Explanatory Notes

to the Outsourcing Notification Form

DeNederlandscheBank

EUROSYSTEEM

Notification of outsourcing

Explanatory notes to the outsourcing notification form in the Digital Supervision Portal (DLT)

This document contains explanatory notes that help you complete the form to notify De Nederlandsche Bank (DNB) – in the Digital Supervision Portal – of relevant instances of (cloud) outsourcing.

It guides you through the form and provides guidance for its accurate and full completion. It also highlights the focus areas in DNB's assessment of your notification.

Contents

1 General

Purpose of this form

Dutch law prescribes that you should notify DNB of material (i.e. significant or critical) instances of outsourcing, including cloud outsourcing. This form is used for the notification of outsourcing and its outsourcing chain.

What should you notify?

- Insurers: should notify DNB of **all** material (i.e. significant or critical) instances of outsourcing.
- Payment institutions: should notify DNB of **all** material (i.e. significant or critical) instances of outsourcing.
- Banks: should notify us of material (i.e. significant or critical) instances of **cloud** outsourcing.
- Pension funds: should notify us of material (i.e. significant or critical) instances of **cloud** outsourcing.

Former notifications by email are not required to be resubmitted unless there are significant changes or in case of dependencies between a new and old notification.

Does the service provider use a subcontractor?

You should complete the form separately for each instance of outsourcing. A service provider may of course engage the services of subcontractors. You can include this in the form, because a notification form also covers subcontracting. If you outsource to multiple principal service providers, however, you should complete separate notification forms.

When does outsourcing qualifies as material, i.e. significant or critical?

You should assess whether outsourcing is material (significant or critical). Such an assessment can be based upon the following criteria:

- The critical nature and inherent risk profile of the activity you are considering to outsource. You should consider whether the activity is vital to your institution's operational management, continuity as a going concern or viability and to its obligations towards its customers, members or policy holders. This means that your institution is unable to provide its services in the absence of the activity concerned.
- The immediate operational consequences which interruptions of the activity may have, and the associated legal and reputation risks.
- The impact which a disruption in the activity may have on your institution's anticipated revenues.
- The impact which a breach of confidentiality or integrity, or unavailability of data may have on your institution or its customers, members or policyholders.

When should I submit the notification?

The notification has to be submitted prior to the implementation of the outsourcing becoming effective. This also holds true for projects being delivered in multiple stages.

Who should complete this form?

Any authorised signatory may complete the form in the DLT. In order to access the DLT, you need to have an active eHerkenning login token. You also have to be authorised to use our "Supervisory applications" web service, which is one of the services we provide subject to eHerkenning. You can find more information on the eHerkenning website.

Please note: A notification form is linked to the user who initiates and submits it, rather than to everyone in the relevant institution who has eHerkenning and holds "Supervisory applications" rights. Only this user will have access to notification forms and related messages in the DLT.

At least one of your institution's authorised signatories must sign the notification. Please use the signatory statement to do so, and attach it to your notification.

For Significant Institutions: Do I need to notify my joint supervisory team (JST)?

If your bank qualifies as a significant institution (SI), we will forward your notification to the relevant JST. You therefore do not need to notify your JST contact.

Complete and correct notification

Please ensure that you complete the form truthfully and in full and include and upload all required documents. Note that the size of any document that you upload can not exceed the limit of 30 MB. The requirement of truthfulness and completeness also applies to all underlying documents.

Note: we will only be able to process notifications, which have been submitted with all required information. A validation on mandatory fields is included in the form.

Mandatory fields are marked with an asterisk (*).

Confidentiality

We will handle the data submitted in this form with due care. We are prohibited from sharing your data with third parties unless permitted by law, e.g. with supervisory and criminal justice authorities in the Netherlands or abroad.

Change in circumstances

You have to inform us promptly and on your own initiative of any changes in circumstances that would cause you to answer the questions in this form differently.

If you discontinue the outsourcing, you must notify us at Uitbestedingen@DNB.nl.

If there are changes to a notified instance of outsourcing, e.g. in the event of subcontracting or if more business units start using the same outsourced services, please notify us through the DLT. Please state the identification number of the initial notification in the description of the outsourced activity or function. You will find this number in the confirmation we have sent you. You only need to complete the mandatory fields and the fields relating to the change.

If applications start using a cloud IaaS/PaaS system of which you notified us in the past, please state the identification number in the form. In that case, we will not reassess the underlying infrastructure.

What will happen to your notification?

Once you have completed the form in the DLT, we will send you an email to confirm its receipt. We will assess the information and inform you of our decision if we have no further questions.

If we should need additional documents or have any questions, we will send you an email to let you know that there is a request for additional information in the DLT. We will reassess your notification after you have provided the requested information.

Any questions about the DLT?

If you have any questions about specific features of the Digital Supervision Portal, e.g. how to export the form, please read the web page on the use of the DLT.

Any other questions?

If you have any other questions, please feel free to contact our Information Desk by telephone at +31 800 20 1068 or by email at info@dnb.nl.

Relevant laws and regulations

The questions in the form are based on the relevant laws and regulations listed below.

Banks, payment institutions and insurers

- Financial Supervision Act (*Wet op het financieel toezicht – Wft*)
  - Section 1:1 Definitions
  - Section 3:17 Sound and ethical business operations
  - Section 3:18 Outsourcing
- Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiele regels – Bpr*)
  - Sections 27-32 Outsourcing

Banks and payment institutions

- Recommendations on outsourcing to cloud service providers (EBA/REC/2017/03) dated 28 March 2018

Insurers

- Solvency II Directive (2009/138/EC)
  - Article 13(28) Definition of outsourcing
  - Article 38 Supervision of outsourced functions and activities
  - Article 41 General governance requirements
  - Article 49 Outsourcing
- Solvency II Regulation (2015/35/EU)
  - Article 258 General governance requirements
  - Article 274 Outsourcing
- EIOPA Guidelines on the system of governance
  - Guidelines 60-64 in Section 11 Outsourcing
- Good practice for managing outsourcing risks, dated 25 April 2018, open for consultation until 30 June 2018

Pension funds

- Sections 34, 105, 143 and 145 of the Pensions Act (*Pensioenwet – Pw*)
- Section 43 of the Mandatory Occupational Pension Scheme Act (*Wet verplichte beroepspensioenregeling – Wvb*)
- Chapter 4 of the Decree implementing the Pensions Act and the Mandatory Occupational Pension Scheme Act (*Besluit uitvoering Pw en Wvb*)
  - Section 12 Activities that must not be outsourced
  - Section 13 Outsourcing agreement
  - Section 14 Controlling risks
  - IORP II Directive, which entered into force on 13 January 2018. Its provisions must be transposed to national law no later than 13 January 2019 (Decree implementing the Pensions Act and the Mandatory Occupational Pension Scheme Act). This will affect Article 14(6), which deals with the outsourcing notification requirement, and Article 14(3) (b), which provides that outsourcing must not increase operational risks.
- DNB's circular on cloud computing dated 6 December 2011

2 Statement

10 **I declare to complete this form completely and truthfully.***

Here you confirm that the information given in the form is complete and true. The information must be given as available within the institution. The form's final question is that you upload a form signed by an authorised signatory confirming that the notification is truthful.

3 Institution details

Legally registered name* Please provide the institution's name.

CoC registration number Please provide the Chamber of Commerce registration number of the institution for which you make the notification.

DNB relationship number Please provide the institution's DNB relationship number, which is stated in the correspondence you receive from us.

Type of institution You can choose from a list of possible types of institution: bank, insurer, pension fund and payment institution. You do not need to complete the form if your type of institution is not listed. If you still wish to notify us of an instance of outsourcing, please email your DNB contact or contact us at uitbestedingen@dnb.nl.

Does the notification concern a single legal entity?
Choose "no" if the notification concerns outsourcing to multiple legal entities, for example in a group. Please also provide the details of the other legal entity or entities. Keep adding the entities to which the notification relates, provided the outsourcing is identical for all of them.

Outsourcing to multiple legal group entities (group structure): a specific type of outsourcing where the outsourcing institution and the service provider are separate legal entities belonging to the same group.

4 General information on the outsourcing

Designation of activity or function outsourced*
Please describe the activity or function, e.g. email system, infrastructure services, data centre services or accounting services.

Description/elaboration
Please elaborate further if you believe this is necessary.

If your notification relates to a previous instance of outsourcing, you can state this here. As a minimum, you must state the identification number of the previous notification.

What is the commencement date of the outsourcing arrangement?
Please enter the date on which your institution will complete implementation of the arrangement and take it into use.

Who is the principal service provider?*
This is the party with which you enter into the outsourcing contract. It is the first link in the event of subcontracting.

Principal service provider's country of residence (which national legislation governs the contract entered into with the principal service provider?)*
Select a country from the drop-down list.

Will the principal service provider process data?*
Please select "yes" or "no".

DNB considers data processing to be:
The principal service provider or its subservice providers are actively involved in your business activities and perform transactions like reading, changing, complementing your data. Please note that in this context solely storing data is not considered to be processing and therefore you may answer "no".

In which country will these data be processed?*
Select a country from the drop-down list.

Select other countries if data will be processed in multiple countries.
Please fill in which other country.

Will the principal service provider store data?*
Please select "yes" or "no".

In which country will these data be stored?*
Select a country from the drop-down list.

Select other countries if data will be stored in multiple countries.
Please write down the countries.

Will the principal service provider use cloud outsourcing?
Please select "yes" or "no".

For DNB cloud outsourcing means outsourcing using cloud computing. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable information technology resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (Source: National Institute of Standards and Technology)

Which type of service model applies?
Please select IaaS, PaaS, SaaS or Other from the drop-down list.

Infrastructure as a service (IaaS): Infrastructure cloud outsourcing. The infrastructure is provided in a virtual environment. The hardware, including servers, network equipment, and workstations, are owned by the service provider. Customers only pay for actual use. This gives the user full freedom of choice concerning the hardware. The operating system and all software are in the cloud. The management layer and all applications and data are administered in-house.

Platform as a Service (PaaS): Platform cloud outsourcing. In addition to infrastructure, operating systems such as Windows and Linux, middleware and their set-up and administration are outsourced. The data and application administration and development of the applications are in-house.

Software as a Service (Saas): Application cloud outsourcing, also referred to as Software on Demand, means that software is provided as an online service. Customers do not need to purchase the software, but enter into a contract specifying a number of months and a number of users. The SaaS provider installs, maintains and administers the software, which the user accesses online. SaaS is viewed as the application layer in cloud outsourcing, with the platform (PaaS) and the infrastructure (IaaS) providing the underlying layers. Without these underlying layers, usage or the number of users cannot be increased or reduced on a flexible basis.

If you use a combination of these models, please select the model that provides the largest shared pool of configurable computing resources.

Your CIA rating of the outsourcing arrangement
The acronym CIA stands for confidentiality, integrity and availability. The CIA classification is used in information security to rate the confidentiality (exclusiveness), the integrity (reliability) and the availability (continuity) of information and systems.

Information systems, operating processes and data are commonly rated according to the CIA classification to establish their target security level. For example, a high-rated system has a 555 rating, whereas a low-rated system could be 111. The rating is used to take appropriate measures.

You can compose your CIA classification by selecting from the drop-down menu, for each aspect:

1. Very low
2. Low
3. Medium
4. High
5. Very high

Availability score*

Information must be available and accessible. The rating considers the potential impact of unavailability of information or a set of information.

Establish the availability classification by selecting from:

1. Very low
2. Low
3. Medium
4. High
5. Very high

This concerns the rights and authorisation to change, add or destroy data held by a defined group of authorised users. The rating considers the potential impact of a situation in which unauthorised persons gain access to information.

Integrity score*

Information must be an accurate reflection of reality, i.e. it must be correct, complete and up to date. Information integrity crucially hinges upon the solid administration of the rights and authorisation to change, add or destroy data held by a defined group of authorised users. The classification considers the potential impact of incorrect, incomplete or obsolete information.

Establish the integrity classification by selecting from:

1. Very low
2. Low
3. Medium
4. High
5. Very high

Confidentiality score*

Establish the confidentiality classification by selecting from:

1. Very low
2. Low
3. Medium
4. High
5. Very high

Does outsourcing involve subcontracting?

Subcontracting is involved if third parties other than the principal service provider and commissioned by the principal service provider perform elements of the outsourced activities. If such other third party in turn outsources activities to another third party, an outsourcing chain is created. This can happen more than once in an outsourced situation.

Attach a diagram illustrating the outsourcing chain*

Please provide a diagram showing the principal service provider and all subsequent service providers. As a minimum, the diagram has to show the activities or functions they perform. Only illustrate the outsourced activities that you rate "high" or "very high" on one or more CIA aspects.

Please answer the following questions for each subsequent service provider.

5 Outsourcing contract

Is a signed contract available for the instance of outsourcing to which the notification relates?*
Please select "yes" or "no".

[A follow-up question will appear if you select "no".]

What is the reason there is not yet a signed contract?*
Please explain why no signed contract is available (yet).

What is the contract's termination date?*
Please enter the contract's termination or renewal date for each instance of outsourcing to which the notification relates.

Does the contract contain an exit clause?*
Please select "yes" or "no".

Attach or enter in the comments field the wording of the exit clause*
Please add the text of the exit clause from the contract, either as an attachment or copied to the comments field.

Why is there no exit clause in the contract?*
Please state the reason why the contract has no exit clause.

Does the contract include provisions for the supervisory right to examine?*
Please select "yes" or "no".

In the event of subcontracting, the supervisory right to examine must pertain to all service providers forming part of the outsourcing chain. This means that a supervisory authority must have effective access to all information and business premises of all service providers forming part of the outsourcing chain.

Attach or enter in the comments field the wording of the provision stipulating the supervisory right to examine*
Please add the text of the provision from the contract dealing with the supervisory authority's inspection right, either as an attachment or copied to the comments field.

Why is the supervisory right to examine missing in the contract?*
Please state the reason why the contract has no provision on a supervisory right to examine.
Please note: Such a provision is mandatory by law.

Does the contract include provisions about your institution's and the independent accountant's audit right?*
Please select "yes" or "no".

In the event of subcontracting, the audit right must pertain to all service providers forming part of the outsourcing chain. This means that your institution and its independent accountant must have effective access to all information and commercial properties of all service providers forming part of the outsourcing chain.

Attach or enter in the comments field the wording of the provision stipulating your institution's and the independent accountant's audit right*
Please add the text of the provision from the contract dealing with your institution's and the independent accountants audit right, either as an attachment or copied to the comments field.

[A follow-up question will appear if you select "no".]

Why are your institution and its independent accountant not granted any audit right?*
Please state the reason why the contract has no provision on the audit right. Please note: Such a provision is mandatory by law for banks and insurers. In addition, the guidance document on outsourcing for pension funds recommends including the provision.

Does the contract include a clause dealing with subcontracting (conditions subject to which a service provider is permitted to subcontract services and statutory obligations that govern all service providers in the outsourcing chain)?*
Please select "yes" or "no".

Attach or enter in the comments field the wording of the subcontracting clause*
Please add the text of the subcontracting clause from the contract, either as an attachment or copied to the comments field.

[A follow-up question will appear if you select "no".]

Why is there no subcontracting clause in the contract?*
Please state the reason why the contract has no clause on subcontracting. Please note: Such a provision is mandatory by law for banks, insurers and payment institutions. In addition, the guidance document on outsourcing for pension funds recommends including the provision.

6 Risk analysis and controls

18

Have you performed a risk analysis?*
Please select "yes" or "no".

[A follow-up question will appear if you select "no".]

Why have you not performed a risk analysis?
Please explain why you have not performed a risk analysis.

[The following question will appear if you select "yes".]

In what format do you submit your risk analysis?

- You have to address all risks listed in the DNB template. This includes both the 10 risks subjects we have selected and the risks specific subjects to your institution.
- You have to deal with the 10 risks subjects we have selected in the DNB template. Deal with the other risks subjects in your own risk analysis report.

10 mandatory subjects for the risk analysis

You have to address the following subjects as a minimum. Annex 1 contains the Excel template you must use.

1	Vendor lock-in	The risk of not easy or not being able to make the transition to another service provider, for example due to technical constraints, a lack of competitors, or the current service provider's inability or unwillingness to assist in the transitioning.
2	A lack of resources needed to manage acquisitions or existing outsourcing contracts	An institution needs resources (i.e. know-how and staff) to make acquisitions, to apply outsourcing solutions and to monitor suppliers. The latter issue concerns a service provider's performance, as well as internal control, IT risk controls and security. A lack of resources means that outsourcing is no longer managed, potentially exposing the institution to unwanted risks that are not detected or addressed.
3	Concentration	If a single service provider supplies multiple outsourcing solutions, the total impact of possible failure could increase with each additional activity outsourced to the service provider.
4	Cessation of operations	Data, systems and services may immediately become unavailable as soon as a service provider ceases operations. The institution's day-to-day operations may be disrupted and it may be difficult or impossible to retrieve data.
5	Non-compliance	An institution is responsible at all times regarding the outsourced activities and needs to make sure the third party and subcontractor apply to applicable law and regulation.
6	Inadequate performance	The service provider fails to meet the quality standards or observe agreements made, even if quantitative service levels are attained. Or the quantitative service levels are met but the qualitative levels are not. Or both quantitative and qualitative levels are not met.
7	Geographical data location	Data are governed by the laws of the jurisdiction in which the data is stored or by which they are transmitted. Locally applicable laws may differ from Dutch legislation, giving rise to risks related to confidentiality requirements.
8	Separation	Failure of facilities ensuring the separation of storage, memory, routing and even the reputations of the various tenants of shared infrastructure can easily fall out.
9	Data access	It may be impossible to verify whether a service provider deals with data in accordance with statutory requirements. This includes compliance with rules about encryption standards, the four-eyes principle, authentication, etc.
10	Cyberattacks	All risk related to cyberattacks, such as DDoS attacks, data interception or leakage, social engineering, unauthorised access, the unauthorised obtaining of rights, and ransomware.

20 The mandatory risk template has the following columns:

Risk	The assessed risk
Remarks	Brief description of the risk
Analysis	Your analysis of this risk in your institution or within the outsourcing chain
Probability	The likelihood of the risk materialising
Impact	The ramifications if the risk materialises. Use the rating scale from very low, low, medium, high and very high.
Rating	The rating established on the basis of probability and impact in accordance with the table below
Measures	The measures you have taken to mitigate the risk
Residual risk	The risk remaining following the measures taken

We expect you to take measures to mitigate medium and high risks, while accepting residual risks at the appropriate management level (management board) within the institution.

If you use your own template for the other risks we expect you to include these elements.

7 Signatory statement

Signatory statement*

Annex (1)
Name
Signatory statement

Here you can upload the signatory statement. This ensures that your application is signed by an authorised signatory of your institution.

If you submit an outsourcing notification in our Digital Supervision Portal, you must upload a signatory statement together with your signed notification. This ensures that your notification is signed by an authorised signatory of your institution.
You will also find the signatory statement when logged in to the Digital Supervision Portal.

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
PO Box 98, 1000 AB Amsterdam
+31 20 524 91 11
dnb.nl