Translation: Regler for Sydbanks eBanking - privat

Rules for Sydbanks eBanking - private

Sydbanks eBanking is the general term used for the electronic self-service functions (eBanking functions) offered by Sydbank, Sydbanks NetBank and Sydbanks MobilBank.

The rules for Sydbanks eBanking are supplemented by special rules for the individual functions, which deviate from the rules for Sydbanks eBanking. The rules for Sydbanks eBanking and the special rules for the individual functions supplement Sydbanks Terms and Conditions.

1. **General information**
   You can find answers to most questions, read instructions on the technical requirements for applying the functions and get information on the latest updates at sydbank.dk.

2. **Registration**
   You can sign up for or request registration of one of more functions in Sydbanks eBanking and sydbank.dk, in Sydbanks NetBank or by contacting your Sydbank branch.

   Depending on the function you sign up for, you can use the function immediately after you have signed up or once you receive a message from Sydbank.

   The first time you use a function in Sydbanks eBanking, you must electronically accept the rules for Sydbanks eBanking and/or the special rules applying to the function.

   If you are under 18, you will only be allowed limited access to the functions in Sydbanks eBanking.

3. **Cookies**
   Sydbank uses cookies and similar technologies in our electronic self-service functions. We do so for statistical and technical reasons.

   If you set your browser to block cookies, it is not possible to log in to Sydbanks NetBank. and Sydbanks MobilBank we prepare statistics anonymously to make our self-service solutions even better. Read more about Sydbank's use of cookies and how to delete them at sydbank.dk/omsydbank/vilkaar/cookies.

4. **Credit rating**
   Whether you will be allowed access to the functions in Sydbanks eBanking depends on an individual credit rating of your commitment with Sydbank. Sydbank is not obliged to allow you access to the functions in Sydbanks eBanking, and Sydbank may decide to only offer you specific functions or part of these.

5. **Power of attorney**
   You may in writing authorise another person to access your accounts with Sydbank or part of them. The person must be a customer of Sydbank and must have signed up for Sydbanks eBanking.

   You must execute a power of attorney via power of attorney forms for Sydbanks eBanking. A power of attorney is effective until you notify Sydbank in writing of the revocation.

   Once you have signed up for Sydbanks eBanking, you may also be granted a power of attorney and get access to other people's accounts or part of them.

   If you are under 18, you cannot be granted a power of attorney for other people's accounts, but you can get access to specific functions in Sydbanks eBanking. We delete the access of an agent under a power of attorney to accounts of persons under 18 at the 18th birthday of the principal under the power of attorney.

   An agent is generally allowed access to and can sign up for the same functions as the principal, but a few functions will not be available to the agent.

   The access of custody account holders to trade various types of securities also applies to the agent, if any.

   Transactions performed by an agent are binding as if the transaction had been performed by the principal. The power of attorney granted by the principal to the agent is of no concern to Sydbank.

   If you have authorised another person to access your accounts, this person also has access to NetBoks which

contains both historical and future documents. The person can also choose between receiving and not receiving paper statements in the same way as you can.

6. Personal security solution

Certain functions in Sydbanks eBanking require that you apply a personal security solution.

Basically, NemID is used, which is provided by Nets DanID A/S.

If you do not already have NemID, you will get NemID which is to be applied as Sydbanks security solution in connection with registration for certain functions in Sydbanks eBanking.

The NemID conditions 1-3 form part of the rules on the use of Sydbanks eBanking. You may view the existing NemID conditions at nemid.nu at any time. The NemID conditions 1-4 can be seen below.

If you enter your mobile phone number in connection with registration for or use of the functions in Sydbanks eBanking, Sydbank saves your mobile phone number for administrative purposes and Sydbank passes on the mobile phone number to Nets DanID A/S, which manages NemID.

If you get a new mobile phone number, it is your responsibility to change your mobile phone number in Sydbanks NetBank and Nets DanID A/S' website nemid.nu.

If, at a later point in time, you wish to use NemID to provide your digital signature or you would like support in connection with this function, please contact Nets DanID A/S via the website nemid.nu or your local "Borgerservice" (citizen service centre).

If for this function you need another type of personal security solution, this will appear from the special rules applying to the function.

7. Transactions in your accounts

In Sydbanks eBanking you have access to your present and future accounts in Sydbank.

You can basically see all your accounts and you can make arrangements relating to your accounts with Sydbank in the same way as when you contact Sydbank in other ways. However, Sydbank may have decided to only allow you limited access.

If you are under 18, you can only view accounts in your name and operate accounts where the deposited amounts are generated by independent employment unless your guardian(s) has/have accepted in writing that you can operate other accounts.

Part of your commitment may be subject to limitations in authority.

Sydbanks eBanking allows you to execute payments at a maximum amount of 500.000 DKK per banking day to a third party regardless of the payments being executed from your own accounts or from accounts that you are authorised to operate.

If you are under 18, you can execute payments at a maximum amount of 30.000 DKK per 24-hour from your own accounts.

If you have registered a mobile phone number with the Bank, the Bank may use this in connection with executing certain transfers and payments. You can see the mobile phone number in one or more of Sydbanks eBanking functions. You are responsible for updating your mobile phone number in the individual eBanking function if it changes.

The Bank may, for instance, use your mobile phone number to send you an SMS if a payment or transfer cannot be executed.

You may also experience that you need to approve certain transfers or payments more than once. This may be prompted by enquiry from the Bank or by an SMS code sent to you If you receive an SMS code, this must be entered in the individuel eBanking function to execute the transaction.

In the event of other limitations to the application of the individual functions, the limitations appear from the special rules applying to the function.

8. Payment execution

In Sydbanks eBanking a payment order has been received when you receive an acknowledgement of this in the individual eBanking function. You can find information om the maximum time it takes to execute a payment on the "Deadlines" page in the NetBank.

On the "Deadlines" page you can also see when to confirm your payments at the latest in order for these to be executed on the same day.

Information on cross-border transfers can be found in "general terms and conditions for cross-border transfers".

9. Stop payment

You can stop payments as long as the stop function of the individual payment is active.

You can also stop recurring payments and payments from Betalingsservice (Payment Service). The deadlines for revoking the different payments and transfers appear from the page "Deadlines" in the NetBank. Revocation is made by activating the stop function in the screen with details of the individual payment.

You find information on cancellation of payments and payment agreements in Betalingsservice (Payment Service) in "General conditions for Betalingsservice debtors" at www.nets.eu. The conditions are also available at sydbank.dk/aftaler and in your NetBoks.

10. Coverage requirements

Sydbank is not obliged to execute your payments from accounts for which there are insufficient funds to cover the amount. Sydbank may refuse to receive payment orders from your if there are insufficient funds in the account from where the payment is to be executed.

11. Spending overview

In some of the functions in Sydbanks eBanking you can see a spending overview of your expenses broken down into different categories. Sydbank uses a number of standard categories, but you can re-categorise your expenses as you like. The Bank uses information about to whom you make payments or transfers and in which places you have used your payment cards to generate the spending overview. The spending overview is solely available to you. You can at any time deactivate the spending overview in the functions in Sydbanks eBanking where spending overview is available.

12. Budget

In Sydbanks Budget you can make different calculations for budgeting purposes.

You can, among other things, prepare a budget on the basis of you payment agreements, create manual budget items and perform budgetary follow-up.

The calculations in Sydbanks Budget only serve as an indicative calculation for your budget preparation.

Sydbank has no responsibility for all relevant debt items and amounts being debited in the budget or for the correctness of these.

Hence, Sydbank cannot be held liable for any transactions made on the basis of the calculations in Sydbanks Budget.

You can delete your budgets on the "Budget" page in Sydbank NetBank.

If you delete a budget, you must be aware that subsequently it cannot be restored and Sydbank cannot print it for you.

13. Electronic signatures on agreements

Your NemID is your electronic signature and it is legally binding in the same way as your signature on a physical agreement. Therefore your NemID is personal and must not be used by others.

There may a deadline by which an agreement must be signed in the NetBank. If you do not sign the agreement by this date, the agreement will no longer be available in NetBoks.

Electronically signed agreements will be saved in your NetBoks.

14. Support

Sydbanks Hotline is hosted by employees who can offer you advice and answer your questions relating to the use of functions in Sydbanks eBanking.

You can contact Sydbanks Hotline at tel. +45 74 37 25 10 or you can forward a mail to Sydbanks Hotline hotline@sydbank.dk.

You can see the opening hours of Sydbanks Hotline on sydbank.dk.

15. Blocking

You are obliged without delay to block the functions of Sydbanks eBanking, if you suspect or become aware of abuse or the possibility of abuse or attemped abuse of the functions of Sydbanks eBanking.

You can always block the functions of Sydbanks eBanking by contacting one of Sydbanks branches or Sydbanks Hotline. Other possibilities of blocking the

function(s) appear from the special rules for the relevant function(s).

You should be aware that blocking of functions in Sydbanks eBanking does not automatically block your NemID. You can read about blocking of NemID at nemid.nu.

16. Liability for private accounts

The responsibility for unauthorised use of Sydbanks eBanking follows the rules laid down in the Danish Payment Services Act. If you are under 18, the responsibility for unauthorised use furthermore follows the rules pertaining to minors' liability to pay damages in the Danish Guardianship Act.

You are liable up to the sum of 1,100 DKK for losses arising from other people's unauthorised use of your access to the functions of Sydbanks eBanking, where a personal security solution has been used.

You are liable up to 8,000 DKK for losses arising from other people's unauthorised use of the functions in Sydbanks eBanking, if Sydbank documents that a personal security solution was applied, and you

- have failed to notify Sydbank as soon as possible after having learned that a personal security solution has been lost or has come to the knowledge of the unauthorised individual
- disclosed the details for a personal security solution to the person who has used the function without authorisation, or
- by gross negligence enabled unauthorised use

You are liable without limit for losses arising from unauthorised use of Sydbanks eBanking by others, where a personal security solution was used and you disclosed the details about your personal security solution to the person who made the unauthorised use of the function where you realised or should have realised that there was a risk of abuse.

You are also liable without limit for losses where you have acted fraudulently, intentionally failed to fulfil your obligations to protect your personal security solution or where you have failed to block the functions in Sydbanks eBanking.

After you have realised the unauthorised use, you must without delay submit your objection against the unauthorised use or your suspicion in this respect to Sydbank. 13 months after the unauthorised use you can in no circumstances raise an objection.

Sydbank considers your objection and meanwhile we will normally credit your account with the amount temporarily. If it is not another person's unauthorised use of Sydbanks eBanking, we will debit your account with the amount again. Sydbank may claim interest subject to the interest rate applying to the account in the period in which the amount was temporarily deposited to your account.

In Sydbanks assessment as to whether you should have been aware of the unauthorised use, we take into account that the Bank issues monthly statements of account to your NetBoks, and that you have access to transactions in Sydbanks eBanking.

You are only liable for losses arising from the unauthorised use of Sydbanks eBanking by other people where the transaction has been correctly registered and booked with Sydbank.

You are not responsible for unauthorised use of Sydbanks eBanking, which takes place after you have blocked the function(s) of Sydbanks eBanking.

In accordance with the Danish Payment Services Act Sydbank is liable for your loss if the payment recipient knew or should have known that Sydbanks eBanking had been subject to unauthorised use.

17. Liability for business accounts

Sydbank is not liable for losses on business accounts as a result of any misuse of Sydbanks eBanking or any misapplication of the functions of Sydbanks eBanking.

Linking business accounts in Sydbanks eBanking is at your own risk. You may cover the risk by taking out insurance.

Retail accounts applied for business purposes are considered to be business accounts and are consequently covered by liability as regards business accounts.

The account holder is liable for losses suffered by Sydbank as a result of the unauthorised use of business accounts in Sydbanks eBanking.

18. Changes to the rules

Sydbank will change the rules of the functions of Sydbanks eBanking without notice provided that the changes are of no disadvantage to you.

For any other instances, Sydbank will change the rules of the functions in Sydbanks eBanking subject to two months' notice, unless the changes are for security reasons and unless the changes relate to the limits for payments per 24-hour period, which will be effective without notice.

You will be informed about any changes by letter or electronically, for instance in NetBoks.

You may be asked to accept the changed rules when logging on or the first time you use the function after the change has come into effect. Any changes of the rules will be deemed accepted, unless you inform Sydbank before the date of the changes coming into force that you do not wish to be bound by the new rules. If you do not wish to be bound by the new rules, the agreement will be terminated with effect from the date when the new rules come into force.

19. Default, termination and cancellation

Your access to Sydbanks eBanking will be terminated without delay and orders will not be executed if Sydbank suspects your or another person's misuse or abuse of the functions in Sydbanks eBanking, or if you default on your commitment or part of it with Sydbank.

In the event of your death or the death of the principal, or where you or the principal are/is administered in bankruptcy, file(s) for debt restructuring or debt rescheduling or initiate(s) some other form of insolvency proceedings, the access to Sydbanks eBanking will immediately be closed and orders will not be executed.

Sydbank can close your access to the functions in Sydbanks eBanking subject to two months' notice.

You can always cancel the functions of Sydbanks eBanking in writing and without notice.

20. Complaints against the Bank

If you want to file a complaint against the Bank, please contact Sydbanks complaints officer. If a complaint is not upheld, complainants may contact Pengeinstitutankenævnet (the Danish Complaint Board of Banking Services) or the Danish Consumer Ombudsman.

21. Fees

Fees incurred on use of functions in Sydbanks eBanking appear from the price list available in the Sydbank NetBank and at sydbank.dk. Any fees are payable quarterly.

22. Right of cancellation

You may cancel this Agreement subject to the Danish Consumer Protection Act within 14 days after the Agreement was signed. You can read about this in Sydbanks "Oplysning om fortrydelsesret" (Information on the right of cancellation), which is available in your NetBoks and at sydbank.dk.

Translation: Regler for Sydbanks eBanking - privat

Rules for Sydbanks NetBank - private

Sydbanks NetBank is your electronic Sydbank branch.

In NetBank the functions are developed on an ongoing basis and you can, among others:

- see transactions on your accounts
- transfer money - also to other countries
- pay bills using inpayment forms/"indbetalingskort".
- follow the development of your custody accounts
- communicate with Sydbank
- access NetBoks.
- sign up for MobilBank
- prepare a budget
- use BeskedService
- administer eBanking - and see which functions you have used.

If you want to use the other functions of Sydbank NetBank, you must sign up and accept the rules for the functions. This includes, e.g., securities transactions.

1. **Personal security solution**
   To apply Sydbank NetBank you must use NemID which consists of a user ID, a password and a code card/code token. Your user ID, your password and your code card/code token are personal and must be used solely by yourself. Consequently, your user ID, password and code card/code token must be stored in such a way that others cannot learn about them.

   In the Netbank you are free to decide whether you want to use a code from your code card/code token in connection with login. If you do not want to use a code in connection with login, you will solely be asked to enter user ID and password in connection with login. If you have chosen that the Netbank should ask for a code in connection with login, you will not be prompted to enter a code to approve a transaction. You only need to enter your password to approve a transaction. If, on the other hand, you have chosen that the Netbank should not ask for a code in connection with login, you will be prompted to enter a code to approve the first transaction. Hereafter you will only need to enter your password when you approve a transaction. Approval of transfers between your own accounts and accounts for which you have a power of attorney does not require a password or code from your code card/code token.

   You can use Sydbanks NetBank every day, but Sydbanks NetBank is closed the night between Saturday and Sunday between 02:00 CET and 06:00 CET and all others days between 03:00 CET and 05:00 CET.

2. **Communication with the bank**
   You can write to your branch or account manager through Sydbank NetBank. Communication via Sydbanks NetBank is encrypted to prevent others from seeing it.

   If you write after 12:00 CET, your inquiry may not be read or executed on that banking day.

3. **Other functions**
   On the "Agreements" page, you can see an overview of the functions of Sydbanks eBanking, for which you have signed up and which relate to the functions in Sydbanks NetBank.

4. **Blocking an unblocking**
   You can block your access to Sydbanks eBanking and Sydbanks NetBank

   - in Sydbank NetBank on the page "Blocking"
   - by contacting Spærreservice (Blocking Service) (available 24 hours a day) at tel. +45 75 94 50 93, stating that you are a client with Sydbank NetBank.

   Your access cannot be unblocked by Spærreservice (Blocking Service).

   When blocking your access to Sydbank NetBank, you receive a written confirmation of the blocking with an indication of the time when the access was blocked. The confirmation comes with a form that you must return to Sydbank in order to unblock your access. You must submit or forward the form to Sydbank, when you wish to have your access unblocked.

Translation: Regler for Sydbanks eBanking - privat

Rules for Sydbanks MobilBank

1. Registration and deregistration

When you sign up for Sydbanks MobilBank, you have access to many of the functions also available in Sydbanks NetBank. The functions of Sydbanks MobilBank will be developed on an ongoing basis. When signing up you will be given a 6-digit mobile code. You must use the code together with your user name when you log on to Sydbanks MobilBank. You can always see your mobile code -and change your code - in NetBank.

If you have a telephone/tablet which supports the use of fingerprints, you can use fingerprints to remember your mobile code. You can activate fingerprints under settings in Sydbanks MobilBank. Your user ID and your mobile code are personal and must not be disclosed or used by any other person than yourself. This is also the case if you use fingerprints to remember your mobile code.

You can at any time deregister Sydbanks MobilBank in NetBank.

1.1. Management and approval of payments and trades

Your total payments per day through Sydbanks MobilBank cannot exceed DKK 100.000. If you are under 18, your total maximum per day is DKK 30.000. Any payments you make through MobilBank are included in the maximum daily amount available to you through Sydbanks eBanking.

We point out that you may be requested to update MobilBanken before log-on. If so, you will receive a message.

When you have made a payment or securities transaction in MobilBank, you must authorise this with your mobile code and a code from your NemID code card or your NemID code token. Transfers between your own accounts and accounts for which you have a power of attorney do not require approval. Your order has been accepted when you receive a confirmation that payment has been effected. Once you have made a securities transaction, you will receive confirmation on your mobile units, provided the call was not ended or interrupted. If you do not receive a confirmation, you have to contact Sydbank to find out whether the order was executed.

1.2. Blocking and unblocking

You must without delay block your access to Sydbanks MobilBank, if you become aware of or suspect irregularities or misuse of your MobilBank, and if you lose your mobile unit. If NetBank is blocked, MobilBanken will also be blocked.

You can unblock your blocking of MobilBank in Sydbanks NetBank.

We recommend that you activate the PIN lock on your mobile units in order to avoid misuse.

Translation: Regler for Sydbanks eBanking - privat

Rules for Sydbanks BeskedService

Sydbanks BeskedService offers you an opportunity to receive a message from the Bank through one or more media (for instance e-mail or SMS). You are free to select which messages you want to receive.

Read more about Sydbanks BeskedService under the Help tab in the NetBank.

1. **Registration and deregistration**
   When you register, you approve the Service that you sign up for with your NemID code as well as the medium on which you want to receive the message.

If the media information about your medium (for instance mobile phone number or e-mail address) is changed, you are responsible for updating such information in Sydbanks NetBank.

You receive messages through the medium until you deregister from Sydbanks BeskedService on the "Beskedservice" page in Sydbank NetBank. You can deregister from BeskedService without notice.

If you have registered Sydbanks BeskedService for an account, to which you have a power of attorney, the account will automatically be deregistered from Sydbanks BeskedService if your power of attorney is revoked.

Translation: Regler for Sydbanks eBanking - privat

Sections 1-4 in NemID conditions for online banking and public digital signatures

1. Introduction

NemID is a security solution that you can use for accessing your online banking service, public authority websites and private websites. You can also use NemID for providing your digital signature.

NemID comprises a user ID, a password and a code card that indicates the one-time passwords (called codes) you must use together with your user ID and your password.

For the IVR solution (Interactive Voice Response) you receive your codes via your telephone.

You also have the option of having an electronic code token to indicate your codes. However, you will still need to retain your code card, as there are some situations in which you will need to use it.

If you wish to use NemID as a public digital signature you also need a linked OCES certificate for NemID. OCES stands for Offentlige Certifikater til Elektronisk Service ((Public certificates for digital service).

The conditions below apply to the use of NemID. If you only want to use NemID for your online banking service, you only need to read through Sections 2 and 3. The use of your NemID for your online banking service is otherwise regulated by your online banking agreement. This will also make clear to what extent the rules on liability in the Danish Payment Services Directive (Betalingstjenesteloven) apply.

If you also wish to use NemID as a public digital signature, please read through Sections 2, 3 and 4.

You can also find these conditions at www.nemid.nu.

Nets DanID refers to Nets DanID A/S, Business Reg. No. (CVR) 30808460

Unit refers to the unit from where NemID is used, e.g., PC, mobile phone or tablet.

2. Obligation

When you use NemID to carry out actions, e.g. to provide your digital signature, you obligate yourself towards the recipient in the same way as you do when you sign a document physically.

3. Conditions for the use of NemID

3.1. Registration for NemID

When you register for NemID, you are obliged to provide sufficient and correct information.

3.2. Storing user ID, password and code card/code tokener

Please note that:

- your user ID, password and code card/code token must be stored securely to prevent others from using them
- you may not disclose your password or your codes, and you may not hand over your code card/code token to others
- you may not scan your code card, enter the codes on external media or in any other way copy the codes or store them digitally
- you are not allowed to write down your password
- you may not store the password together with your code card/code token or write the password on your code card/code token.

3.3. Security when using NemID

You must make sure that:

- your user ID, password and code card/code token are only used by you and only in accordance with the conditions
- others cannot read your password when you enter it
- you use NemID on a computer where the operating system, Internet browser and other programmes are regularly updated with the latest security updates.

You must regularly check that you have not lost your code card /code token and that NemID has not been misused. You can for example, choose to record where you use NemID in the activity log by using the self-service function at www.nemid.nu. This will enable you to check that NemID has only been used for the websites of service providers you have visited.

3.4. Temporary password

The first time you register for NemID, you will receive a temporary password that you can use to log in. This also applies if you have blocked your password; see Section 3.5 on blocking.

If you suspect that others have knowledge of your temporary password, e.g., if the letter with the temporary password has been tampered with, you should immediately request a new temporary password from Nets DanID or your Bank.

3.5. Blocking

3.5.1. Your duty to block immediately

You must immediately block:

- your code card if you suspect others have or might have gained knowledge of the codes on your code card, e.g., if the letter containing the code card has been tampered with when you receive it.
- your code token if the letter containing the code token has been tampered with when you receive it.
- your code card/code token if you have lost it. If you find your lost code card/code token, it must be destroyed.
- your password if you suspect that others have or might have gained knowledge of it, unless you are immediately able to change the password via www.nemid.nu.

3.5.2. Blocking - what to do

When you block your password and/or code card/code token, you must provide your name, address and civil reg. no. (CPR) as required, or your user ID, or code card number or code token number. You must also indicate whether you want to block your password or the code card/code token. When you have blocked your password, Nets DanID will send you an acknowledgement, stating the time and cause of the blocking.

You can block your password and/or your code card/code token by:

- dialling: +45 72 24 70 10 (24 hours a day)
- going to www.nemid.nu (24 hours a day)
- contacting your bank or local citizen service centre (if your NemID is associated with a public digital signature).

You can use the activity log at www.nemid.nu at any time to check the time that your password and/or code card/code token was blocked and the reason why.

3.5.3. Blocking by Nets DanID

Nets DanID will block your

- password if Nets DanID suspects or learns that others have gained access to your password
- password if the password has been entered incorrectly a certain number of times
- code card/code token if Nets DanID suspects or learns that others have gained access to codes from your code card/code token
- NemID, if Nets DanID learns that you have not complied with the conditions for NemID
- NemID, if the information you provided when registering for NemID is incorrect, or
- NemID, if Nets DanID is informed that you have passed away.

3.5.4. Using NemID after blocking

You cannot use NemID when your NemID or password has been blocked. If only your code card/code token has been blocked, some Banks may allow you limited access to online banking, for instance to check your account information.

3.6. Terminating your access to NemID

If you no longer wish to use NemID, you may terminate your access at any time. See section 3.5.2 on blocking. Please note that you will no longer be able to use the services that make use of NemID.

3.7. Processing of personal data

If you have registered for NemID via your Bank, Nets DanID will process your personal data on behalf of the Bank. Nets DanID will process your data, i.e., name, address and civil reg. no. (CPR), to be able to identify you. Nets DanID will also use your e-mail address, if you have provided one, to notify you of any blocking, for example.

If your mobile phone number is registered with Nets DanID, Nets DanID will use your mobile phone number to send you text messages regarding NemID, for instance, messages regarding temporary passwords.

Log files can be saved on the user's unit whenever NemID is used. The user may delete these if desired. As part of the security Nets DanID registers the times that you use NemID, the IP address and any other information about the unit from which you use NemID.

Read more about log files and security at https://www.nemid.nu/om_nemid/sikkerhed/logning/.

If you use the self-service function at www.nemid.nu and choose to record where you have used NemID in the activity log, Nets DanID will also log the service providers with which you have used NemID. You can always deactivate this registration in which case Nets DanID will no longer log where you have used NemID. Nets DanID will keep the data for the current year + five years, after which it will be deleted.

3.8. Claims related to NemID

Any claims that arise as a result of your use of NemID through your online banking service must be made to your bank in accordance with your online banking agreement. Any claims that arise as a result of your use of NemID at other websites must be made to the service provider or to Nets DanID.

3.9. IVR solution - special note

The IVR solution is primarily designed for the blind and people with impaired vision. If you receive codes via the IVR solution, you must take the proper precautions for the telephone on which you receive codes.
This means that:

- you must ensure that the telephone on which you receive codes is independent of the computer/telephone you subsequently use to type in the code
- you must immediately block your password if you lose the telephone on which you receive the codes, or if you discover that your telephone line is being misused.

3.10. Amendment of the conditions for using NemID

DanID may amend the conditions for NemID without prior notice, if the amendment is due to a change of the NemID security requirements. Amendments will enter into force once published at www.nemid.nu. If you have registered your e-mail address with DanID, you will also be notified of amendments by e-mail. Other amendments will be announced at www.nemid.nu no later than three months before becoming effective.

4. Special rules regarding public digital signature

- If you choose to use NemID for public digital signature, the conditions in Section 4 supplement the conditions in Section 2 and 3.
- You can ask for different NemIDs and thereby also different code cards/code tokens and user IDs to use for your online banking solution and your public digital signature, respectively.

4.1. Processing of personal data

When you have an OCES certificate issued and linked to NemID, you accept

- that Nets DanID makes a search in the CPR register to retrieve your name and your address
- that Nets DanID discloses the connection between your public digital signature and your civil reg. no. (CPR) to the public PID service at the Danish Agency for Digitisation (Digitaliseringsstyrelsen). The PID service is used for

searches from public service providers to identify you. A private service provider can only have your civil reg. no. (CPR) disclosed if you accept this when you log on to the service provider

- that Nets DanID makes searches in the public PID service to retrieve any PID number from a previous digital signature.

When you have registered for NemID in connection with your online banking solution and you also want to use NemID for public digital signature, you also accept that the Bank discloses your personal details (name, address, civil reg. no. and any e-mail address and mobile phone number) to Nets DanID so that Nets DanID can use your information to issue and manage your public digital signature.

When you have received NemID in connection with the issue of public digital signature and you also want to use NemID for your online banking solution, you at the same time accept at the enquiry of the Bank that Nets DanID discloses information about NemID to your Bank so you can use NemID in your online banking solution.

If you no longer want your personal information and/or information about NemID to be processed as described above, you can either block your public digital signature by contacting Nets DanID or a citizen service centre and/or close your access to your online banking solution by contacting your Bank.

If you block your public digital signature, you can only use NemID in your online banking solution; if you close your access to your online banking solution, you can only use NemID for public digital signature.

4.2. Your obligations and your responsibility as owner of a public digital signature with an OCES certificate

You must make sure that information about name and any e-mail address in the OCES certificate is correct.

If the information that appears from the OCES certificate is changed - for instance if you change your name - you must within 30 days renew your OCES certificate. If the OCES certificate is not renewed within 30 days and Nets DanID is aware that the information is not correct, Nets DanID blocks your OCES certificate.

You cannot use your OCES certificate to issue certificates to others.

4.3. Blocking of your OCES certificate

Nets DanID will block your OCES certificate if

- you ask Nets DanID to do so
- Nets DanID learns that you have not complied with the conditions for NemID.

When you block your OCES certificate, Nets DanID will send you an acknowledgement that the blocking has been completed, either in a signed e-mail or in a letter to your registered address if Nets DanID has access to it. If Nets DanID does not have access to your registered address, the acknowledgement is sent to the address that you have registered with Nets DanID. If Nets DanID blocks your OCES certificate without you having requested it, Nets DanID will notify you about the reason in a signed e-mail if possible.

4.4. Renewal of your OCES certificate

The validity period of the OCES certificate appears from your OCES certificate. An OCES certificate is valid for up to four years. No later than four weeks before the OCES certificate expires, Nets DanID will notify you in an e-mail or in a letter to your registered address if Nets DanID has access to it. Before the validity period expires, you may renew your OCES certificate by using the old OCES certificate. If your OCES certificate has expired or is blocked, you must order a new certificate.

4.5. Obligations and duties when you receive digitally signed data

If you receive digitally signed data, for instance because you exchange digitally signed e-mails or documents, you must, before you trust the OCES certificate, make sure that the sender's OCES certificate

- is valid - i.e. that the validity period, which appears from the OCES certificate, has not been exceeded

- is not blocked - i.e. that it is not listed on Nets DanID's blocking list at Nets DanID's website
- is used in accordance with any application limitations which appear from the OCES certificate.

4.6. Nets DanID's liability towards you as owner of an OCES certificate

Nets DanID's liability for damages in case of unauthorised or fraudulent use follows the general rules of Danish law. Nets DanID is not liable for losses if you did not comply with the NemID conditions. You must claim any damages relating to your OCES certificate from Nets DanID. The NemID conditions are subject to Danish law. Any discrepancies between you and Nets DanID, which cannot be resolved by negotiation, may be brought before the City Court of Copenhagen.

4.7. Nets DanID's liability to you when you receive digitally signed data

Nets DanID is liable for losses you suffer when you reasonably trust a sender's OCES certificate if the loss is caused by Nets DanID making a mistake in connection with registration, issue and blocking of the certificate. Nets DanID is not liable for losses if Nets DanID can establish that Nets DanID did not act negligently or intentionally.

Translation

The above is a translation of the Danish "Regler for Sydbanks eBanking - privat". In case of doubt the Danish original will apply.