Instructions for handling of Personal Data in SEB in Norway

Approved by the Norwegian Extended Management 27. May 2019

1. Introduction

1.1. Background

This Manual is adopted by SEB Norway (SEB) in the light of the implementation of the EU General Data Protection Regulation (GDPR) into Norwegian law (Personopplysningsloven) and to ensure that SEB comply with the relevant legal obligations. The instruction must be supplemented by more detailed work instructions and guidelines set by the relevant units within SEB.

The instruction will form the basic principles for SEB's collection of personal data as well as record keeping, retention, deletion and clean up routines. It will also cover procedures for our interaction with clients and others when it comes to handling personal data.

Personal data is data or information about an identifiable individual. To require that the person is "identifiable" doesn't mean that the individual has to be named or that we have to know who the person is; it means that given the information – the person can be uniquely identified.

GDPR and similar regulations are in place to protect each individual's right to privacy. This is not the same as confidentiality, but both privacy and confidentiality is closely linked together. Information may be private while not being confidential, and information may certainly be confidential without being private or even personal. One of the intentions of GDPR is also to give customers and employees greater control over their data, including the ability to export it, withdraw consent and request access to it.

Confidential information is restricted in the sense that there are only a limited number of persons that should have access to the information and only for given purposes (need to know). Private information, on the other hand, may be something that is public information, but that the person to whom it relates, doesn't want to share or for everyone to be aware of.

Privacy regulations generally apply to all organisations, but SEB, as a financial services organisation, are already and to a large extent handling personal data in line with the basic GDPR-principles due to the banking secrecy requirements and other regulations that require SEB to collect and store significant amounts of personal data, for significant amounts of time.

All personal data processing within SEB shall follow the following principles:

1. Personal Data shall only be processed on a legitimate basis
2. Processing of Personal Data shall be transparent to the data subject
3. No processing of Personal Data shall be undertaken other than for the stated purpose(s) for which it was obtained
4. Personal data, like all other data processed by SEB, shall be reviewed routinely to ensure that such is accurate and reliable, and where no longer required to be retained, shall be archived and deleted.
5. Personal Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Additionally, data subjects have the right to:

1. Be informed of how SEB's will process data about the individual
2. Obtain a transcript about the individual held by SEB
3. Inform SEB of information in SEB's records that is incorrect and to have it rectified; and
4. Be "forgotten".

GDPR has also set specific requirements on SEB which cannot be directly linked to a specific data subject, but are general obligations in relation to complying with the regulation, such as:

1. The duty to notify the relevant authorities where SEB knows or has reason to believe that the personal data has been stolen or security measures designed to protect the personal data have been breached, and in some instances also notify the data subject whose personal data have (potentially) been affected
2. To assess processing which may constitute high risk for the natural person(s) and in relevant instances abstain from engaging in such processing
3. To enter into appropriate agreements to govern the relationship between SEB and any 3rd party who acts as a processor for data of which SEB is a controller, and
4. To enter into appropriate agreements for the transfer of Personal Data in scope of GDPR to a 3rd country.

1.2. Exception Approvals

The contents of this Manual have been approved by Norway Management Group.

Deviations from the Instructions and Procedures set out herein shall be permitted only on a case-by-case basis and where approved by the Head of SEB Norway after consultation with the Local Data Privacy Committee. A record of such approved deviations shall be placed upon the relevant transaction or administrative file.

1.3. Annual Reviews

The Head of SEB Norway should review the contents of this Manual on, at least on a bi-annual basis unless regulatory or organisational changes require an earlier review, to ensure that it reflects practice in the office and in the market generally. To the extent that it is required to be updated following such review, changes should be proposed to data protection responsible persons. Further details should be outlined in the local GDPR governance instruction.

1.4. Responsibility

Each member of staff shall ensure that he or she is fully familiar with the contents of this Manual. Anyone who is unclear about the mechanism or reason for any procedure should seek immediate clarification from their manager or the Local Data Privacy Officer (DPO) or Local Data Privacy Responsible (DPR).

Failure to comply with any aspect of the policies and procedures set out in this manual may result in disciplinary action being taken against the relevant individual.

2. Governance

The Head of SEB Norway shall implement[1] a governance structure in line with the "Instruction for Confidentiality and Personal data Protection in the SEB Group", which shall set the overall responsibilities for the compliance with GDPR.

3. Data Privacy Policy

3.1. Responsibility

SEB shall take appropriate measures to provide clients with information about the purposes of the processing of personal data as well as the legal basis for this and how personal data is processed within the bank. It is required that such information should be given in a concise, transparent, intelligible and easily accessible form, thus SEB shall issue and keep updated information about SEBs processing of personal data. It is the responsibility of the Local Data Privacy Committee to ensure that a Privacy Policy is adopted and implemented in SEB[2]. The Privacy Policy should be reviewed by the Local Data Privacy Committee, on, at least, a bi-annual basis unless regulatory or organisational changes require an earlier review.

The content off this policy shall be in line with the requirement set in GDPR art 13 and 14.

3.2. General information to clients

In addition to the general information about Privacy Data as referred to in section 3.1 each unit shall ensure that any new client is duly informed about the collection and processing of personal data in i.e. any electronic or paper based client on-boarding form or other forms or agreements where SEB require the client to register personal data. This may be done through a short notice and an electronic link to the relevant page on seb.no where the complete privacy policy is to be found.

It is also important that any employee that prepare any contractual agreements, incl. templates or standard terms and conditions, makes an assessment of the need for any information about or references to the Data Privacy Policy in such documents.
A short version of the language to be included in such documents and forms is attached to the Manual in Schedule 1.

4. Collection and retention of personal data and information to clients

4.1. Responsibility

Process owners (or as the case may be, the product owner or a manager of a business unit) are responsible to specify records to be created, processed and retained from such processing. It is important that these records are set up in a way that makes them easily accessible for the purpose of later correction and deletion of data which are subject to such requirements.

---

[1] Instruction for Personal Data Protection Governance structure in SEB Norway
[2] Generelle regler om behandling av personopplysninger (kundeopplysninger) i Skandinaviska Enskilda Banken AB (publ) Oslofilialen og SEB Kort Bank AB Oslofilialen

Employees whose job description includes carrying out the process are responsible to adhere to the process and in doing so create such records that are required to be kept. Where information is created in a process which has no process owner, or in the course of activities which are not characterised as a process; employees are responsible to create records required by this instruction to the extent they engage in activities generating data to be recorded.

With regard to meetings and other communication through non-recorded media, to the extent such are in scope of the record keeping requirements, the chairman or functional equivalent of such meetings should be responsible to create relevant records, unless such responsibility has been delegated to another person.

Employees should always bear in mind that certain legal requirements and SEB group wide or local instructions and procedures requires both collection and retention of personal data and that adherence to such rules and regulations most likely will entail compliance with the GDPR rules. Thus all employees shall always, when implementing new routines and processes, assess whether or not the actual need is already covered by existing routines or procedures.

It is the overall responsibility for each Client Executive to ensure that any personal data collected in relation to a client is handled in line with this Manual. The same applies for the local SEB HR function in relation to SEB employees, former employees as well as recruits applying for a position within SEB.

4.2. Record keeping – where and how to store

Record keeping and retention is both a regulatory requirement as well an important factor in reducing operational risk, protecting the bank and in serving our clients.

Record keeping (and retention and clean up) procedures shall be in place with the purpose of:

- supporting policy formulation and managerial decision-making;
- meeting legislative, regulatory or contractual requirements;
- protection of the rights and interests of employees, clients and involved parties of SEB;
- improving performance of business activities in SEB;
- protecting and supporting the bank when involved in litigation, including improving management of risks associated with insufficient audit trails of SEB activities;
- supporting consistency, continuity and productivity in management and administration;
- documenting SEB activities, development and achievements;
- supporting research and development activities, and
- supporting requirement setting towards external suppliers and partners.

Please refer to SEB's Information Security and general Security Policies and Instructions regarding security issues.

4.3. Retention method

4.3.1. Agreements

SEB has set different procedures for storing client agreements, i.e. Global Agreement System (GAS), local CRM-systems and for Procurements (i.e. for storing of data processing agreements etc). Thus such agreements shall only be retained in these systems and not in any local or private drives or files.

Neither this instruction, nor any SEB policy, does impose specific requirements to retain originals of any record. Where an original is not retained, a copy shall be retained in a format which accurately reflects and allows for accurate reproduction of the original. Note however that there can be specific regulatory requirements that require the retention of original documents, i.e. certificate of mortgages etc. If in doubt consult Legal or Local Group Compliance.

4.3.2.Media

All records shall be kept in a durable medium. A durable medium is such a medium which does not deteriorate with regard to the ability to retrieve, review or reproduce the record over time. The media may provide for the ability to alter or update the record, provided the adequate procedural or technical safe-guards are in place to ensure that such alterations or updates are also record kept.

Regardless of whether originals, copies or both are retained, such shall be retained in a space which protects the record from deterioration such as environmental harm – e.g. sunlight, heat, fire, water, moisture and other environmental harm.

4.3.3.Location

Records may be stored at SEB's premises or at other locations provided there are adequate arrangements in place to adhere with this instruction and other Group Policies and Instructions regarding inter alia security standards.

4.4. Accessibility

Records shall be maintained in a manner which enables such to be readily retrievable and accessible for the retention period. Readily shall be understood in the context of which the record may be required to be accessed and may range from near instantaneous access to being retrievable in a matter of a week or similar, under normal operating conditions and while processing a normal number of requests to retrieve records. Where a regulation provides specific guidance relating to what constitutes "readily" retrievable, such guidance shall prevail in relation to such records.

The record keeper is required to ensure that records maintained on media which is becoming obsolete are transferred to another media if the record is required to be kept beyond the point at which access to the record would otherwise become unreliable.

4.5. Period of retention

According to GDPR personal data can only be retained to the extent it is legally required or where it is necessary in relation to the purposes for which they are processed.
As a licensed bank SEB is subject to several legal requirements that require SEB to collect, process and store personal data, both for internal business, monitoring and control reasons, but also related to its extensive reporting obligations. These different laws and regulations require SEB to store information for different periods, normally between 5, 7 and 10 years. Examples of legal requirements are the legislation related to;

Anti-money laundering and terrorist financing (AML)
Investment services (MiFID)
Sanctions (screening of customers and beneficial owners)
Tax related legislation
Central Securities Depositories
Financial agreements
Payment services and transactions
Market Abuse

In relation to several of these regulatory items SEB will also have extensive reporting obligations both towards customers and public authorities as well as market operators. Examples of this are;

Tax reporting – national as well as FATCA/CRS
Transaction reporting (TRS) according to MiFID
Suspicious transaction reporting bot in relation to AML and Market Abuse
Client reporting (daily, quarterly and yearly statements)

In addition to this SEB will have contractual obligations related to granting of credits and the internal processes for such handling, account holding and agreements in relation to any other banking services as well as investment services and investment banking services.

SEB will collect and store personal data in many different systems and applications of which most of these are integrated in such a way that one application collects (or is provided) certain data from one or several another system(s) (i.e. a central client register). These systems and applications are integrated in such ways that it will be a considerable risk that partly deletion of information in one database/application may have effect on other applications (which may not be obvious) and their ability to perform i.e. the required tax reporting or suspicious transaction report.

As long as certain basic legal requirements set a minimum time for storing information, which must include personal data, to 10 years and i.e. the tax authorities has the right to reverse decisions within a timeframe of 10 years it is not justifiable to do any deletions in any systems or application before the end of the 10th year after the end of a client relationship.

Based on the above SEB has decided[3] that it will not erase any personal data related to any client, client representative, beneficial owner or closely related person to these persons, or employees before the end of the 10th year after the end of the contractual relationship At that time SEB will initiate a complete erasure of personal data in all relevant systems and applications as well as in any physical archives which shall be completed within the end of the second year thereafter.

5. Client requests for information – right to access

5.1. Procedures – personal data view

All private individuals (persons) with a relationship to SEB have the right to access their personal data. This gives them the right to obtain a copy of their personal data as well as other supplementary information from SEB. See below.

[3] A separate interpretation/background memo has been issued about processing, storing and erasure of personal data, dated 27052019.

A client can make a subject request to SEB verbally or in writing. It can also be made to any part of our organisation (including social media) and it doesn't have to be addressed to a specific person or a contact point. This presents a challenge as any of our employees could receive a valid request. However, it's up to each employee to identify that a client has made a request and to handle it accordingly. If in doubt, you should seek advice from the DPO or the DPR.

The request does not have to include any specific phrase such as "request for personal data, as long as it's clear that the client is asking for their own personal data.

SEB has provided an electronic contact point at seb.no, so that request can be made electronically. Request for personal data by other means should, to the extent possible, be routed through that contact point. Please seek advice from the DPO if in doubt. A request coming through SEB's electronic contact point will automatically be forwarded to E- journal and be picked up by Operations and handled in accordance with a separate instruction.

SEB shall act on a request without undue delay, and at the latest within one month of receipt. The time is calculated from the day after SEB has received the request. SEB can extend the time to respond by a further two months if the request is complex, or SEB has received a number of requests from the same person. If SEB process a large amount of information about a person SEB may ask the person to clarify the extent of the request.

A person may submit a request via a third party, often a solicitor acting on behalf of the person. In such cases the person handling the request must take the necessary steps to assure that such a third party is entitled to act on behalf of the person, normally through a written authority or a power of attorney.

The utmost care must be placed with the verification of the authorisation of each request, which include at least a call back to a phone number already registered in relevant CRM-system. If in doubt about the identity of the person submitting a request SEB is entitled to seek additional information to confirm the person's identity before responding to the request.

SEB may refuse to comply with a request if certain exceptions are present. If in doubt please contact the DPO or DPR for advice.

Requests for personal data relates to the data held at the time the request was received by SEB. It is not acceptable to amend or delete the data if we would not otherwise have done so and present legislation states that it is an offence to make any amendments to the information with the intention of preventing its disclosure. It might, in special cases, be possible to make certain amendments before sending the information, provided written approval from the DPO.
Responding to a request may involve providing information that relates both to the individual submitting the request and to another individual. In such cases SEB are not obliged to deal with the request if it would mean disclosing information about another individual that can be identified from that information, except if the other individual has consented, or it it`s reasonable to comply with the request without consent. In such cases advice shall be obtained from the DPO or the DPR, before any information is submitted to the requesting person.

Due to the fact that the response to the client in the form of a Personal Data View (PDV) may contain a large amounts of personal data put together, thus the complete report(s) will be very sensitive. It is

therefore of the utmost importance to protect this information and it is under no circumstance acceptable to send such information by ordinary e-mail or similar.

Clients should only receive reports in physical form and delivered in person or by registered mail unless encrypted mail can be utilised. In doubt contact the Local DPO.

5.2. Recording of requests

All requests received by SEB units in Norway shall be recorded and stored. A register of the requests shall be maintained so that SEB are able to track the timely and adequate response to data subjects' requests. Operations shall implement work routines for the handling and recording of all requests for personal data view. Such routines shall be approved by the local DPO or DPR. The routines shall include language about information duties towards the local DPO.

The record shall be in the form of an Excel spread sheet which can be found on the local intranet and shall contain information the client's request (when it was receive, what the request is about (access, correction, portability, erasure etc. and by whom) and further to whom it is designated for formal handling and the deadline for the response to the client.

6. Rectification and erasure (the right to be forgotten)

6.1. General principles

All private individuals (persons) with a relationship to SEB have the right to obtain from SEB the rectification of inaccurate personal data concerning that person. The person shall also have a right to have incomplete personal data completed.

Unless specifically and explicitly required by regulation or contract, a record that is required to be destroyed may be destroyed through removal of the record in its primary record keeping facility preventing its retrieval through ordinary and regular procedures.

Destruction of archived copies, redundant back-ups and similar is not a prerequisite of the record considered to be destroyed, e.g. in instances and circumstances where it may be accessed solely by a highly limited number of persons and for a limited set of circumstances, for all practical purposes and in compliance with this instruction, the record may be considered destroyed. Certain records may also be destroyed by terminating the link between records, where the very link constitutes the record to be destroyed.
If in doubt consult the local DPO/DPR.

6.2. Regular deletion SEB initiated

Where GDPR requires that personal data is required to be deleted; the following may be considered as guidance regarding steps that are sufficient to comply with the requirements:

- Process and system owners shall establish steps to annually identify data subjects that have been inactive for the past 12 months. Such data subjects shall be listed and compared to previously generated lists of inactive data subjects. A data subject may be considered active despite not engaging in any activity for the past 12 months to the extent a valid agreement or contract still exists.

- Data subjects that have been inactive for 10 years shall be removed from active directories, separating them from the active population of data subjects. This means that their profiles and similar shall, at a minimum, be made unavailable[4] for use in the process unless actively re-instated. They may still be available as records in systems but only insofar as being able to see that there is an inactive profile which may be reinstated.

- Certain data of a data subject may become inactive at different times, and processes should as far as practically possible, capture such differences. Monitoring and cleaning routines should as far as possible keep in mind the purposes for which specific records are obtained.

Each system or process owner shall establish routines and procedures for these clean up processes.

6.3. Client requests

A request for rectification, completion or erasure shall be forwarded and handled in the same way as decided for the personal data view in section 5.1 above.

When receiving a request for rectification SEB shall take reasonable steps to ensure that the data is accurate and to rectify the relevant data if necessary. There is no legal definition of the term accuracy, thus SEB should interpret accuracy as personal data that is incorrect or misleading. A data subject has the right to request restriction of the processing of their personal data where they contest its accuracy and while SEB is investigating whether or not this is correct.

If SEB conclude that the existing data is accurate SEB shall inform the data subject of this conclusion, the reason for this and that SEB will not amend the data, as well as the data subject's right to make a complaint to the local DPO or the Norwegian Data Protection Agency. In such cases a note of the situation shall be recorded in relevant CRM-system.

SEB may decline to comply with a request for rectification if the request is manifestly unfounded or excessive. In such cases SEB may request a reasonable fee to deal with the request or simply refuse to deal with it. If such an event occur the request shall be handled by, or in cooperation with the local DPO and any decisions taken shall be recorded and include the reason for declining the request.

If the data that are subject to the request under this section has been disclosed by SEB to third parties, SEB shall inform the relevant third party about the rectification, completion or erasure of the personal data, unless this proves impossible or involves disproportionate effort.
All requests for rectification must be recorded in accordance with 5.3 above.

7. Data Privacy Impact Assessment (DPIA)

New products or services may involve a new processing activity in relation to personal data, thus we may be required to conduct a Data Privacy Impact Assessment. The Data Protection Impact Assessment is a process which helps us to identify and minimize the data protection risks. SEB has implemented a global setup for the DPIA process that shall be followed in SEB Oslo Branch.

[4] See preamble 67 to GDPR

The first part of a DPIA is pre-assessment that will provide input regarding where a full DPIA needs to be made. If uncertain, it is recommended that you complete the pre-assessment to document that the matter has been considered.

The DPIA is developed to identify processing that poses a high or significant risk in to the privacy of the data subjects. Where a high risk is identified, additional safety measures may need to be put into place regarding processing. While the data processing may have one objective and purpose, the data set could also be used to identify or profile the individuals and could easily be combined with other data related to the data subjects. More information regarding when, why and how to conduct a DPIA is available on the GDPR intranet site. A DPIA shall always be carried out when SEB shall implement new technology or intend or shall combine, compare or match personal data from different data sources or if the processing is entirely dependent on client's consent.

In relation to new products or services we shall use the current NPAC set up and include the DPIA in this process.

If a more general or periodic DPIA is required this should be included as part of the joint Risk Assessments conducted by Risk Control, Internal Audit and Group Compliance

A template Data Protection Impact Assessment questionnaire and a process description to be used in the DPIA are available on the Intranet.

8. Breach notification

Significant and severe personal data incidents need to be alerted to the relevant supervisory authority (Datatilsynet) and in certain cases also to the potentially affected data subjects. When an incident is identified, such as where information has been lost, stolen or accessed by unauthorised persons (hacked), or where personal data has been sent to wrong persons (i.e. erroneous distribution of account statements or invoices) the employee that identify such incidents should, when the incident may affect any data subjects' right to data privacy, immediately report this to the local DPO or DPR in order to assess whether the incident needs to be reported. Data privacy breaches must be reported in 72 hours so it is vital that incidents are raised promptly.
A more detailed breach notification procedure[5] shall be decided by the local DPO in cooperation with the local DPR, taking into account among other things the fact that SEB only have a very short period of time to determine what has happened, what type of incident and then working on how the breach can be handled. When the timing is not met, reasons will have to be provided to the Norwegian Data Protection Agency. The need for public notification of data subjects must also be considered in the unlikely situation that it is impossible to notify the data subjects individually.

Detailed procedures for internal breach notification are available on the Intranet under "GDPR Personvern".

9. Incidents register

All incidents need to be registered. Incidents shall be included in the DPO incidents register and in ORMIS to the extent required.

[5] Varslingsrutine ved brudd på personvernregelverket(GDPR)

A form to be used shall be developed by the Local DPO in cooperation with the local DPR.

10. Data Processor Agreement (DPA)

As there is a requirement that all Personal Data processing is lawful by the processor – outsourcing and certain service arrangements need to include Data Processor Agreements. This is to clarify who is the "controller" of the data, who the processor is and what roles and responsibilities they have. Where we bring in a new service provider or external hosting of a system, it's important to include any Data Privacy issues from the start of the requirement setting and negotiations. SEB has developed a DPA to be used in Norway and all such agreements shall be handled and recorded by Procurement.

Clients of SEB may from time to time wish to discuss entering into a DPA with SEB in relation our services. As a main rule SEB will not be a data processor on behalf of third parties. If in doubt contact the local DPO, DPR or Procurement.

Schedule 1 - General information to clients – short version

SEB will collect and process personal data that is necessary in order to execute contractual agreements to which you are, or will be, a party and to meet our legal obligations following, among others, the Anti Money Laundering Directive and Markets in Financial Instruments Directive. Supplementary information about the processing of personal data and your rights can be found in the SEB's data privacy policy which is available on Seb.no under the link "Personvern".

Where the collection of personal data is a consequence of a contractual agreement, i.e. where SEB enter into agreements with legal entities that shall submit personal data of its representatives, the Client grants SEB the authority to process or arrange for processing of personal data on the Client's behalf for the purposes of the services provided pursuant to the agreement in accordance with any applicable laws and regulations. When SEB process such data, SEB shall take appropriate technical and organisational measures designed to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. In particular, SEB shall process personal data only for the purposes contemplated by the contractual agreement and relationship. SEB shall act on the Client's instructions only (given for such purposes). SEB may also process or arrange for processing of personal data in order to support the maintenance of quality and standards in SEB's work or to facilitate the administration of SEB's business or to support its infrastructure. The Client shall be responsible for informing its representatives and other privat individuals within their organisation affected by the above of the effects on their data privacy.

Notwithstanding SEB's ability to appoint sub-contractors in accordance with any agreements, SEB shall answer the Client's reasonable enquiries to enable the Client to monitor SEB's compliance with this provision. SEB shall not sub-contract the processing of personal data (unless to the SEB Group, or other parties that are required to take equivalent measures when processing personal data) without the Client's prior written consent.