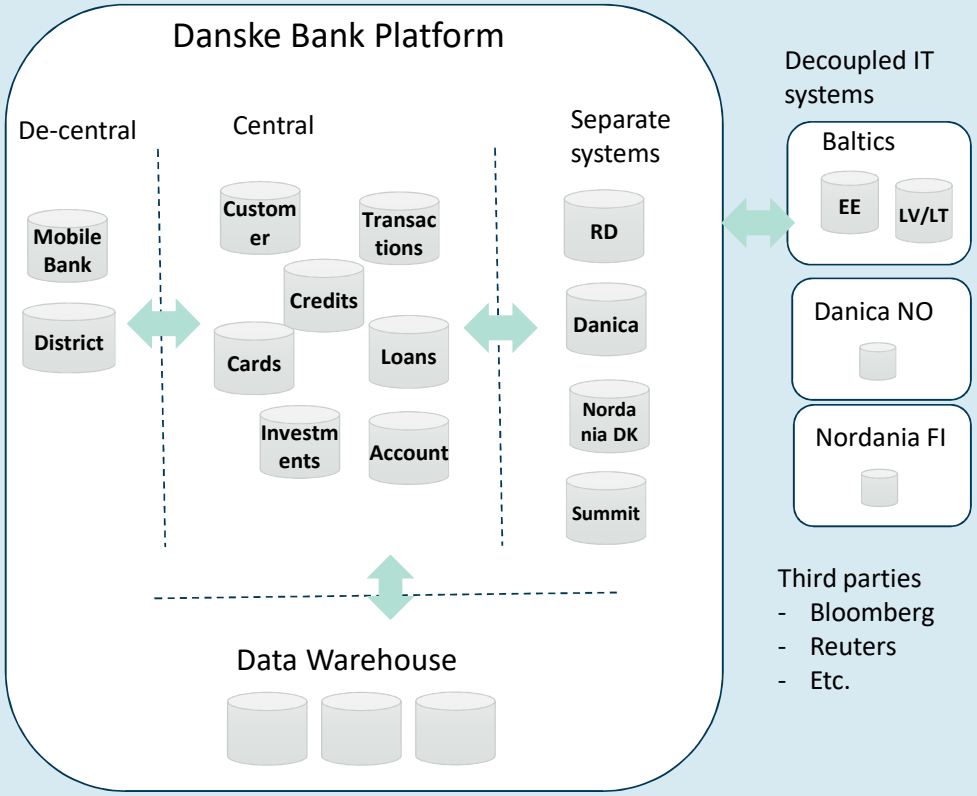


Examples: Signed agreements, print-out, microfiche

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

EXHIBIT 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

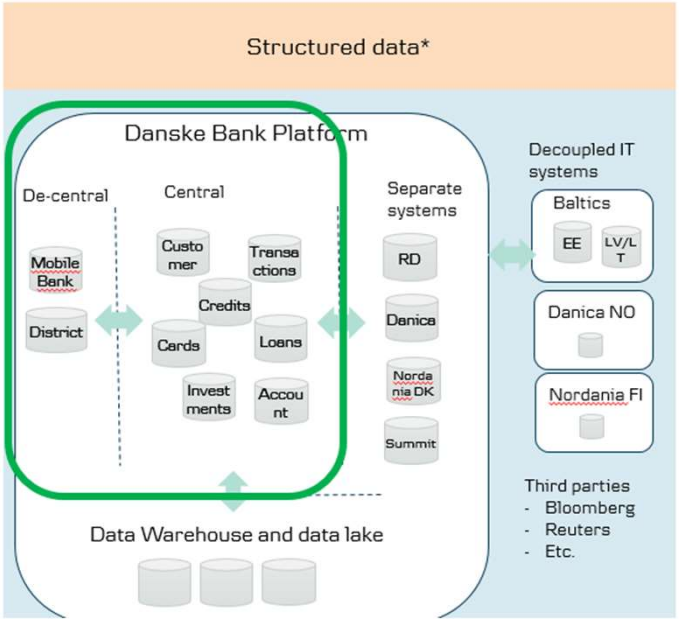
Central retention

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

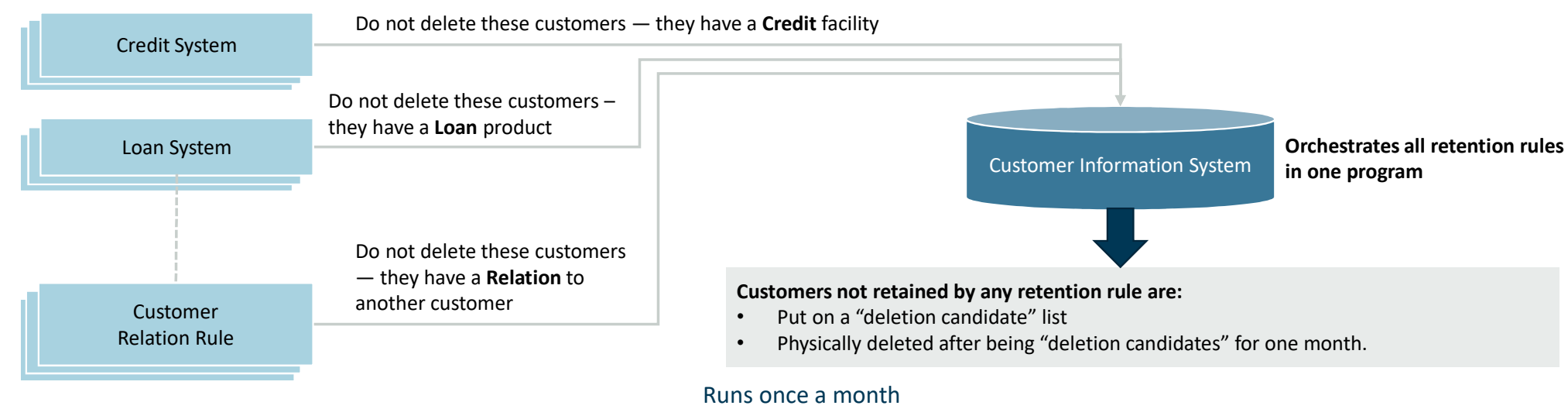
Danske Bank

EXHIBIT 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)



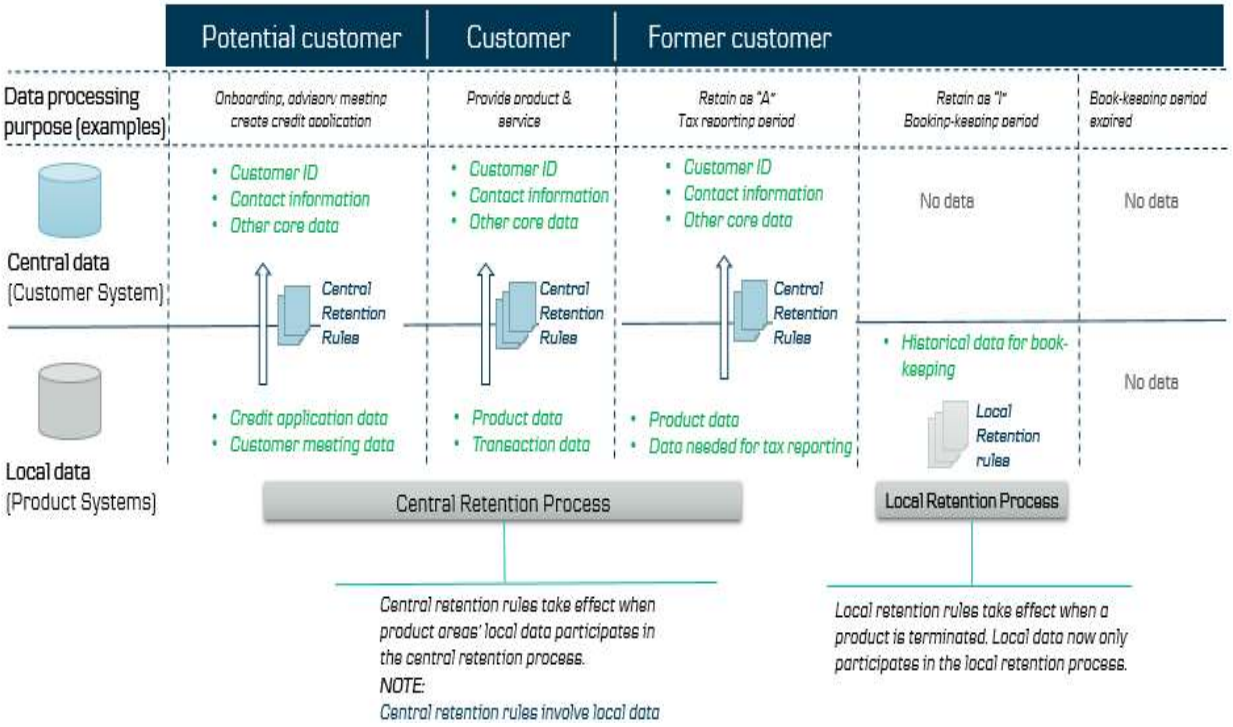
PUB/SUB setup implemented during 2019, and used by some areas for local retention

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

EXHIBIT 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

EXHIBIT 5

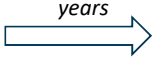
Deletion by default – automatic clean-up – customers - example

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

EXHIBIT 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