Confidentiality and integrity

Digital Supervision Portal (DLT)

This document discusses the operation of the Digital Supervision Portal (Digitaal Loket Toezicht – DLT) and the measures De Nederlandsche Bank (DNB) has taken to ensure the security and reliability of the DLT reporting environment.

Under the Financial Supervision Act (Wet op het financieel toezicht – Wft), enterprises wishing to enter the financial market must have obtained permission to do so, for example by applying for authorisation. They can submit an application for authorisation to DNB.

As part of our legal duties we assess intended and prospective directors and supervisory board members on fitness and propriety for their position. They can use the DLT system to submit their application for assessment. The exchange of data between you and us through the DLT takes place over the internet. The data you submit to us are confidential, whereas the internet is a public network. It will be clear that this combination carries certain risks. We have therefore taken several measures to safeguard the confidentiality and integrity of the data submitted

Encryption during connection

Encryption prevents third parties from accessing the information that is exchanged between you and us.

Strong authentication

Authentication enables both you and us to establish unequivocally the identity of the party we exchange data with. The DLT system uses eHerkenning (eRecognition), assurance level 3 (two-factor authentication).

A secure infrastructure

The DLT system is a client-server system. Your computer system and internet browser are the client environment, while the DLT application and the computer system on which it runs are the server environment. We have taken measures in the server environment to safeguard the confidentiality and integrity of the application system. It is your responsibility to take adequate security measuresin the client environment.

Our influence on the client environment is limited

Except for authentication data, the DLT therefore never stores data in the client environment, but always in the server environment, This applies equally to applications that have not yet been finalised and submitted. This set-up enables us to take adequate measures to ensure the security of stored data. This also means that DNB staff is unable to view any application until it has been submitted. We verify on a regular basis whether access to the DLT server is as intended. Each year we carry out security assessments, including penetration tests. Where needed, we use the outcome of these periodic assessments to further improve our system. We have a responsible disclosure policy under which users may report vulnerabilities.

Security procedures

We have several different procedures in place to further enhance the security of the DLT system. The number of DNB system administrators authorised to access the system is restricted and system use is logged. Incoming system abuse is monitored, and we will take measures if we observe such abuse. We will shut down the system if needed. The DLT system will terminate the connection with an applicant if it has not been used for a while.

Risk awareness

Integrity is one of DNB's core values and as such we give it our ongoing attention. Our staff and management are aware of their responsible position in society, and they act accordingly. We are well aware that what was secure yesterday need no longer be secure tomorrow. We therefore test and evaluate all the above measures on a regular basis.