Online portal agreement DNB version 18.06.25

This online portal agreement is entered into between DNB Bank ASA and the customer. In this agreement, 'DNB', 'the Bank' and 'the Group' mean DNB Bank ASA with subsidiaries and underlying companies, including DNB Livsforsikring AS and DNB Asset Management AS.

1. What the agreement regulates

The agreement regulates customers' general access to DNB's online portal. The online portal provides access to the online bank and the customer's 'Total overview', which provides a clear presentation of most of the products and financial instruments that the customer has agreements on with one or more companies in the Group.

The customer is also given a presentation of most of the products and services offered by the various companies in the Group. This agreement does not in itself mean that a customer relationship has been established with the Bank or other companies in the Group. A customer relationship is established when agreements on services or products are entered into.

Agreements relating to individual products can be entered into electronically through the online portal and secure authentication and proof of identity (electronic signature). Unless expressly stated otherwise, the terms set out in this agreement apply in addition to the individual service agreement that the customer has at any given time. For customers who are members of collective agreements entered into by their employer or trade union, the terms set out in this agreement apply in addition to the provisions and product conditions etc. accepted by the customer's employer or trade union when entering into the collective agreement.

2. Entry into the agreement

BankID may be used to enter into agreements with the various companies in the Group, see section 1. In the case of agreements entered into through the online portal, the bank will be considered to be the intermediary between the customer and the company with which the agreement is entered into. Information the Bank acquires relating to agreements with other undertakings in connection with the use of the online portal, can be used by the Bank in its role as an intermediary. If a customer relationship has been established with the Bank, knowledge about such agreements can also be included in this.

3. Consent to electronic communication

Messages concerning the customer relationship from the various companies in the Group will be made available in the customer's mailbox in the online portal unless the customer has opted out of electronic communication. This also includes regulatory and agreed notifications, terminations, etc. unless paper-based information is mandatory.

Some types of correspondence will only be sent as regular mail. The customer may opt out of electronic communication at any time by changing the consent settings in the portal, and instead have messages sent in paper form. Receiving written messages in paper form may be subject to fees.

Messages to the customer will take effect for the customer when they are made available in the customer's mailbox in the online portal.

In the event of messages concerning cancellation, termination, blocking, legal enforcement of debt repayment or similar matters that it is essential that the customer is made aware of, DNB may, if necessary, contact the customer by SMS, email, telephone or some other means of communication to ensure that the customer has received the message.

Messages from the customer to DNB are considered to have been received when they have been sent, or otherwise made available to DNB, in a responsible way. The customer must use communication channels provided by DNB, such as the phone number (+47) 915 04800.

4. Codes, security procedures and computer equipment

The customer can sign in using BankID issued by other banks permitted to engage in banking operations in Norway. Customers who do not have BankID may be sent their own security device for use when logging in. The security solutions are protected by a password/code and are personal and not to be used by others. The customer must use the security solutions in accordance with the terms of issue and use, and otherwise follow DNB's instructions and safety advice that are applicable at any given time. It is vital that passwords/codes are created in accordance with the requirements of the security solution concerned and never divulged or written down in a way that would enable unauthorised persons to pretend to be the customer vis-à-vis the Group. The password must be changed in accordance with the stated requirements for the security solution concerned at any given time. Passwords/codes generated by the security solution is the customer's signature when using the Group's online services. When this signature is used, it will be assumed that it is the customer who has entered into the agreement, or made use of the individual service.

5. Copyright and proprietary rights
The Bank or any other company in the Group that has issued a security device has full copyright and proprietary rights to any such security device, user manual and related documentation provided by the Bank or other company in the Group. Such security devices, user manuals and related documentation are not to be handed over to others, sold, copied, modified, manipulated, or otherwise used for purposes not authorised by DNB.

6. Security rules
The customer is responsible for ensuring that no one else, not even somebody who is acting on behalf of the police, bank or household members of the customers, has access the security device and password/code or similar, to ensure that unauthorised persons cannot pretend to be the customer vis-à-vis the various companies in the Group. Passwords/codes or other identifiers are not to be noted down in such a way that they can be understood or used by others.

Provided that the customer has satisfactory and virus-free computer equipment at all times, DNB is responsible for ensuring that the customer can use the services for which they have entered into an agreement. The customer is obliged to ensure that their security solutions, routers and/or firewalls do not block data to and from the electronic services in the online portal. It is the customers' responsibility to ensure that their computer equipment, applications, and networks meet DNB's requirements for the use of the services at all times.

Customers must notify DNB without undue delay if they become aware of the loss, theft, unauthorised use or acquisition of a security device and password/code and/or if they become aware of any unauthorised access to the online portal (security breach, hacking, etc.). Customers must use the communication channels provided by DNB, and otherwise assist DNB so that the security device and access to the online portal are blocked as quickly as possible.

7. The responsibility of the Bank
The Bank is liable for third parties' unlawful dispositions in the web portal, unless the customer's correct identifier (password/code or similar) has been used. The Bank is not liable for losses arising as a result of, for example:

- Errors or problems with networks, operational disruptions, miscommunication or problems on the part of the customer or of the customer's business partners, or other issues relating to the customer or the customer's business partners,
- Errors or problems - including capacity problems or other issues relating to communication networks,
- Errors or problems - including capacity problems or other issues of any kind before the assignment enters the Bank's network or within the Bank's network in the time before the Bank has confirmed that it has received the customer's assignment.

The Bank's liability may be limited or cease to apply altogether if the customer uses software or documentation in breach of this agreement, including engaging in activities such as manipulation and unauthorised modification, or if the customer exceeds specified limits.

The same limitations of liability apply to other companies in the Group that the customer has a product or service agreement with.

8. Information under the customer's Total overview in the online portal
The information under the customer's Total overview is based on data obtained from the various companies in the Group. The overview may therefore contain errors. For example, the information may not necessarily be up to date at all times. For some of the services, the online portal may show the time of the last update under the individual products. In light of this, the customer's Total oaverview is only meant to provide indicative information and cannot be used as a basis for financial transactions.

9. Temporary cessation of DNB's obligations (force majeure)
DNB's obligations under this agreement cease temporarily in the event of exceptional circumstances beyond DNB's control, which DNB could not reasonably have foreseen or avoided the consequences of. The same applies to issues caused by obligations imposed on DNB by law or in accordance with the law.

Exceptional circumstances include, but are not limited to, defects in or failure of power supply, computer or communication systems or other electronic communication systems. They also include government interventions, natural disasters, acts of war, terrorist acts, sabotage, vandalism (including computer viruses and hacking), strikes, blockades, boycotts, lockouts, and/or national or international sanctions.

10. Termination of the agreement
The customer may terminate the agreement without prior notice unless specifically agreed otherwise. DNB may terminate the agreement with 2 months' written notice if it is based upon reasonable grounds.

DNB may, in writing, cancel the agreement in the event of material breaches on the part of the customer, including if the customer acts in breach of the intentions of the agreement. The same applies if the customer uses (or allows others to use) the services for an unlawful purpose, in an unlawful manner or in connection with a criminal act. DNB may terminate the agreement if this is necessary in order for the Bank to fulfil its statutory obligations, or to comply with orders from public authorities or courts, or with sanctions rules and legislation. The reason for the cancellation/termination must be disclosed unless laws, rules or objectively justified security considerations prevent this.

DNB may block access to the services under the agreement if there is an objective reason for doing so, including if this is necessary for security reasons, if there are suspicions of misuse or a danger of fraud, and when there are grounds for cancellation or termination. Blocking may also be carried out in combination with termination.

In the event of the customer's death, DNB has the right to block access and terminate the agreement. If the agreement is terminated, or if DNB demands that it should be terminated on other objective grounds, the customer must immediately return any security device issued by a company in the Group.

If the customer relationship is terminated, the online portal and electronic mailbox will no longer be accessible. DNB urges all customers to make a copy of any documents in the mailbox/archive that they wish to keep before the customer relationship is terminated.