

Uitoefenen van het bedrijf van betaaldienstverlener

DeNederlandscheBank

EUROSYSTEEM

Toelichting bij het aanvraagformulier voor een vergunning ten behoeve van een betaaldienstverlener -PSD2

De Nederlandsche Bank

De Nederlandsche Bank (DNB) heeft op grond van de Wet financieel toezicht (Wft) tot taak het prudentieel toezicht op betaalinstanties uit te oefenen en te beslissen over de toelating van betaalinstanties tot de financiële markt. Het is DNB wettelijk toegestaan om in het kader van haar toezicht informatie te delen met de Autoriteit Financiële Markten (AFM) en met de Autoriteit Persoonsgegevens (AP). Dit geldt ook in het kader van de beoordeling van een vergunningaanvraag.

Autoriteit Financiële Markten

De AFM heeft op grond van de Wft tot taak het gedragstoezicht uit te oefenen op betaalinstanties. Dit kan een relatie hebben met bepaalde onderdelen van de vergunningaanvraag.

Autoriteit Persoonsgegevens

De AP heeft op grond van de Algemene Verordening Gegevensbescherming (AVG) tot taak toezicht te houden op het verwerken van persoonsgegevens. Dit kan een relatie hebben met bepaalde onderdelen van de vergunningaanvraag.

Inhoud

1	Algemene gegevens	4
2	Business case	8
3	Inrichting bedrijfsvoering voor beheerste uitoefening van het bedrijf	11
4	Inrichting bedrijfsvoering voor integrale uitoefening van het bedrijf	32
5	Betrouwbaarheid en geschiktheid (mede) beleidsbepalers	38
6	Twee dagelijks beleidsbepalers werkzaam vanuit Nederland	40
7	Transparantie zeggenschapsstructuur	41
8	Gekwalificeerde deelneming(en)	42
9	Zekerstelling van gelden van betaaldienstgebruikers	44
10	Minimum eigen vermogen en solvabiliteit	46
11	Aansprakelijkheids-verzekering	48
	Bijlage: Overzicht van de documenten die in het aanvraagformulier worden opgevraagd	51

1 Algemene gegevens

4

1.1 Gegevens van de onderneming

Graag ontvangen wij een aantal gegevens van uw onderneming. Ook vragen wij u een aantal bijlagen mee te sturen, waaronder een gewaarmerkte kopie (afschrift) van de notariële akte van de statuten van de onderneming. Let erop dat de doelomschrijving in de statuten aansluit bij de daadwerkelijk door uw onderneming te verrichten activiteiten. De doelomschrijving mag geen activiteiten omvatten waarvoor een andere vergunningplicht geldt, tenzij u daarvoor al een vergunning heeft. Tijdens de behandeling van de vergunningaanvraag volstaat een finale concept versie van de statuten, indien u nog niet beschikt over een afschrift van de notariële akte van de statuten. De beslissing op uw aanvraag kan DNB overigens pas nemen zodra wij een gewaarmerkt afschrift ontvangen van de statuten van uw onderneming.

1.2 Gegevens externe adviseur

Wij raden u aan om u tijdens de vergunningaanvraag te laten bijstaan door een adviseur. In de praktijk zien we dat de ingediende aanvraag vaker volledig en kwalitatief beduidend beter is als de aanvrager zich laat bijstaan door een expert, bijvoorbeeld een (juridisch) adviseur die gespecialiseerd is in de Wet op het financieel toezicht. Een complete en goed onderbouwde vergunningaanvraag kunnen wij sneller en beter beoordelen. Indien u zich laat bijstaan door een adviseur, dan ontvangen wij ook graag de gegevens van deze adviseur.

1.3 Reeds actief als (vrijgestelde) betaaldienstverlener?

Mogelijk is uw onderneming al actief. Wij gaan ervan uit dat u zich er dan van heeft verzekerd dat u op dit moment nog geen vergunningplichtige betaaldiensten verleent. Als u aangeeft dat uw onderneming al actief is onder de Vrijstellingsregeling Wft, dan vragen wij u aan te geven per wanneer de onderneming is ingeschreven als vrijgestelde betaaldienstverlener in het openbaar register van DNB. Indien u wel actief bent als betaaldienstverlener, maar niet bent ingeschreven als vrijgestelde betaaldienstverlener, dan vragen wij u dit toe te lichten. Als u al over een vergunning beschikt voor betaalinstelling vragen wij u aan te geven, op welke betaaldiensten uw huidige vergunning ziet.

1.4 Reeds onder financieel toezicht van andere (buitenlandse) toezichthouder

Graag willen wij ook weten of uw onderneming al onder financieel toezicht staat van een andere (buitenlandse) toezichthouder. Indien dat het geval is, vragen wij u toe te lichten om wat voor financiële activiteiten het gaat, welk land het betreft en wie uw toezichthouder is.

Ook indien u eerder onder financieel toezicht van een (buitenlandse) toezichthouder stond en dit niet meer het geval is, vragen wij u dit aan te geven en toe te lichten.

1.5 Voorwaarden vergunningaanvraag

Een betaaldienstverlener is een onderneming die zijn bedrijf maakt van het verlenen van betaaldiensten. Deze definitie volgt uit artikel 1:1 van de Wet op het financieel toezicht (Wft). Hierbij gaat het om diensten die worden verleend aan de betaler (consument) en/of de betalingsdienstgebruiker (winkelier). De betaaldienstverlener vervult daarbij een intermediaire rol.

Om vast te stellen of een onderneming gekwalificeerd kan worden als betaaldienstverlener zijn de volgende afwegingen van belang.

1. Zijn de voorgenomen activiteiten te kwalificeren als een betaaldienst? Let hierbij op dat de Wft een aantal diensten specifiek niet aanmerkt als betaaldienst. Dit zijn diensten die zijn uitgezonderd van de vergunningplicht.
2. Is de onderneming voornemens 'het bedrijf uit te oefenen'* van het verlenen van betaaldiensten?
3. Valt uw onderneming onder de Vrijstellingsregeling?

Is één van de wettelijke uitzonderingen van toepassing?

De wet zondert specifiek een aantal diensten uit die zich daardoor niet kwalificeren als betaaldienst. In artikel 1:5a, tweede lid Wft staan deze uitzonderingen opgesomd. Denk hierbij bijvoorbeeld aan de handelsagentuitzondering of de beperkte netwerk-uitzondering. Zie de Q&A's op Open Boek Toezicht voor een toelichting op die uitzonderingen.

Verleent uw onderneming betaaldiensten als bedoeld in artikel 1:1 van de Wft?

U stelt eerst vast of de onderneming volgens de Wft (artikel 1:1) daadwerkelijk een betaal-dienstverlener is. Er zijn 8 verschillende soorten betaaldiensten. Deze betaaldiensten kunnen zowel zelfstandig als in combinatie met elkaar worden aangeboden.

Het onderscheid tussen de verschillende betaaldiensten wordt gemaakt op basis van de bijlage bij de herziene Richtlijn betaaldiensten (EU) 2015/2366 (hierna PSD2), waarnaar de Wft verwijst.

1. Diensten waarmee de mogelijkheid wordt geboden contanten te plaatsen op een door de betaaldienstverlener aangehouden betaalrekening, en alle verrichtingen die vereist zijn voor het exploiteren van een betaalrekening. Bij deze dienst gaat het om de mogelijkheid om contanten (munten of bankbiljetten) te plaatsen op een betaalrekening bij de aanbieder van deze dienst.
2. Diensten waarmee de mogelijkheid wordt geboden contanten van een betaalrekening op te nemen, en alle verrichtingen die vereist zijn voor het beheren van een betaalrekening. Bij deze dienst gaat het om de mogelijkheid om (giraal) geld, dat wordt aangehouden op een betaalrekening bij de aanbieder van de dienst, in contanten op te nemen.

- 6
3. Diensten waarmee betalingstransacties, inclusief geldovermakingen, worden uitgevoerd op een betaalrekening bij de betaaldienstverlener van de gebruiker of bij een andere betaaldienstverlener:
 - Uitvoering van automatische debiteringen, inclusief eenmalige
 - Uitvoering van betalingstransacties via een betaalkaart of vergelijkbaar betaalinstrument
 - Uitvoering van overmakingen, inclusief automatische betalingsopdrachtenDeze dienst betreft het verrichten van betalingstransacties op betaalrekeningen van de betaaldienstgebruikers, bedoeld in de omschrijving van de diensten 1 en 2, of op betaalrekening van betaaldienstgebruikers bij een andere betaaldienstverlener. Hieronder valt ook een onderneming die als dienst de mogelijkheid biedt om contant geld op te nemen en/of te storten via een afstort- of geldautomaat, waarbij de tegenwaarde wordt af- of bijgeschreven op een betaalrekening.
 4. Diensten waarmee betalingstransacties worden uitgevoerd waarbij de geldmiddelen zijn gedekt door een kredietlijn die aan de betaaldienstgebruiker wordt verstrekt:
 - Uitvoering van automatische debiteringen, inclusief eenmalige
 - Uitvoering van betalingstransacties via een betaalkaart of vergelijkbaar betaalinstrument
 - Uitvoering van overmakingen, inclusief doorlopende opdrachtenBij een kredietlijn kunt u denken aan de situatie waarbij het te betalen bedrag door de betaaldienstverlener wordt voorgesloten.
 5. Diensten waarmee betaalinstrumenten worden uitgegeven of aanvaard.

Een betaalinstrument is een middel of methode waarmee een opdracht tot betaling kan worden gegeven. Een betaalinstrument kan ook een fysiek voorwerp zijn, zoals een pas (bijvoorbeeld een creditcard). Van aanvaarding van een betaalinstrument is sprake als een onderneming instaat voor de afwikkeling van transacties via een betaalinstrument door middel van een overeenkomst met de begunstigde (bijvoorbeeld een webwinkel); de entiteit in kwestie (de acquirer) zorgt voor betaling aan de begunstigde op basis van de ontvangen betaalopdrachten. Bij ondernemingen die aan (web)winkeliers diensten verlenen voor de acceptatie van betaalmiddelen, is bijvoorbeeld sprake van dienst 5.
 6. Geldtransfers (moneytransfers)

Van geldtransfers is sprake als een betaalinstelling van een betaler geld ontvangt met als enig doel het daarmee corresponderende bedrag over te maken rechtstreeks aan een begunstigde of aan een andere betalingsdienstverlener die de gelden aan de uiteindelijk begunstigde uitkeert. Hierbij wordt geen rekening op naam van de betaler geopend. Geldtransfers worden in de praktijk vooral verleend voor het overmaken van geld naar begunstigten in het buitenland. Met name naar landen met een minder ontwikkeld banksysteem en waar het gebruik van bankrekeningen minder voorkomt. Ook voor onverwachte spoedbetalingen wordt van geldtransfers gebruikgemaakt.

7. Het initiëren van een betaalopdracht op verzoek van de betaaldienstgebruiker, met betrekking tot een betaalrekening die bij een ander betaaldienstverlener wordt aangehouden.
8. Het verstrekken van geconsolideerde informatie over een of meer betaalrekeningen die de betaaldienstgebruiker bij een andere betaaldienstverlener of bij meer dan één betaaldienstverlener aanhoudt.

Wij verzoeken u hier samen met een juridisch adviseur goed naar te kijken.

Wij vragen u in het aanvraagformulier om aan te geven of u voornemens bent om te bemiddelen in producten en diensten. Voor het bemiddelen in financiële producten is doorgaans een vergunning van de AFM nodig. Kijk voor meer informatie op www.afm.nl.

In het aanvraagformulier worden een aantal controlevragen gesteld, om er zeker van te zijn dat u een vergunning voor de juiste betaaldiensten aanvraagt en of u niet ook een aanvullende vergunning nodig heeft. Het betreft de volgende vragen.

1. Is uw onderneming op enig moment voornemens om te bemiddelen in (financiële) producten of diensten?
2. Is uw onderneming op enig moment voornemens om krediet te verschaffen?
3. Komt de onderneming bijvoorbeeld op enig moment in het beheer van derdengelden?

Biedt uw onderneming de betaaldiensten bedrijfsmatig aan?

Een onderneming is vergunningplichtig als de betaaldiensten die zij verleent bedrijfsmatig worden verricht. Het aanbieden van diensten aan verschillende klanten is een aanwijzing dat die diensten bedrijfsmatig worden aangeboden. Er is in ieder geval sprake van een vergunningplichtige betaaldienst indien u deze dienst actief aanbiedt, bijvoorbeeld doordat u reclame maakt. Gaat het om het eenmalig of zeer incidenteel aanbieden van betaaldiensten, dan kwalificeert een onderneming zich niet als betaaldienstverlener.

Mocht u twijfels hebben over de juridische kwalificatie van de door u voorgenomen activiteiten dan adviseren wij u om zich daarover te laten adviseren door een juridisch expert.

2 Business case

8

2.1 Bedrijfsplan

Bij de vergunningaanvraag overlegt u namens de onderneming een bedrijfsplan (o.a. programma van werkzaamheden). Hierbij levert u ook een budgetprognose voor de eerste drie boekjaren aan waarmee u aantoont gebruik te maken van passende en evenredige systemen, middelen en procedures die u in staat stellen op een (financieel) gezonde basis te werken.

U mag het bedrijfsplan en budgetprognose geïntegreerd aanleveren. Let daarbij op de samenhang met de aan te leveren templates onder hoofdstuk 11 Minimum eigen vermogen en solvabiliteit. DNB verwacht echter wel dat u in ieder geval onderstaande elementen aanlevert:

- Een schematisch overzicht van de activiteiten van de onderneming uitgewerkt per betaaldienst en de wijze waarop de betaaldiensten zullen worden verricht. DNB ontvangt tevens graag een opgave van overige activiteiten van de onderneming (ook van de niet-vergunningplichtige activiteiten).
- Een beschrijving van eventuele aanvullende diensten en/of nevendiensten zoals genoemd in artikel 18, lid 1 van de PSD2. Nevendiensten hebben betrekking op diensten die zijn gerelateerd aan de betaaldiensten. Hierbij dient u ook in te gaan op eventuele ambities om de komende drie jaar dergelijke activiteiten te verrichten.
- De strategie van de onderneming, waarbij de volgende aspecten aan de orde komen:
 - Het beoogde marktaandeel per betaaloplossing.
 - De beoogde herkomst van de betaaldienstgebruikers.
 - De groeiambities inclusief onderbouwing.
 - Sterkte-zwakke analyse (SWOT).
 - Uitbesteding van processen.
 - De partners (bijvoorbeeld acquirers, aanbrengrers van klanten, e.d.).
- Wanneer beschikbaar, voor bestaande ondernemingen, gecertificeerde jaarrekeningen over de voorgaande drie jaar of, voor ondernemingen die nog geen jaarrekeningen hebben opgesteld, een samenvatting van de financiële situatie.
- Een vertaling van de strategie naar een budgetprognose van minimaal drie jaar (lopende boekjaar en drie daaropvolgende boekjaren) met een volledige winst- en verliesrekening en een balans. Tevens moeten daarbij de volgende aspecten zijn uitgewerkt:
 - Het verwachte eigen vermogen van de onderneming in samenhang met de aan te leveren templates onder hoofdstuk 11 Minimum eigen vermogen en solvabiliteit.
 - De gehanteerde aannames / rekenprijzen die ten grondslag liggen aan de financiële prognose zoals investeringskosten, uitbestedingskosten, bestuurskosten, fees en marktaandeel.

1 Dit is een analyse van de sterke en zwakke kanten van uw onderneming zodat op een overzichtelijke manier duidelijk wordt gemaakt (via een matrix) of de door u voorgenomen diensten potentie hebben om succesvol te worden. S = Strengths, W = Weaknesses, O = Opportunities, T = Threats. Op basis van een SWOT-analyse kunt u een doel stellen en vervolgens een strategie bepalen om het doel te behalen.

- Verschillende (stress)scenario's waarmee u aantoont dat de business case van uw onderneming robuust genoeg is om ook bij tegenvallende resultaten en/of omstandigheden aan uw verplichtingen te kunnen voldoen.
- Het beleid van de onderneming ten aanzien van de waarborgen van de continuïteit van de onderneming in normale, matig tegenvallende en zwaar tegenvallende omstandigheden, zie ook herstelplan.
- Een gedetailleerde specificatie van de geraamde inkomende en uitgaande kasstromen – uw liquiditeitspositie – voor de komende drie jaren, bij voorkeur ook grafisch weergegeven.
- Een marketingplan inclusief een analyse van de concurrentiepositie van de onderneming, een beschrijving van de gebruikers per betaaldienst en een beschrijving van de verwachte marketinginspanningen en distributiekkanalen.
- Een inschatting en beschrijving van de verschillende locaties van waaruit de onderneming de betaaldiensten en daaraan gerelateerde activiteiten wil uitvoeren.

2.2 Stroomschema gelden

Indien uw onderneming uitsluitend dienst 7 en/of 8 aanbiedt, is dit onderdeel niet van toepassing.

Omdat het bij de beoordeling van uw vergunningaanvraag van belang is om te weten hoe de geldstromen lopen, verzoeken wij u om de verschillende geldstromen per betaaldienst in kaart te brengen. Wij vragen u daarom om een schematisch overzicht (stroomschema) van de geldstromen in te dienen, waarbij u tevens het aantal transacties per betaaloplossing en de verwerkingstijden (processing times) aangeeft alsmede welke partijen hierbij betrokken zijn.

2.3 Herstel- en exitplan

U stelt een herstelplan op waarin u laat zien hoe u in staat zult zijn te herstellen in zorgelijke financiële omstandigheden. Daarom voorziet een herstelplan in ieder geval in maatregelen om de verslechtering tijdig vast te stellen en om tijdig te herstellen. Het doel hiervan is uw instelling terug te laten keren naar een stabiele financiële situatie. Daarnaast stelt u een exitplan op om tijdig te kunnen anticiperen op eventuele beëindiging of overdracht van de betaaldienstactiviteiten of onderneming. Het doel daarvan is dat, indien afwikkeling zich daadwerkelijk voordoet, de geldmiddelen beheerst en met zo min mogelijk nadelige gevolgen voor de betaaldienstgebruikers en andere rechthebbenden kunnen worden uitbetaald of doorbetaald en dat relevante data wordt gewist. Hoewel het herstelplan en het exitplan een verschillend doel hebben, mogen ze worden geïntegreerd in één plan. U hoeft dan maar één document op te loaden. In het vervolg van deze paragraaf wordt dan ook de term herstel- en exitplan gehanteerd. Het herstel- en exitplan moet uiteraard aansluiten op uw bedrijfsplan.

10 Het herstel- en exitplan dient zich te richten op alle bedrijfsactiviteiten, producten en processen van de onderneming. Het plan heeft een duidelijke eindverantwoordelijke binnen de onderneming (eigenaar) en wordt vooraf door het bestuur en – indien aanwezig – het toezichthoudend orgaan van de instelling goedgekeurd en wordt periodiek geëvalueerd. Dit wordt ook in het plan vermeld. Proportionaliteit is het algemene uitgangspunt bij het opstellen van het herstel- en exitplan en als onderneming bepaalt u in beginsel zelf welke mate van detaillering gepast is.

In het kader van het themaonderzoek naar de herstel- en exitplannen van betaalinstanties heeft DNB guidance gegeven voor het opstellen van deze plannen. Deze guidance is te vinden op Open Boek (<http://www.toezicht.dnb.nl/binaries/50-236219.pdf>). Het herstel- en exitplan heeft minimaal de elementen zoals gepresenteerd in deze guidance. Daarnaast moet in het exitplan specifiek ingegaan worden op een beheerste omgang met data van betaaldienstgebruikers bij afwikkeling van de instelling.

Tot slot heeft DNB een 'good practice' opgesteld. Deze good practice bevat additionele inzichten naar aanleiding van eerder ingediende herstel- en exitplannen van betaalinstanties. Dit kan dienen ter inspiratie bij het opstellen van het herstel- en exitplan. Voor deze good practice verwijzen wij u ook naar Open Boek (<http://www.toezicht.dnb.nl/binaries/50-236731.pdf>).

3 Inrichting bedrijfsvoering voor beheerste uitoefening van het bedrijf

De bedrijfsvoering van uw onderneming zal zodanig ingericht moeten worden dat deze een beheerste en integere uitoefening van het bedrijf waarborgt. Dit houdt in dat u een analyse maakt van de risico's van de bedrijfsvoering en maatregelen treft om die risico's te mitigeren.

11

Werkt u met een stichting derdengelden ter bescherming van de gelden van de betaaldienstgebruikers, dan moet ook deze stichting derdengelden in deze risicoanalyse worden betrokken. Ook activiteiten die zijn uitbesteed moet u meenemen in de risicoanalyse.

DNB kijkt in het kader van de beoordeling van beheerste uitoefening van het bedrijf onder meer naar de volgende onderdelen.

- Risicoanalyse ten behoeve van beheersing van bedrijfsprocessen en bedrijfsrisico's.
- Risicobeheersingskader.
- En duidelijke, evenwichtige en adequate organisatiestructuur.
- Compliancefunctie.
- Interne controlefunctie.
- Procedurehandboek.
- Accountantscontrole.
- Internationale dienstverlening.
- Informatiesystemen, infrastructuur en beveiliging.
- Authenticatie.
- Veilige communicatie.
- Datacollectie.
- Uitbesteding.
- Omgang met incidenten.
- Bedrijfscontinuïteitsbeheer (business continuity management).
- Beheerst beloningsbeleid.
- Eed of belofte.
- Training en opleiding.

Wij lichten deze punten hieronder voor u toe.

3.1 Risicoanalyse ten behoeve van beheersing van bedrijfsprocessen en bedrijfsrisico's

Om vast te kunnen stellen in hoeverre de inrichting van de bedrijfsvoering van uw onderneming passend is bij de risico's die uw onderneming loopt, dient u een actuele en uitgebreide beoordeling te verstrekken van de risico's die aan uw onderneming en aan de door uw onderneming aangeboden diensten verbonden zijn. Ook dient u daarbij de toereikendheid te beoordelen van de in reactie op deze risico's getroffen risicobeperkende

12 maatregelen en ingevoerde controlemechanismen. De hiertoe uit te voeren en aan te leveren risicoanalyse dient te worden opgesteld conform het door uw onderneming ontworpen risicobeheersingskader.

Het beheerst uitoefenen van het bedrijf van betaaldienstverlener begint bij het identificeren van de risico's. Deze risicoanalyse is een startpunt en een voorwaarde voor een toereikende inrichting van de beheerste bedrijfsvoering. De analyse moet herleidbaar zijn, dus vastgelegd in een apart document, en het restant van uw risicobeheersingskader is mede gebaseerd op de uitkomsten van de risicoanalyse. U hanteert hierbij een begrijpelijke kwantificeringsmethode. De risicoanalyse gaat uit van bruto (inherente) en netto (rest) risico's en gaat in op de kans en impact van deze risico's. De omvang van de netto risico's en het effect van de maatregelen en procedures zijn realistisch ingeschat. Denk bij het analyseren van de netto risico's ook aan een vergelijking met de risicobereidheid van uw instelling. Daarover meer in de paragraaf Risicobeheersingskader.

De risicoanalyse bevat minimaal een analyse van de relevante risico's voor uw onderneming. Denk daarbij aan de deze risicocategoriën: kredietrisico's, marktrisico's, renterisico's², concentratierisico's, liquiditeitsrisico's, operationele risico's (inclusief IT risico's en uitbestedingsrisico's) en verzekeringsrisico's, integriteitsrisico's (voor de vergunningaanvraag aan te leveren in een aparte analyse (SIRA) bij het onderdeel Inrichting bedrijfsvoering voor integere uitoefening van het bedrijf). Vervolgens dient u per risicocategorie in te gaan op de onderliggende risico's. Daarbij moet uit de analyse blijken met welke beheersmaatregelen de onderneming dit verhoogde risico compenseert, wanneer een hoog bruto risico wordt gedefinieerd. In het bijzonder moet u ingaan op uw betalingsdiensten en een beschrijving van de maatregelen op het gebied van beveiliging en risicobeperking die worden genomen om de gebruikers van de betalingsdiensten afdoende tegen de vastgestelde beveiligingsrisico's, waaronder fraude en illegaal gebruik van betaalgegevens, te beschermen. Hiertoe stelt u ook een beveiligingsbeleid op, zie paragraaf 3.10.

Uit de procedures en maatregelen moet een duidelijke samenhang blijken met de specifieke risico's die in de risicoanalyse zijn geïdentificeerd. De beheersmaatregelen die u heeft ingericht of gaat inrichten zijn herleidbaar toegesneden op de aard, omvang, complexiteit en het risicoprofiel van de werkzaamheden van uw onderneming én voldoen aan de hiervoor gestelde minimale vereisten.

2 De procedures en maatregelen voor beheersing van het liquiditeitsrisico hebben betrekking op het beheer van de actuele en toekomstige netto financiële positie en behoeften.

3.2 Risicobeheersingskader

Graag ontvangen wij een beschrijving van het risicobeheersingskader van uw onderneming. In dit beleidsdocument dient u onder meer in te gaan op beleid, inclusief een beschrijving van de risicobereidheid, van uw onderneming, dat u voert gericht op het beheersen van relevante risico's. Ook dient u daarbij in te gaan op de opzet en inrichting van de risicobeheersingsfunctie en hoe u ervoor zorgt dat het beleid wordt vastgelegd in procedures en maatregelen ter beheersing van relevante risico's en geïntegreerd in de bedrijfsprocessen (zie ook Procedurehandboek). Daarbij ontvangen wij graag een onderbouwing dat uw onderneming met dit risicobeheersingskader een beheerste uitoefening van het bedrijf kan waarborgen. Wij verwachten ook dat de overige onderdelen binnen dit hoofdstuk over de beheerste bedrijfsvoering in overeenstemming zijn met het risicobeheersingskader van uw onderneming.

Wij verwachten dat uw onderneming het beleid heeft ingericht op het beheersen van relevante risico's en in lijn met de risicobereidheid. Daartoe is het van belang een beschrijving van de risicobereidheid van uw onderneming per risicogebied op te stellen. Denk daarbij onder meer aan kredietrisico's, marktrisico's, renterisico's, valutarisico's, concentratierisico's, liquiditeitsrisico's, operationele risico's (inclusief IT risico's en uitbestedingsrisico's) en verzekeringsrisico's.

U legt het beleid ten aanzien van de risicobeheersing vast in procedures en maatregelen. Deze procedures en maatregelen zijn afgestemd op de aard, omvang, het risicoprofiel en de complexiteit van de werkzaamheden van de onderneming en beslaan minstens de volgende vier gebieden:

- Autorisatieprocedures.
- Limietstellingen.
- Limietbewaking.
- Procedures en maatregelen voor noodsituatie.

De concrete uitwerking van de procedures en maatregelen moet duidelijk zijn vastgelegd, bijvoorbeeld in het procedurehandboek (zie paragraaf 3.6). Ze worden op een eenduidige wijze, bij voorkeur schriftelijk, gecommuniceerd aan alle bedrijfsonderdelen van de betaalinstantie waarop de risico's betrekking kunnen hebben.

Uw onderneming dient te beschikken over een onafhankelijke risicomanagement- / risicobeheersingsfunctie die op systematische wijze het risicomanagement voor uw onderneming verzorgt. Dat risicomanagement is gericht op het identificeren, meten en evalueren van de risico's waaraan uw betaalinstantie is of kan worden blootgesteld. Het risicomanagement wordt uitgevoerd zowel ten aanzien van de onderneming als geheel, als ten aanzien van de onderscheiden bedrijfsonderdelen. De risicomanagement- / risicobeheersingsfunctie beschikt over de nodige autoriteit en toegang tot alle noodzakelijke

14

informatie om haar taken te kunnen uitoefenen. Wij verwachten dat een toelichting op de inrichting van de risicomanagement-/risicobeheersingsfunctie is opgenomen in de beschrijving van het risicobeheersingskader. Wij verwachten daarbij ook een toelichting op de periodieke en permanente controlemaatregelen inclusief de frequentie daarvan en de capaciteit (in fte en/of EUR) die uw onderneming daarvoor beschikbaar maakt.

Voor de beheersing van operationele (IT) en beveiligingsrisico's dient u een doeltreffend kader voor de beheersing van operationele en beveiligingsrisico's te creëren, dat eveneens minstens één keer per jaar goedgekeurd en gecontroleerd moet worden door het leidinggevend orgaan en, indien nodig, door de directie. Deze regeling dient te voorzien in beveiligingsmaatregelen om de operationele en beveiligingsrisico's te beperken en moet volledig geïntegreerd worden in de allesomvattende risicobeheersingsprocessen van de betalingsdienstaanbieder. Later in dit hoofdstuk meer over het beheersen van operationele (IT) en beveiligingsrisico's.

3.3 Een duidelijke, evenwichtige en adequate organisatiestructuur

Uw onderneming moet bij de inrichting van haar bedrijfsvoering voor een beheerste uitoefening van het bedrijf (inclusief de stichting derdengelden indien daarvan sprake is) de volgende zes uitgangspunten hanteren:

- Uw onderneming beschikt over een duidelijke, evenwichtige en adequate organisatiestructuur.
- Uw onderneming kent een duidelijke, evenwichtige en adequate verdeling van taken, bevoegdheden en verantwoordelijkheden (governance).
- Rechten en verplichtingen van en binnen uw onderneming zijn adequaat vastgelegd.
- Uw onderneming kent eenduidige rapportagelijnen.
- Uw onderneming heeft een adequaat systeem van informatievoorziening en communicatie.
- Uw onderneming heeft de bedrijfsvoering op inzichtelijke wijze vastgelegd en toetst deze regelmatig.

Uw onderneming moet op alle niveaus en voor alle onderdelen een duidelijke, evenwichtige en adequate verdeling van taken en bevoegdheden hebben. De rapportagelijnen moeten hiermee in overeenstemming zijn.

De taakverdeling en de rapportagelijnen dienen op zodanige wijze te zijn vastgelegd en gecommuniceerd dat alle geledingen van uw onderneming een goed begrip hebben van hun taken, bevoegdheden en verantwoordelijkheden, hun rol in de organisatie en het beheersingsproces en de manier waarop zij verantwoording afleggen.

Bij gesignaleerde tekortkomingen en gebreken draagt u er zorg voor dat de organisatie-inrichting en de procedures en maatregelen zodanig worden bijgesteld dat deze tekortkomingen worden opgeheven. Bij een onderneming met een directeur-groootaandeelhouderstructuur (DGA-structuur) of een internationaal complexe groeps- en/of organisatiestructuur is bijzondere aandacht voor een evenwichtige corporate governance op zijn plaats. Indien daarvan sprake is, verwachten wij dat u dit nader toelicht.

DGA-structuur

Wij vragen u in het aanvraagformulier expliciet aan te geven of er sprake is van een DGA-structuur of een daarmee vergelijkbare zeggenschapsstructuur. De governance ziet in algemene zin op een verdeling van taken, verantwoordelijkheden en bevoegdheden gericht op een evenwichtige invloed van bij de vennootschap en haar onderneming direct betrokkenen, waaronder met name bestuurders, commissarissen en kapitaalverschaffers. Van belang is dat binnen de onderneming voortdurend sprake is van een deskundige en evenwichtige bedrijfsvoering met adequate checks and balances en juiste prikkelwerking.

DNB verstaat onder een DGA-structuur de situatie dat een natuurlijk persoon zowel (indirect) groot aandeelhouder als bestuurder is. In een dergelijke situatie kan een DGA, wanneer adequaat tegenwicht binnen de onderneming ontbreekt (checks and balances), een onwenselijk grote invloed hebben op de gang van zaken binnen de onderneming. De DGA kan bijvoorbeeld in de positie komen om het eigen (aandeelhouders)belang boven het (lange termijn)belang van de vennootschap of andere betrokkenen (stakeholders) te plaatsen. Afgezien van mogelijke belangenconflicten, bestaat tevens het risico dat een DGA zich in een zodanige mate vereenzelvigd met zijn onderneming, dat de DGA niet in staat is om in zijn hoedanigheid van bestuurder de vereiste objectiviteit en onafhankelijkheid aan de dag te leggen en te waarborgen, bijvoorbeeld als een onderneming in een kritische situatie komt te verkeren.

Of een DGA-structuur al dan niet toelaatbaar is, hangt af van de omstandigheden van het geval. Indien er binnen uw onderneming sprake is van een dergelijke structuur moet u in uw vergunningaanvraag goed onderbouwen dat u de kwetsbaarheden die een dergelijke structuur met zich meebrengt voldoende heeft gemitigeerd. Denk bijvoorbeeld aan een raad van commissarissen of aan de aanwezigheid van adequate regelingen om in het geval van conflicterende belangen tussen de vennootschap en de aandeelhouder/bestuurder tot een weloverwogen besluit te kunnen komen.

International complexe organisatiestructuren

Ook voor internationaal complexe organisatiestructuren verwacht DNB expliciet een goede onderbouwing van de mogelijke risico's en bijbehorende beheersingsmaatregelen. Hierbij kan tevens het instellen van een raad van commissarissen als mitigerende maatregel worden gekozen. Bovendien geldt dat, indien uw onderneming onderdeel is

van een groep van ondernemingen, uw onderneming er verantwoordelijk voor is dat de beheersing van bedrijfsprocessen in die moederorganisatie goed aansluit op die van haar dochterondernemingen en andere ondernemingen die met uw onderneming in een formele of feitelijke zeggenschapsstructuur zijn verbonden. Op die manier wordt voorkomen dat afbreuk kan worden gedaan aan een beheerste bedrijfsvoering van uw onderneming.

Als uw onderneming beschikt over een raad van commissarissen of voornemens is een raad van commissarissen te installeren, dan is het van belang dat deze raad van commissarissen onafhankelijk kan functioneren. Zie voor een verdere toelichting hierop, <http://www.toezicht.dnb.nl/3/50-226002.jsp#>.

Organogram

Wij vragen u bij de aanvraag een actueel organogram aan te leveren waarin alle eventuele divisies, afdelingen of andere structuurvarianten zijn opgenomen. Wij verwachten dat u daarbij ook opneemt welke personen leiding geven aan de eventuele de divisies, afdelingen of andere structuurvarianten waarbij wij in het bijzonder aandacht vragen voor de personen die leiding geven aan de interne controle functies (risicobeheersingsfuncties, management (business), compliancefunctie, auditfunctie en (eventuele) afdelingen). Indien deze personen nog niet bekend zijn, ontvangen wij graag een concrete profielomschrijving voor deze functies. Het organogram dient te worden begeleid door een beschrijving van de functies en verantwoordelijkheden van de divisies, afdelingen of andere structuurvarianten. Ook verwachten wij een prognose van het totaal aantal medewerkers en fte's gedurende de komende drie jaar. Neem ook op in het organogram welke functies (mogelijk) worden uitbesteed en welke personen meerdere functies vervullen.

Functiescheiding

De taken, bevoegdheden en verantwoordelijkheden van zowel personen als afdelingen binnen uw onderneming moeten zodanig verdeeld zijn dat het risico van fouten en het oneigenlijke gebruik en/of oneigenlijk inzien van activa of gegevens wordt beperkt. Voorkomen moet bijvoorbeeld worden dat functies bevoegdheden omvatten waarbij één persoon ongecontroleerd transacties of verplichtingen kan aangaan, kan autoriseren, verwerken en afwikkelen, vrije toegang heeft tot activa of in staat is financiële en/of andere gegevens te manipuleren. Als u weining personeel in dienst heeft kan het uitdagend zijn om functiescheidingen te realiseren. Het alleen toelichten dat functiescheiding lastig te organiseren is in een kleine organisatie, volstaat niet. DNB verwacht dat u in een dergelijke situatie alternatieve maatregelen treft. Dat kan bijvoorbeeld door werkzaamheden uit te besteden aan een derde, wat het ontbreken van interne functiescheidingen kan compenseren. Uiteraard is het van belang voldoende in control te blijven en wij verwachten dan ook dat u bij de aanvraag duidelijk toelicht hoe u dat waarborgt. Zie ook paragraaf 3.8 (Uitbesteding).

3.4 Compliancefunctie

Uw onderneming moet beschikken over een organisatieonderdeel met een onafhankelijke en effectieve compliancefunctie. Een onafhankelijke compliancefunctie is van belang om toezicht te houden op de naleving van wettelijke regels en interne regels, voorschriften en procedures. Het toezien op de naleving van deze regels, voorschriften en procedures houdt bijvoorbeeld in het beoordelen van nieuwe wetgeving en het toetsen of nieuwe producten en procedures in overeenstemming zijn met de regelgeving. De wijze waarop deze functie wordt vormgegeven is afhankelijk van de aard en omvang van de betaalinstelling. Onafhankelijk betekent op z'n minst dat de compliancefunctie zich niet laat leiden door commerciële belangen. De taken en verantwoordelijkheden van de compliancefunctie worden in een compliance-charter vastgelegd en vervolgens worden de werkzaamheden nader uitgewerkt in een compliancejaarplan. Het meesturen van een compliance-charter en compliancejaarplan is niet verplicht, maar kan bijdragen aan een goede onderbouwing van de vergunningaanvraag.

Compliance-charter (optioneel)

In het compliance-charter kan onder andere het volgende worden opgenomen:

- Definitie en reikwijdte.
- Missie van compliance.
- Functieprofiel met daarbij de belangrijkste taken, bevoegdheden en verantwoordelijkheden van de compliance officer.
- De bijzondere positie van de compliancefunctie binnen de onderneming.
- Waarborging functiescheiding.
- De namen van de interne en/of externe compliance officer(s)/medewerker(s).

In het compliance-charter staan de verschillende rollen precies vermeld. Zo is duidelijk voor de gehele organisatie, maar ook voor externen zoals toezichthouders, wat van de compliancefunctie, van het management en van andere staffunctionarissen verwacht kan worden op het gebied van het waarborgen van een beheerste en integere bedrijfsuitoefening.

Compliancejaarplan (optioneel)

Aan het compliancejaarplan ligt een risicoanalyse ten grondslag. Door een plan op te stellen wordt een zichtbare verantwoording van de te besteden capaciteit gepresenteerd. Het jaarplan stemt de compliancefunctie af met het management. Ook zorgt de compliancefunctie ervoor dat eventuele andere stakeholders instemmen met de inhoud van het plan.

3.5 Interne controlefunctie

Uw organisatie moet beschikken over een organisatieonderdeel dat een interne controlefunctie uitoefent. Deze interne controlefunctie moet de effectiviteit van de organisatie-inrichting en van de procedures en maatregelen binnen uw onderneming onafhankelijk toetsen.

Met onafhankelijk wordt hier bedoeld: onafhankelijk van het lijnmanagement en los van de controlemaatregelen die in de diverse bedrijfsprocessen zijn geïntegreerd.

Onafhankelijke interne toetsing is een continu proces, waarbij rekening wordt gehouden met veranderende interne en externe omstandigheden, nieuwe producten, diensten en ondersteunende processen, en dient ten minste jaarlijks te worden uitgevoerd. Daarbij is het ook belangrijk dat u toelicht hoe uw onderneming ervoor zorgt dat als er tekortkomingen worden gesignaleerd, deze worden opgeheven.

Zoals u bij de toelichting onder accountantscontrole (3.7) en uitbesteding (3.8) kunt lezen, kunt u de interne controlefunctie uitbesteden. DNB verwacht dan wel dat u dat adequaat toelicht. Ook verwacht DNB dat u bij deze toelichting ingaat op het jaarplan met de uit te voeren controlewerkzaamheden.

3.6 Het procedurehandboek

Het risicobeheersingskader, de organisatiestructuur, de compliancefunctie en de interne controlefunctie vormen belangrijke onderdelen van de inrichting van de bedrijfsvoering ten behoeve van een beheerste uitoefening van uw bedrijf. De algemene inrichting van uw bedrijfsvoering is echter ook van belang. Daartoe dient u de uitwerking van de algemene procedures en maatregelen van uw onderneming ter ondersteuning van de beheerste uitoefening van uw bedrijf in één helder en eenvoudig toegankelijk document op te nemen en aan te leveren: het procedurehandboek. In het procedurehandboek wordt de opzet (het beleid van uw onderneming) vertaald naar concrete procedures en maatregelen voor de bedrijfsvoering. Daarin staan ook de verschillende procedures voor de uitvoering van periodieke en permanente controles opgenomen, met de frequentie en het hieraan toegewezen personeel in lijn met het risicobeheersingskader van uw onderneming. Dit betekent dat als u in de voorgaande documenten nog niet in detail bent ingegaan op de procedures en maatregelen volgend uit of behorend bij het risicobeheersingskader, de organisatiestructuur, de compliancefunctie en/of de interne controlefunctie, u daar in het procedurehandboek wel verder invulling aan moet geven.

U stelt een procedurehandboek op om het beleid van uw onderneming te vertalen naar praktische procedures en maatregelen. In een procedurehandboek neemt u op hoe uw onderneming de administratieve organisatie heeft ingericht. Hiermee bedoelen we het systematisch verzamelen, vastleggen en verwerken van gegevens voor drie onderdelen van uw bedrijfsvoering.

- Het besturen van een betaalinstelling.
- Het doen functioneren van een betaalinstelling.
- Het afleggen van verantwoording daarover.

Een procedurehandboek dient de volgende doelstellingen:

1. Inzicht: het verschaft inzicht in de structuur van de administratieve organisatie. In het procedurehandboek is daartoe geformuleerd hoe processen zijn georganiseerd en volgens welke richtlijnen moet worden gewerkt.
2. Basis voor efficiency en effectiviteit van processen: het procedurehandboek vormt de basis voor het realiseren van een administratieve organisatie (AO) gericht op efficiency en effectiviteit van processen.
3. Kennisoverdracht: bij het opleiden en het inwerken van nieuwe medewerkers kan het procedurehandboek als hulpmiddel worden gebruikt, terwijl door eenduidige omschrijving van processen een uniforme werkwijze in de organisatie kan worden bewerkstelligd.
4. Bevoegdheden en verantwoordelijkheden: de afbakening van verantwoordelijkheden en bevoegdheden binnen de processen is duidelijk vastgelegd. Door verantwoordelijkheden aan te wijzen (bijvoorbeeld 'tekenbevoegdheden') worden risico's beperkt.
5. Controle: het draagt bij aan een goede opzet en uitvoering van de interne controle.
6. Automatisering: het verschaft basisinformatie voor de automatisering, onder andere voor autorisaties.

3.7 Accountantscontrole

Dit onderdeel is niet van toepassing als uw onderneming uitsluitend dienst 8 aanbiedt.

Als uw onderneming een accountant de opdracht heeft gegeven tot het uitvoeren van een controle op de jaarrekening verwachten wij dat de opdracht tot onderzoek van de jaarrekening minimaal voorziet in een toetsing en beoordeling op hoofdlijnen met betrekking tot de toereikendheid van de organisatie-inrichting en risicobeheersing. De toetsing door de externe accountant moet ook gericht zijn op de beheersing van die risico's die een materiële invloed kunnen hebben op de financiële prestaties, financiële positie en continuïteit van de onderneming. De toetsing door de externe accountant wordt zoveel mogelijk geïntegreerd binnen het kader van onderzoek van de jaarrekening. In het verslag van de jaarrekening vermeldt de accountant ook zijn bevindingen over de bedrijfsvoering. Wij vragen u een kopie van de opdrachtovereenkomst bij uw vergunningaanvraag aan te leveren.

3.8 Uitbesteding

Omdat DNB toezicht moet kunnen houden op alle werkzaamheden en bedrijfsprocessen van uw onderneming (ook als die zijn uitbesteed) is het van belang dat DNB alle informatie kan ontvangen op grond waarvan zij kan beoordelen of alle werkzaamheden, dus ook de uitbesteede werkzaamheden, worden uitgevoerd volgens de wet.

Uw onderneming mag werkzaamheden uitbesteden voor zover dit geen belemmering vormt of kan vormen voor een adequate naleving van de regelgeving. Er zijn ook werkzaamheden die niet uitbesteed mogen worden, namelijk de taken en werkzaamheden van personen die het dagelijks beleid bepalen, waaronder het vaststellen van het beleid en het afleggen van verantwoording over het gevoerde beleid.

20

Een interne controlefunctie beschikt over vaktechnische deskundigheid, detailkennis van de structuur van de eigen organisatie en is permanent beschikbaar. Het uitbesteden van deze functie aan een niet met de betaalinstelling in een formele of feitelijke zeggenschapsstructuur verbonden onderneming zal daarom vaak een belemmering zijn voor het waarborgen van de kwaliteit van de interne controle. Dit betekent dat als een interne controlefunctie wordt uitbesteed, deze moet geschieden onder sturing en toezicht van de betaalinstelling. Uw onderneming moet altijd verantwoording kunnen afleggen over de opzet en werking van de bedrijfsvoering. Bij het bepalen welke derde de auditwerkzaamheden gaat uitvoeren en wie binnen de betaalinstelling verantwoordelijk is voor de sturing en het toezicht, is van belang dat het risico van belangenverstrengelingen expliciet wordt meegewogen.

Uitbestedingsbeleid

Uw onderneming voert een adequaat beleid en beschikt over procedures en maatregelen om werkzaamheden op structurele basis uit te besteden. Daarnaast beschikt uw onderneming over toereikende procedures, maatregelen, deskundigheid en informatie om de uitvoering van de op structurele basis uitbestede werkzaamheden te kunnen beoordelen. De onderneming legt te allen tijde de afspraken met de derde waaraan de werkzaamheden op structurele basis worden uitbesteed schriftelijk vast in een overeenkomst. Wij verwachten dat u het uitbestedingsbeleid aanlevert bij de aanvraag.

Bij het voeren van een adequaat beleid voor het op structurele basis uitbesteden van werkzaamheden is het van belang dat uw onderneming aandacht heeft voor de invloed van het uitbesteden van werkzaamheden op de beheerste uitoefening van het bedrijf. Hierbij kunt u denken aan procedures en maatregelen in geval van tekortschietende dienstverlening door de derde en calamiteiten. Het is van belang dat een betaalinstelling die werkzaamheden uitbesteedt, de risico's die daarmee samenhangen systematisch analyseert. Risicoanalyse is ook een essentieel element om op voorhand te beoordelen of de werkzaamheden wel of niet kunnen worden uitbesteed.

U stelt per dienstverlener een risicoanalyse op. In het handboek dient te beschrijven hoe het proces van het opstellen van een uitbestedingsrisicoanalyse plaats vindt en voor elke uitbesteding van wezenlijk belang dient u een risicoanalyse te overhandigen. Hiermee worden werkzaamheden bedoeld die als ze gebrekkig of tekortschietend uitgevoerd worden, wezenlijk afbreuk (kunnen) doen aan de naleving door de betaalinstelling van de vergunningvereisten, aan haar financiële resultaten of de soliditeit of continuïteit van haar betaaldiensten

Uitbestedingsovereenkomst

Voor een adequate beoordeling van de uitbestede werkzaamheden dient de (uitbestedende) ondernemer over voldoende informatie te beschikken van de onderneming waaraan de werkzaamheden zijn uitbesteed. Tevens beschikt de onderneming over de deskundigheid om die informatie te kunnen beoordelen.

In de uitbestedingsovereenkomst wordt in ieder geval het volgende geregeld:

De onderlinge informatie-uitwisseling, met inbegrip van afspraken over het beschikbaar stellen van informatie waarom de toezichthouders ter uitvoering van hun wettelijke taak verzoeken.

- De mogelijkheid voor de onderneming om te allen tijde wijzigingen aan te brengen in de wijze waarop de uitvoering van de werkzaamheden door de derde geschiedt.
- De verplichting voor de derde om de onderneming in staat te stellen blijvend te voldoen aan het bij of krachtens de wet bepaalde.
- De mogelijkheid voor de toezichthouders om onderzoek ter plaatse te doen of te laten doen bij de derde.
- De wijze waarop de overeenkomst wordt beëindigd en de wijze waarop gewaarborgd wordt dat de onderneming de werkzaamheden na beëindiging van de overeenkomst weer zelf kan uitvoeren of door een andere derde kan laten uitvoeren.

Indien sprake is van onder-uitbesteding (uitbesteding door de dienstverlener waaraan uw onderneming op haar beurt diensten heeft uitbesteed) dan zijn de hierboven beschreven eisen ook van toepassing.

Echter, indien sprake is van uitbesteding aan ondernemingen met zetel in een lidstaat die deel uitmaken van de groep waartoe uw onderneming behoort, is het niet vereist om daartoe over beleid, procedures en uitbestedingsovereenkomsten te beschikken. Wel moeten de werkzaamheden voldoen aan het vereiste van een beheerste bedrijfsvoering en verwacht DNB dat u duidelijk maakt hoe u met die uitvoering van de werkzaamheden in control bent.

DNB heeft ook aandacht voor de uitbesteding aan een cloud dienstverlener. Onder verwijzing naar de Cloud Circulaire (<http://www.toezicht.dnb.nl/2/5/50-230433.jsp#>) dient het gebruik van cloud-diensten altijd te worden gemeld, vanwege het concentratierisico.

Ten slotte moet de onderneming er bij de uitbesteding van werkzaamheden voor zorgen dat de uitbesteding niet van negatieve invloed is op de verplichtingen van de betaalinstanties tegenover haar cliënten en de wettelijke rechten van haar cliënten.

Op Open Boek Toezicht van DNB wordt eind 2018 meer gepubliceerd over uitbesteding. Hou daarom Open Boek Toezicht in de gaten.

3.9 Internationale dienstverlening

Betaalinstanties met zetel in Nederland kunnen in elke andere lidstaat van de Europese Economische Ruimte (EER) opereren op basis van de door DNB verleende vergunning, dus zonder dat zij in die andere lidstaat een vergunning hoeven aan te vragen. Wel moeten betaalinstanties hiervoor een notificatieprocedure bij DNB doorlopen. De achtergrond en de soorten notificaties vindt u op <http://www.toezicht.dnb.nl/2/50-224483.jsp>.

22

Vooruitlopend op eventuele internationale dienstverlening en voor een tijdige behandeling van eventuele notificaties vragen wij een overzicht van de wijze waarop de onderneming van plan is om op korte termijn internationale diensten te verlenen. Betrek in uw antwoord naar welke lidstaten en/of eventueel derde landen de onderneming voornemens is om activiteiten te verrichten. Beschrijf ook de wijze waarop eventuele agenten en/of bijkantoren worden gemonitord en gecontroleerd als onderdeel van de interne controle en beschrijf daarbij vooral ook de monitorings- en controleprocessen in het kader van financiële criminaliteit en naleving sanctiewetgeving. Indien de onderneming gebruik maakt van agenten verwacht DNB ook een beschrijving van de IT-systemen, processen en infrastructuur die de agenten gebruiken om namens de werkzaamheden uit te voeren.

3.10 Informatiesystemen, infrastructuur en beveiliging

De PSD2 vereist nadere aandacht voor de beheersing van operationele en beveiligingsrisico's. In deze en de hierna volgende paragrafen (3.10 tot en met 3.15) wordt ingegaan op de verwachtingen van DNB ten aanzien van de beheersing van deze risico's. Een overlap met andere onderwerpen uit dit hoofdstuk is hierbij onvermijdelijk. Dit betekent niet dat u bij uw aanvraag hetzelfde document meerdere keren dient aan te leveren. Wel moet u bij uw aanvraag duidelijk maken waar wij de gevraagde informatie kunnen vinden door duidelijke verwijzingen op te nemen.

Uw onderneming beschikt over een informatiesysteem en een informatie-infrastructuur ter ondersteuning van de bedrijfsprocessen en die voorzien in de interne en externe informatiebehoeften. De bijbehorende operationele- en beveiligingsrisico's moeten effectief worden beheerst. In dat kader is het bijvoorbeeld van belang dat het informatiesysteem en de informatie-infrastructuur erin voorzien dat transacties en boekingen in gegevensbestanden steeds herleidbaar zijn tot geautoriseerde brondocumenten of bewerkingen door daartoe geautoriseerde personen en/of geautoriseerde systemen.

De beheerste geautomatiseerde gegevensverwerking en de bijbehorende beheerste infrastructuur moeten een geïntegreerd onderdeel zijn van de onderneming en de geautomatiseerde gegevens dienen te voldoen aan de eisen behorend bij de aard van de werkzaamheden en de wettelijke eisen.

Een onderneming die gebruik maakt van geautomatiseerde gegevensverwerking en die geautomatiseerde diensten aanbiedt dient daarom maatregelen te treffen en te beschikken over procedures die de integriteit van de geautomatiseerde gegevensverwerking waarborgen, de gegevens beschermen tegen onrechtmatig inzien en /of verwerken en de beschikbaarheid van gegevens en de geautomatiseerde gegevensverwerking waarborgen.

De bij de aanvraag aan te leveren beschrijving van de maatregelen en procedures ten aanzien van het beheersen van operationele en beveiligingsrisico's moet ingaan op de volgende onderdelen.

- a. De IT strategie, het IT beleid en het beveiligingsbeleid van de onderneming.
- b. Het IT-landschap, de informatiesystemen en bijbehorende infrastructuur inclusief de interne en externe koppelingen.
- c. De informatiesystemen, infrastructuur onderdelen en koppelingen die als bedrijfskritisch worden geclassificeerd inclusief de classificatie criteria en de motivatie.
- d. Het operationele en beveiligingsrisico's raamwerk: het risicobeheersingskader.
- e. Het risico- en beheersingsmodel inclusief gedetailleerde risicoanalyse.
- f. De identificatie, classificatie van bedrijfsfuncties, processen en resources met aandacht voor de beschikbaarheid, de Integriteit en de vertrouwelijkheid van systemen, infrastructuur, data en processen.
- g. De beschermingsmaatregelen om zowel data, informatiesystemen en informatie infrastructuur te beschermen als de integriteit van informatiesystemen, infrastructuur en data te waarborgen, inclusief beveiligingsmaatregelen, logische en fysieke toegangsbeveiliging, en een eventuele gelaagdheid in beschermingsmaatregelen.
- h. Het continu monitoren / detecteren van interne en externe bedreigingen en kwetsbaarheden die van impact kunnen zijn voor de informatiesystemen en de informatie-infrastructuur en hoe hiermee wordt omgegaan.
- i. Het beleid, het proces met bijbehorende procedures en de uitwerking hiervan met betrekking tot logische toegangsbeveiliging waarbij onder meer inzicht wordt gegeven hoe de organisatorische functiescheiding is gerealiseerd in de logische toegangsbeveiliging tot data, informatiesystemen en informatie-infrastructuur.
- j. Het continue controleren op afwijkingen en ongewenste activiteiten in de informatiesystemen en de informatie-infrastructuur.
- k. Het testen van de getroffen beveiligingsmaatregelen om de robuustheid en effectiviteit van de maatregelen te bepalen inclusief het regelmatig uitvoeren van een scan op kwetsbaarheden en een penetratietest (minimaal jaarlijks).
- l. Het proces en bijbehorende procedures voor het wijzigen van informatiesystemen, informatie-infrastructuur en de getroffen beveiligingsmaatregelen inclusief het doorvoeren van ongeplande wijzigingen op zeer korte termijn (zogenaamde emergency changes).
- m. Het proces waarmee continu inzicht wordt verkregen in de beveiligings- en operationele kwetsbaarheden binnen de IT en de financiële sector, die van impact kunnen zijn voor de eigen informatiesystemen en de informatiestructuur en het (indien nodig) delen van geconstateerde kwetsbaarheden met de sector.
- n. Het onderrichten (opleiden) van medewerkers op het gebied van (informatie) beveiliging.
- o. Het informeren van de gebruikers / klanten over (informatie) beveiliging.
- p. Het proces en bijbehorende procedures van maatregelen om data op een veilige manier te delen en het op een veilige manier versturen van verplichtte rapportages.
- q. Het proces van een onafhankelijk toetsing van de beveiligingsmaatregelen, uitgevoerd door auditors met deskundigheid op het gebied van IT beveiliging en betalingen en die operationeel onafhankelijk zijn binnen of ten opzichte van uw organisatie.

3.11 Authenticatie

Authenticatie dient om de identiteit van betaaldienstgebruikers en derden vast te stellen. Indien uw organisatie direct contact heeft met betaaldienstgebruikers past u sterke cliëntauthenticatie toe. Deze authenticatie is gebaseerd op twee of meer elementen die als kennis, bezit en inherentie (iets wat men weet, bezit of is) worden gekwalificeerd en die resulteren in het genereren van een authenticatiecode.

Het procedurehandboek gaat in op de volgende punten:

- De wijze van het gebruik en de beheersing van deze cliëntauthenticatiemiddelen
- De ondersteunende processen en middelen (hardware en software)
- De bescherming van de authenticatiecode in overeenstemming met de verordening van de Europese commissie (2018/389).

Indien uw organisatie meent vrijgesteld te zijn van het gebruik van een sterke cliëntauthenticatie dient u dit te motiveren.

Bij de autorisatie van een betalingstransactie moet de specifiek voor deze betalingstransactie gegenereerde authenticatiecode worden gekoppeld aan de betalingstransactie (zogenaamde Dynamic Link / Dynamische koppeling vereiste uit de verordening 2018/389). In het procedurehandboek beschrijft u hoe u het proces en de bescherming vorm geeft.

Het proces en de maatregelen van cliëntauthenticatie test u regelmatig. U zorgt ervoor dat ze geëvalueerd en gecontroleerd worden door auditors met deskundigheid op het gebied van IT-beveiliging en -betalingen en die onafhankelijk zijn binnen of ten opzichte van uw organisatie.

3.12 Veilige communicatie

Uw organisatie maakt gebruik van elektronische (digitale) communicatie met derden. Om de beschikbaarheid van de communicatie en de vertrouwelijkheid en de integriteit van data te waarborgen, dient uw organisatie maatregelen te treffen. In het handboek dient u te beschrijven welke maatregelen u hebt genomen, en welke processen en procedures ingericht zijn voor de beheersing van de getroffen maatregelen.

Betaaldienstverleners zorgen voor veilige identificatie bij de communicatie tussen de apparatuur van de betaler en de apparatuur van de betalingsbegunstigde voor het accepteren van elektronische betalingen. Betaaldienstverleners zorgen ervoor dat het risico dat communicatie plaatsvindt naar onbevoegde partijen worden beperkt. De wijze waarop u dit doet, beschrijft u in het procedurehandboek.

Betaaldienstverleners beschikken over procedures die borgen dat alle betalingstransacties en andere interacties – met de betaaldienstgebruiker:

- met andere betaaldienstverleners; en
- met andere entiteiten, daaronder begrepen handelaren, in het kader van het verrichten van de betaaldienst traceerbaar zijn, zodat achteraf alle gebeurtenissen die relevant zijn voor de elektronische transactie in alle verschillende fasen, bekend zijn.

Betaaldienstverleners zorgen ervoor dat communicatiesessies die tot stand komen met de betaaldienstgebruiker, andere betaaldienstverleners en andere entiteiten, daaronder begrepen handelaren, gebruikmaken van elk van de volgende elementen.

- a. Een unieke identicator van de sessie.
- b. Beveiligingsmechanismen voor een gedetailleerde logging van de transactie, met onder meer een transactienummer, tijdstempel en alle relevante transactiegegevens.
- c. Tijdstempels die zijn gebaseerd op een gemaakt tijdsreferentiesysteem en die zijn gesynchroniseerd met een officieel tijdsignaal.

In het procedurehandboek geeft u aan hoe dit in uw organisatie realiseert.

Indien de onderneming gebruik maakt van cryptografische middelen, dient u in het handboek te beschrijven van welke technologie gebruikt gemaakt wordt en hoe deze middelen (o.a. sleutels, certificaten, etc.) worden beheerd.

3.13 Datacollectie

Uw onderneming krijgt door middel van de beoogde dienstverlening op enig moment te maken met gevoelige betalingsgegevens. Hiermee worden gegevens bedoeld waarmee fraude kan worden gepleegd. Hier vallen in ieder geval persoonlijke beveiligingsgegevens onder.³

De gevoelige betalingsgegevens mogen onder geen beding in de verkeerde handen komen en daarom dient u een beschrijving aan te leveren van het proces om gevoelige betalingsgegevens op te slaan, te monitoren, te traceren en de toegang te beperken. Neemt u in de beschrijving in ieder geval de volgende vier onderdelen op:

- Een beschrijving van de datastromen in verhouding tot uw business model.
- Een beschrijving van het opslaan van de gecollecteerde data: deze beschrijving is niet nodig indien u uitsluitend dienst 7 aanvraagt, want dan mag u geen gevoelige betalingsgegevens opslaan.

3 Voor de activiteiten van betalingsinitiatiedienstaanbieders en rekeninginformatiedienstaanbieders vormen de naam van de rekeninghouder en het rekeningnummer geen gevoelige betalingsgegevens.

- Een beschrijving van de verwachte interne en/of externe toepassingen inclusief eventuele tegenpartijen met betrekking tot de gecollecteerde en opgeslagen data: deze beschrijving is niet nodig indien u uitsluitend dienst 7 aanvraagt want dan mag u geen gevoelige betalingsgegevens opslaan.
- Een opsomming van en toelichting op de individuen, bedrijfsonderdelen en/of comités die toegang hebben tot de gevoelige betalingsgegevens.

Let op, het bovenstaande is geen limitatieve opsomming.

Wanneer uw onderneming een vergunning verkrijgt dan geldt in het kader van *gegevensbescherming* het volgende voor uw organisatie:

- Biedt uw onderneming betaaldienst 1 t/m 7 aan, dan mag uw onderneming alleen met de uitdrukkelijke toestemming van de betaaldienstgebruiker toegang krijgen tot diens persoonsgegevens om deze gegevens te verwerken en te bewaren voor zover noodzakelijk voor het verlenen van betaaldiensten⁴.
- In het handboek dient u te beschrijven hoe uw onderneming hier invulling aan geeft, hierbij rekening houdend met een eventuele tijdelijke opslag van betalingsgegevens, veiligheids- en authenticatiegegevens, en hoe onder andere de vastlegging van de toestemming plaatsvindt.
- Biedt uw onderneming betaaldienst 8 aan, dan mag u deze dienst slechts aanbieden met de uitdrukkelijke instemming van de betaaldienstgebruiker⁵.
- In het handboek dient u te beschrijven hoe uw onderneming hier invulling aan geeft, hierbij rekening houdend met een eventuele tijdelijke opslag van betalingsgegevens, veiligheids- en authenticatiegegevens, en hoe onder andere de vastlegging van de toestemming plaatsvindt.

3.14 Opvolging van incidenten

Operationele incidenten of beveiligingsincidenten

Een operationeel of beveiligingsincident is een gebeurtenis die een gevaar vormt voor de beschikbaarheid van de aangeboden diensten en/of de vertrouwelijkheid of integriteit van de aan uw onderneming toevertrouwde gegevens. Vanwege de invloed van dergelijke incidenten op uw bedrijfsuitvoering, treft u maatregelen om het risico op dergelijke incidenten te minimaliseren.

De onderneming moet beschikken over beleid, procedures en maatregelen om goed om te gaan met operationele of beveiligingsincidenten. Minimaal betekent dit dat de volgende procedures en maatregelen omschreven moeten zijn:

- Vastlegging van het incident.
- Classificatiemechanisme op basis van door de wetgever bepaalde criteria, waarbij onderscheid wordt gemaakt tussen majeure en niet-majeure incidenten en dat voorziet

4 Het op dit moment voorgestelde nieuwe artikel 26e Besluit Prudentiële regels Wft

5 Het op dit moment voorgestelde nieuwe artikel 26j Besluit Prudentiële regels Wft.

in een deugdelijke analyse van de interne en externe impact van het incident inclusief een eventuele impact voor collega-betaalinstellingen en/of buiten Nederland.

- Het binnen 4 uur kunnen melden van een majeur incident aan DNB conform de gestelde procedure en met de verplichtte informatie.
- De procedures waarmee DNB regelmatig over de voortgang van het oplossen van het incident wordt geïnformeerd.
- Het uitvoeren van een root cause analyse nadat het incident is opgelost.
- Volledig informeren van DNB op basis van de voorgeschreven procedure.
- De onderneming dient in het kader van beveiligingsincidenten zorg te dragen voor een klachtenprocedure waarmee betaaldienstgebruikers melding kunnen maken van (mogelijke) beveiligingsrisico's en incidenten.

DNB is verplicht om operationele- of beveiligingsincidenten te delen met de Europese Bankautoriteit (EBA) en de Europese Centrale Bank (ECB). De EBA en/of de ECB kunnen naar aanleiding van deze informatie rechtstreeks contact kan opnemen met de onderneming (zie EBA-GL-2017-10).

Uw onderneming beschrijft het beleid rond operationele of beveiligingsincident inclusief de bijbehorende procedures en maatregelen in het procedurehandboek.

De onderneming is zelf verantwoordelijk voor de melding van operationele of beveiligingsincidenten aan overige autoriteiten in Nederland indien noodzakelijk, zoals de Autoriteit Persoonsgegevens (AP).

Integriteitsincidenten

Een incident is een gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van uw onderneming. Vanwege de invloed die incidenten kunnen hebben op een onderneming is het van belang dat u de bedrijfsvoering zo inricht dat het risico op incidenten zoveel mogelijk wordt beperkt. Voorkomen moet worden dat de onderneming betrokken raakt bij strafbare feiten, of handelingen verricht die ingaan tegen hetgeen volgens het ongeschreven recht in het maatschappelijk verkeer betamelijk wordt geacht. Het maakt hierbij niet uit door wie een dergelijke handeling wordt verricht: het kan gaan om gedragingen van personeelsleden, bestuurders, leden van het orgaan dat is belast met het toezicht of van natuurlijke of rechtspersonen die werkzaamheden verrichten voor uw onderneming. Onder gedragingen wordt zowel doen als nalaten verstaan.

Daarom moet uw onderneming beschikken over procedures en maatregelen om goed om te gaan met incidenten. Minimaal betekent dit het volgende:

- De vastlegging van incidenten.
- De wijze van afhandeling van incidenten.
- Informatieverstrekking aan de toezichthouder.

De vastlegging van het incident stelt DNB in staat om te beoordelen of uw onderneming op een juiste manier omgaat met incidenten. Uit de gegevens moet DNB bijvoorbeeld de kenmerken van het incident, degene(n) die het incident hebben veroorzaakt of bevorderd en de genomen maatregelen kunnen opmaken. U moet DNB direct op de hoogte stellen van een incident.

Frauderapportage

Een betaalinstelling is verplicht om fraudegegevens te verzamelen en deze op reguliere basis volgens een opgelegd formaat aan DNB te verstrekken. Halfjaarlijks dient fraude-informatie aan DNB te worden verstrekt over kwartaal fraude gegevens.

De onderneming dient te beschikken over procedures en maatregelen om de juiste gegevens vast te leggen om te kunnen voldoen aan de verplichte frauderapportage. Deze procedures en bijbehorende maatregelen dient u te beschrijven in het procedurehandboek.

Omdat de definitieve vereisten nog niet zijn vastgesteld verwijzen wij voor dit onderdeel naar de EBA-website: <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-fraud-reporting-under-psd2>

3.15 Bedrijfscontinuïteitsbeheer (business continuity management)

Voor de continuïteit van de bedrijfsvoering moet de onderneming beschikking over een business continuity management (BCM) systeem om bij een (ernstige) interne of externe verstoring de diensten zo spoedig mogelijk binnen de gemaakte afspraken en de maatschappelijk verwachte tijden te kunnen herstellen.

In het BCM-systeem, beschreven in het procedurehandboek, dient de onderneming minimaal invulling te geven aan de volgende acht onderdelen:

- BCM-beleid met aandacht voor onder andere de organisatie tijdens een verstoring, classificatie van verstoringen, maximale hersteltijden van systemen en processen, interne en externe communicatie, escalatie, informeren van autoriteiten, verlies van data, etc.
- Business-impact-analyse, rekening houdend met de interne en externe impact.
- De wijze waarop en welke maatregelen getroffen zijn om invulling te kunnen geven aan haar beleid en de gemaakte afspraken .
- Gebruik maken van diverse scenario's van verstoringen.
- Een communicatieplan.
- Een crisismanagementplan.
- De menselijke factor.
- Een plan hoe en met welke frequentie het BCM-systeem getest wordt, waarbij kan worden aangetoond dat de onderneming in staat is om te allen tijde te voldoen aan haar beleid.

3.16 Beheerst beloningsbeleid

Uw onderneming voert als onderdeel van haar beheerste bedrijfsvoering een beheerstbeloningsbeleid dat schriftelijk wordt vastgelegd. Dit dient in een afzonderlijk document te zijn vervat (dus niet in het procedurehandboek te zijn opgenomen). Kort gezegd houdt het beloningsbeleid in dat de beloning er niet toe aanmoedigt dat medewerkers meer risico's nemen dan aanvaardbaar is voor de onderneming met het oog op haar soliditeit.

Het beloningsbeleid brengt op een gestructureerde en logische manier in kaart of er mogelijk negatieve prikkels van uitgaan in het kader van de beheersing van relevante risico's, en het beschrijft de manier waarop uw elektronischgeldinstelling deze prikkels voorkomt en beheerst. Het spreekt voor zich dat het opstellen van een beheerst beloningsbeleid een uitvoerige analyse vergt van mogelijke ongunstige prikkelwerking van beloningsstructuren en beloningscomponenten. Bij die analyse moet u in het bijzonder aandacht besteden aan de prikkels die kunnen ontstaan op basis van variabele beloningscomponenten. Ook positieve prikkelwerking in het kader van claw back-mogelijkheden kunnen in de analyse worden betrokken.

In uw beschrijving van het beloningsbeleid beantwoordt u de volgende vier vragen:

- Passen de passende verhoudingen tussen de vaste en variabele beloning binnen de onderneming? Hierbij houdt u rekening met de algemene aspecten die van belang zijn bij het beloningsbeleid, zoals de aard van de activiteiten, omvang van de elektronischgeldinstelling en de gevolgen voor de behandeling van klanten. Bij het vormgeven van de passende verhouding dient blijft uw elektronischgeldinstelling uiteraard binnen de grenzen van het bonusplafond.
- Hoe is de verhouding tussen de toegekende en uitgekeerde variabele beloning?
- Wat is precies de samenstelling van de variabele beloning?
- Op welke criteria en prestaties is de variabele beloning gebaseerd? Beschrijf hier niet uitsluitend de prestaties en resultaten van de persoon die de variabele beloning ontvangt, maar ook de prestaties van het bedrijfsonderdeel waar deze medewerker werkzaam is en om prestaties van de elektronischgeldinstelling als geheel. Bij de beoordeling van een individuele medewerker worden naast financiële criteria ook niet-financiële criteria gehanteerd, bijvoorbeeld strategische doelen, klanttevredenheid, het naleven van beleid ten aanzien van risicobeheersing, compliance met interne en externe regels, leiderschap, managementvaardigheden, samenwerken met andere personen en bedrijfsonderdelen, creativiteit, motivatie, duurzaamheid en maatschappelijk bewust handelen. Negatieve resultaten op niet-financiële criteria, in het bijzonder waar het onethisch of non-compliant gedrag betreft, doen positieve resultaten op financiële criteria te niet. In dergelijke gevallen dient de variabele beloning te worden verlaagd tot nul. De variabele beloning wordt voor ten minste 50% gebaseerd op niet-financiële criteria. Ook geldt er een maximum voor de

30

hoogte van de variabele beloning (hiervoor verwijzen wij naar artikel 1:121 e.v. van de Wft). DNB heeft de regels over het beloningsbeleid nader uitgewerkt in de Regeling beheerst beloningsbeleid Wft 2014 (zie www.overheid.nl).

Wij vragen het beloningsbeleid met het aanvraagformulier mee te sturen. Verder vragen wij u om ook kort in uw eigen woorden aan te geven waaruit blijkt dat het beloningsbeleid niet aanmoedigt tot het nemen van meer risico's dan aanvaardbaar is voor de onderneming.

3.17 Eed of belofte

Uw onderneming dient over over procedures en maatregelen te beschikken die waarborgen dat natuurlijke personen die in Nederland werkzaam zijn onder uw verantwoordelijkheid en wier werkzaamheden het risicoprofiel van de onderneming wezenlijk kunnen beïnvloeden of die zich rechtstreeks bezighouden met het verlenen van financiële diensten, een eed of belofte afleggen. Een dergelijke regeling dient u op te stellen, conform de Regeling eed of belofte financiële sector 2015.

3.18 Training en opleiding

Een toereikende implementatie van de processen en procedures hangt voornamelijk af van ervaring en kennis van de medewerkers. Kennis van en ervaring met de beheersing van de risico's (onder andere van witwassen en terrorismefinanciering) zijn dan ook belangrijke voorwaarden voor een toereikend beheersingskader. Opleidingen en trainingen van het personeel zijn daarbij belangrijke manieren om kennis te communiceren en de naleving van de Wet ter voorkoming van witwassen en financieren van terrorisme (WWFT) en de Sanctiewet 1977 (SW), de integriteitbeleidsuitgangspunten en procedures te borgen.

Uw onderneming moet daartoe opleidingen aanbieden, die de medewerkers bekend maken met de bepalingen van de WWFT en de SW en die de medewerkers in staat stellen het cliëntenonderzoek goed en volledig uit te voeren en ongebruikelijke transacties te herkennen. Deze opleidingen behandelen witwas- en terrorismefinancieringstechnieken, methodes en trends, de internationale context en standaarden, en nieuwe ontwikkelingen op dat gebied. Om op de hoogte te blijven van de nieuwe ontwikkelingen en de bewustwording blijvend te bevorderen, is een training in de regel niet eenmalig, maar wordt deze regelmatig en ook op verschillende niveaus aangeboden. Het ligt in de rede dat ook de compliancefunctie aanvullende opleiding en training volgt om op de hoogte te blijven van ontwikkelingen inzake de –internationale- wet- en regelgeving en witwas- en terrorismefinancieringsrisico's.

Graag ontvangen wij het opleidingsplan van uw onderneming. Ook ontvangen wij graag een beschrijving waaruit blijkt dat de onderneming de bedrijfsvoering ten aanzien van opleiding en training zo heeft ingericht dat beheerste uitoefening van het bedrijf is gewaarborgd. De beschrijving kan onderdeel zijn van het procedurehandboek van uw onderneming of in een apart document zijn opgenomen. Wij vragen u in het formulier aan te geven waar wij deze kunnen terugvinden.

4 Inrichting bedrijfsvoering voor integere uitoefening van het bedrijf

32

Een integere uitoefening van uw onderneming is één van de pijlers van vertrouwen en dus een randvoorwaarde voor het goed functioneren van de onderneming. Het gaat er hierbij om dat uw onderneming voorkomt dat zij betrokken raakt bij handelingen die tegen de wet ingaan of handelingen die maatschappelijk onbetamelijk zijn. Centraal staat daarbij de beheersing van integriteitsrisico's. Hierbij denken wij met name aan het tegengaan van financieel-economische criminaliteit. Bij financieel-economische criminaliteit moet u met name denken aan witwassen, financiering van terrorisme en belangenverstrengeling.

De verplichting tot een integere bedrijfsuitoefening staat beschreven in de artikelen 3:10 en 3:17 Wet op het financieel toezicht (Wft) en de uitwerking van deze artikelen in het Besluit prudentiële regels Wft (Bpr). Daarnaast zijn de relevante artikelen uit de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) en de Sanctiewet 1977 (Sw) van toepassing. Uw onderneming moet een adequaat beleid voeren dat een integere uitoefening van het bedrijf waarborgt. Dit houdt in dat het beleid is uitgewerkt en geïmplementeerd in heldere, eenvoudig toegankelijke procedures en maatregelen. De uitwerking van deze procedures en maatregelen moet zijn vastgelegd in het procedurehandboek.

Het regelgevend kader voor een adequaat integriteitsbeleid is risico-gebaseerd. Dit betekent dat uw onderneming alle maatregelen toepast die de wet voorschrijft. De intensiteit waarmee u dat doet stemt u echter af op de risico's die uw onderneming loopt. Deze kunnen bijvoorbeeld voortvloeien uit de aard en achtergrond van uw cliënten, het type product (iDEAL, pinterminal, money transfer etc.) of dienst (1 t/m 8). U maakt zelf een inschatting van de relevante risico's en stelt daar vervolgens voldoende mitigerende maatregelen tegenover.

De volgende onderwerpen moeten in ieder geval aan bod komen:

- Systematische analyse van integriteitsrisico's
- Tegengaan van verstrengeling van belangen
- Omgang met en vastlegging van incidenten
- Betrouwbaarheid van medewerkers in integriteitsgevoelige functies
- Cliëntenonderzoek⁶
- Sanctiewet 1977
- Monitoring van transacties en melding van ongebruikelijke transacties⁷
- Klachtenprocedure

6 Over de vereisten van het cliëntonderzoek bij dienst 7 en 8 heeft DNB een Q&A gemaakt. Deze kunt u vinden op onze PSD2 webpagina: <http://www.toezicht.dnb.nl/4/1/50-236570.jsp>

7 Over de vereisten van transactiemonitoring bij dienst 7 en 8 heeft DNB een Q&A gemaakt. Deze kunt u vinden op onze PSD2 webpagina: <http://www.toezicht.dnb.nl/4/1/50-236570.jsp> worden gepubliceerd.

Hieronder worden deze onderwerpen nader uitgewerkt. De (Europese) regelgeving op het gebied van betaaldiensten alsook de (Europese) regelgeving op witwassen en terrorismefinanciering is continu aan verandering onderhevig. U dient ervoor zorg te dragen dat het beleid en de procedures up-to-date blijven aan geldende wet- en regelgeving.

4.1 Systematische analyse van integriteitsrisico's (SIRA)

Het integriteitsbeleid van uw onderneming en de uitvoering daarvan begint bij het identificeren van de integriteitsrisico's die zij loopt. Zo'n systematische integriteitsrisicoanalyse (SIRA) is een voorwaarde voor een toereikende inrichting van de integere bedrijfsvoering. De analyse is herleidbaar, dus vastgelegd in een apart document, en het integriteitsbeleid is gebaseerd op de uitkomsten van de SIRA. Ook wordt een begrijpelijke kwantificeringsmethode gehanteerd. De SIRA gaat uit van bruto (inherente) en netto (rest) risico's en gaat in op de kans en impact van de risico's. De omvang van de netto risico's is begrijpelijk en het effect van de maatregelen en procedures is plausibel.

De SIRA bevat, op grond van scenario's minimaal een analyse van de volgende risico's: belangenverstremgeling, witwassen, terrorismefinanciering, overtreding van sanctieregelgeving en (internet-)fraude/oplichting. Verder bepaalt u in de SIRA de risico's die met de producten/diensten van uw klanten (merchants of natuurlijke personen) gepaard gaan en betreft deze bij de te hanteren cliëntprofielen. In het verlengde hiervan besteedt u, indien van toepassing, bijzondere aandacht aan online cliëntacceptatie. Er wordt duidelijk naar voren gebracht dat dit altijd een hoog risico met zich meebrengt en uit de analyse blijkt met welke beheersmaatregelen de onderneming dit verhoogde risico compenseert.

Uit de procedures en maatregelen blijkt een duidelijke samenhang met de specifieke risico's die in de SIRA zijn geïdentificeerd. De beheersmaatregelen zijn herleidbaar toegesneden op de aard, omvang, complexiteit en het risicoprofiel van de werkzaamheden van uw onderneming. Meer informatie over de SIRA vindt u in de guidance van DNB voor het opzetten van een goede SIRA: 'De integriteitsrisicoanalyse. Meer waar het moet, minder waar het kan': <http://www.toezicht.dnb.nl/binaries/50-234068.pdf>.

34 4.2 Tegengaan van verstrengeling van (privé)belangen

Belangenverstrengeling, of de schijn daarvan, kan negatieve gevolgen hebben voor zowel uw cliënten als voor uw onderneming zelf. Uw onderneming moet daarom beschikken over procedures en maatregelen met betrekking tot het tegengaan van verstrengeling van privébelangen. Het gaat daarbij om verschillende groepen:

- beleidsbepalers;
- groepsbestuurders;
- commissarissen; en
- andere werknemers of personen die op structurele basis werkzaamheden voor de betaalinstelling verrichten.

In het beleid maakt uw onderneming duidelijk hoe er bijvoorbeeld wordt omgegaan met zaken als:

- persoonlijke, professionele en financiële belangen in relatie tot het omgaan met cliënten en andere relaties;
- het omgaan met vertrouwelijke informatie;
- het aangaan van cliëntrelaties;
- het verrichten van transacties in de privésfeer; en
- het vervullen van nevenactiviteiten.

4.3 Betrouwbaarheid integriteitsgevoelige functies

Er bestaan binnen financiële ondernemingen naast de functie van bestuurder of leden van het orgaan dat belast is met het toezicht, ook andere functies die van invloed kunnen zijn op de integere uitoefening van het bedrijf. Dit zijn 'integriteitsgevoelige functies'. U moet zelf vaststellen welke functies als integriteitsgevoelig kwalificeren. Voor de personen in deze functies maakt u vervolgens een onderbouwde beoordeling van de betrouwbaarheid. Dit geldt ook voor tijdelijke werknemers.

Een integriteitsgevoelige functie is in ieder geval:

- een leidinggevende direct onder de (mede)beleidsbepalers
- een functie waaraan een bevoegdheid is verbonden die een wezenlijk risico inhoudt voor de integere uitoefening van het bedrijf

4.4 Cliëntenonderzoek

Dienstverlening aan een cliënt mag pas beginnen nadat de identificatie en verificatie van de cliënt en de UBO (ultimate beneficial owner) hebben plaatsgevonden, het zogenaamde cliëntonderzoek / customer due diligence. In het procedurehandboek legt u daarom de

procedures en maatregelen over het cliëntenonderzoek op heldere wijze vast. De procedures en maatregelen over de acceptatie van cliënten sluiten aan bij het integriteitbeleid en uitgevoerde SIRA.

Het raamwerk van de Wft (integere bedrijfsvoering) en WWFT gaan ervan uit dat een onderneming haar cliënten in risicocategorieën indeelt op basis van het onderscheid in aard en omvang van het risico. De risicocategorieën variëren van laag tot hoog risico en de indeling geschiedt op basis van objectieve en kenbare indicatoren. Hoe hoger de risico's, des te meer inspanningen de instelling verricht om die risico's te mitigeren. Tevens is van belang dat u aangeeft welke risico's onacceptabel zijn.

Bij het cliëntonderzoek houdt u rekening met de volgende zaken:

- De onderneming verifieert de identiteit van elke cliënt aan de hand van onafhankelijke en betrouwbare documenten. Indien de cliënt een juridische entiteit is, geldt dit ook voor de vertegenwoordigers en uiteindelijk belanghebbende(n).
- De onderneming heeft daarbij voldoende inzicht in de eigendoms- en zeggenschapsstructuur van de cliënt/juridische entiteit.
- De onderneming heeft inzicht in waarom en waarvoor de cliënt de dienstverlening wil gebruiken, heeft dit goed gedocumenteerd en verwerkt in het risicoprofiel van de cliënt.
- Op alle cliënten wordt PEP (politically exposed person, politiek prominent persoon)- en sanctiescreening uitgevoerd.
- De betreffende gegevens worden aantoonbaar en op toegankelijke wijze tot in ieder geval vijf jaar na de dienstverlening of het beëindigen van de zakelijke relatie bewaard door de onderneming.
- Alle gegevens betreffende de cliënt en uiteindelijk belanghebbende worden centraal bewaard op een manier die toegankelijk is voor compliance en andere relevante medewerkers. Onder meer legt uw onderneming vast wanneer een verscherpt cliëntenonderzoek aan de orde is en welke maatregelen de onderneming in die gevallen treft. Als een cliënt, prospect of UBO een PEP is wordt dit ook vastgelegd. De cliënten worden ingedeeld in risicocategorieën en aangegeven wordt op basis van welke overwegingen cliënten, producten of diensten in een bepaalde risicocategorie worden ingedeeld. Deze indeling is adequaat en sluit aan op de eerdergenoemde SIRA. Cliënten worden bij acceptatie gescreend tegen de sanctielijsten, PEP-lijsten en eventuele andere lijsten. Eventuele 'hits' worden vastgelegd in het cliëntdossier en waar nodig wordt actie ondernomen. Deze eventuele hits worden ook verwerkt in het risicoprofiel van de cliënt en gemeld aan DNB. Ten slotte is er een exitbeleid voor cliënten die niet geïdentificeerd kunnen of willen worden of waarvan de identiteit niet (op juiste wijze) geverifieerd kan worden. Dit wordt in voorkomende gevallen (aantoonbaar) opgevolgd.

In procedures en maatregelen ligt vast op welke wijze en door wie het cliëntenonderzoek wordt uitgevoerd. Geborgd is dat relevante medewerkers op de hoogte zijn van de interne en wettelijke eisen die aan het cliëntenonderzoek gesteld worden. De cliëntacceptaties worden goedgekeurd volgens het vier-ogen principe, door daartoe bevoegde werknemers of management. Zie voor meer guidance ten aanzien van dit onderwerp, de DNB leidraad WWFT en SW: <http://www.toezicht.dnb.nl/binaries/50-212353.pdf>.

4.5 Sanctiewet 1977

In uw procedurehandboek hebt u het beleid over sanctieregelgeving geformuleerd en dit beleid vastgelegd in procedures. Deze procedures waarborgen een volledige (actuele) inventarisatie van de dienstverlening in relatie tot landen, (rechts)personen, groepen en entiteiten waarop sanctieregelgeving van toepassing is. Tevens is er een procedure voor de ontvangst en interne distributie van de sanctielijsten; dit geldt voor ten minste de Nederlandse sanctielijst en de EU-verordeningen.

De procedures en maatregelen zien erop toe dat het relatiebestand periodiek gecontroleerd wordt op het overeenkomen van relaties met de entiteiten zoals bedoeld in de sanctieregelgeving. De procedures omvatten de controle op nationale en internationale diensten. De procedures en maatregelen houden rekening met de verschillende normen en doelstellingen van de diverse sanctieregelingen, dus sanctiemaatregelen jegens personen of entiteiten en jegens landen.

De procedures en maatregelen zijn zo ingericht dat financiële middelen bij hits kunnen worden bevroren dan wel dat kan worden voorkomen dat financiële middelen of diensten ter beschikking worden gesteld aan gesanctioneerde personen of entiteiten. De onderneming heeft voldoende maatregelen die waarborgen dat (mogelijke) hits tijdig worden gerapporteerd aan de verantwoordelijke centrale persoon of afdeling, die deze vervolgens, indien van toepassing, meldt aan DNB.

Zie voor meer guidance ten aanzien van dit onderwerp, de DNB leidraad WWFT en SW: <http://www.toezicht.dnb.nl/binaries/50-212353.pdf> en de volgende pagina wegwijs in sanctieregelgeving op Open Boek Toezicht <http://www.toezicht.dnb.nl/2/50-221960.jsp>.

4.6 Monitoring transacties en melding van ongebruikelijke transacties

37

Uw onderneming heeft procedures en processen om de rekeningen, activiteiten en/of transacties van cliënten te monitoren om inzicht te krijgen en te houden in de aard en achtergrond van cliënten, en hun financieel gedrag, en om ongebruikelijke transactiepatronen en transacties te detecteren die naar hun aard een hoger risico lopen op witwassen of financieren van terrorisme. In procedures en processen is vastgelegd hoe transactiemonitoring plaatsvindt, welke alerts en red flags worden gebruikt, en welke acties moeten worden ondernomen indien er zich transacties voordoen die mogelijk ongebruikelijk zijn. Er zijn gemotiveerde en begrijpelijke keuzes gemaakt tussen automatische monitoring en handmatige controle. Op grote aantallen transacties zal automatische monitoring uitkomst bieden. In beleid en procedures is vastgelegd hoe ongebruikelijke transacties, nadat het ongebruikelijke karakter bekend is geworden, onverwijld aan de FIU worden gemeld.

Zie voor meer guidance over dit onderwerp, de DNB guidance voor transactiemonitoring bij betaalinstanties. <http://www.toezicht.dnb.nl/2/50-236674.jsp>

5 Betrouwbaarheid en geschiktheid (mede) beleidsbepalers

38

5.1 Geschikte beleidsbepalers

De beleidsbepalers⁸ van de onderneming dienen geschikt te zijn voor hun functie. Let er bij uw aanvraag dan ook op dat u personen voordraagt die naar verwachting door de geschiktheidstoets van DNB zullen komen. Bij een beoordeling van geschiktheid stelt DNB vast of de kandidaat beschikt over voldoende relevante kennis, vaardigheden en professioneel gedrag om de functie te vervullen. Dit moet blijkt onder meer uit opleiding, werkervaring en competenties.

Omdat de beoordeling is gekoppeld aan de functie, houdt DNB rekening met:

- de specifieke functie van de kandidaat;
- de aard, omvang, complexiteit en het risicoprofiel van de onderneming; en
- de samenstelling en het functioneren van het collectief.

DNB hanteert de Beleidsregel geschiktheid 2012. Voor meer informatie verwijzen wij u naar de specifieke Open Boek pagina over geschiktheid: <http://www.toezicht.dnb.nl/4/2/16/50-229353.jsp>.

Indien wordt gekozen voor een RvC of een RvC door DNB wordt verlangd, wordt gegeven het belang van een integere en beheerste bedrijfsvoering verwacht dat de RvC onafhankelijk functioneert. Voor meer informatie verwijzen wij naar de specifieke openboek pagina: <http://www.toezicht.dnb.nl/3/50-226002.jsp>

Om een kandidaat aan te melden gebruikt u het Aanvraagformulier Aanvangstoetsing dat via het Digitaal Loket Toezicht beschikbaar is. In de praktijk blijkt dat formulieren nog wel eens onvolledig worden aangeleverd. Dat leidt tot onnodige vertraging. Op de website van DNB vindt u daarom tips voor een goede voorbereiding van de toetsing: <http://www.toezicht.dnb.nl/4/2/16/50-229355.jsp>

Let op: voor bestuurders en commissarissen geldt op basis van de Wet bestuur en toezicht een maximum aantal toezichthoudende functies.

5.2 Betrouwbare (mede)beleidsbepalers

8 Beleidsbepalers zijn de bestuurders van de onderneming en indien van toepassing leden van de raad van commissarissen of toezicht. Medebeleidsbepalers hoeven niet op geschiktheid getoetst te worden. Zie onder 'betrouwbare (mede) beleidsbepalers' wat verstaan wordt onder een medebeleidsbepaler.

Ook van de medebeleidsbepalers van uw onderneming (de bestuurders van de onderneming en de raad van commissarissen of toezicht, indien van toepassing) moet de betrouwbaarheid buiten twijfel staan.

Personen die direct of indirect een gekwalificeerde deelneming in de onderneming houden, zijn medebeleidsbepalers. Houders van een gekwalificeerde deelneming zijn alle natuurlijke personen en/of rechtspersonen die een direct of indirect aandelenbelang of zeggenschapsbelang in de onderneming hebben van 10 procent of meer. Ook personen die feitelijk invloed van betekenis kunnen uitoefenen op de dagelijkse leiding van de onderneming, worden aangemerkt als medebeleidsbepaler.

DNB stelt vast of de betrouwbaarheid van een kandidaat buiten twijfel staat. Het gaat daarbij om voornemens, handelingen en antecedenten van de betreffende persoon die het vervullen van de functie in de weg staan. DNB kijkt hierbij vooral naar strafrechtelijke, financiële, toezicht-, fiscaal bestuursrechtelijke antecedenten en overige antecedenten.

De beoordeling van betrouwbaarheid is in beginsel eenmalig. Een kandidaat die al eerder een positief besluit heeft ontvangen, hoeft niet opnieuw te worden getoetst. Het besluit blijft gelden, tenzij een verandering in relevante feiten of omstandigheden een redelijke aanleiding geeft om de betrouwbaarheid opnieuw te bezien.

De beoordeling van betrouwbaarheid gaat louter over de kandidaat zelf. Dit betekent dat het besluit – in tegenstelling tot een aanvangstoetsing geschiktheid – niet afhankelijk is van de omstandigheden zoals de samenstelling van het bestuur, het soort onderneming waarop de voorgenomen benoeming betrekking heeft, of de specifieke functie die de betrokkene zou moeten gaan vervullen. De beoordeling van betrouwbaarheid vindt plaats op basis van informatie die de onderneming aanlevert en een beoordeling door DNB.

Zie voor meer informatie: <http://www.toezicht.dnb.nl/4/2/16/50-229351.jsp>.

6 Twee dagelijks beleidsbepalers werkzaam vanuit Nederland

- 40 Het dagelijks beleid van uw onderneming dient bepaald te worden door ten minste twee natuurlijke personen. Deze personen dienen hun werkzaamheden in verband hiermee vanuit Nederland te verrichten.
- Hierin komt het zogenaamde vier-ogen-beginsel of het beginsel van tweehoofdige dagelijkse leiding tot uitdrukking. De regel dat twee of meer natuurlijke personen het dagelijks beleid van een betaalinstantie bepalen, zorgt voor waarborging van de continuïteit en kwaliteit van uitoefening van het bedrijf en de dienstverlening.

7 Transparantie zeggenschapsstructuur

Uw onderneming moet een transparante zeggenschapsstructuur hebben. Dit betekent kort gezegd dat de formele zeggenschapsstructuur gelijk is aan de feitelijke zeggenschapsstructuur. Daarbij geldt dat er geen sprake mag zijn van een zeggenschapsstructuur die een belemmering meebrengt voor het adequaat uitoefenen van toezicht. Dit is het geval wanneer door de zeggenschapsstructuur personen aan de onderneming verbonden zijn, waarop het recht van toepassing is van een staat buiten de EU. De wetgever heeft deze bepaling opgenomen om te voorkomen dat de organisatorische structuur waarin de activiteiten van deze zeggenschapsstructuur plaatsvinden, sterk afwijkt van de juridische structuur waarin die activiteiten zijn ingebed. Een dergelijke organisatorische structuur belemmert DNB in het toezicht op de onderneming. Denk hierbij aan het traceren van de risico's waaraan de onderneming blootstaat, of het beoordelen of de bedrijfsvoering wel gezond en prudent is.

41

Wij vragen u de zeggenschap visueel te maken door middel van een structuuroverzicht van de juridische structuur (UBO, moedermaatschappij, eventuele dochter- en zustermaatschappijen) waar uw onderneming (de betaalinstantie) deel van uitmaakt. Dit structuuroverzicht moet een duidelijk beeld geven van de feitelijke situatie. Uit dit structuuroverzicht blijkt wie een gekwalificeerde deelneming houden in uw onderneming, alsmede de omvang van de desbetreffende gekwalificeerde deelneming. Houders van een gekwalificeerde deelneming zijn alle natuurlijke personen en/of rechtspersonen die een direct of indirect aandelenbelang of zeggenschap in de onderneming hebben van 10 procent of meer. Ook de UBO moet hieruit blijken. Ten slotte vragen wij u in het structuuroverzicht aan te geven wie de bestuurders zijn van alle rechtspersonen en vennootschappen binnen de groep.

Concernverhouding

Is de onderneming onderdeel van een (internationaal) concern of aangesloten groep van bedrijven binnen of buiten de EU, dan ontvangen wij graag een beschrijving van de wijze van besluitvorming binnen de groep en de rol die uw onderneming daarbij inneemt.

8 Gekwalificeerde deelneming(en)

42

Dit onderdeel is niet van toepassing indien u uitsluitend dienst 8 aanbiedt.

Ondernemingen met een gekwalificeerd aandelenbelang of zeggenschapsbelang in uw onderneming hebben voorafgaande goedkeuring nodig van DNB. Deze ondernemingen moeten dan een Verklaring van geen bezwaar (vvgb) als bedoeld in artikel 3:95 van de Wft aanvragen.

Wanneer is sprake van een gekwalificeerde deelneming?

Er is sprake van een gekwalificeerde deelneming – en dus van een vvgb-plicht – in de volgende gevallen.

- Een rechtspersoon of natuurlijk persoon heeft of verwerft een rechtstreeks of middellijk (indirect) belang van ten minste 10% in het geplaatste kapitaal van uw onderneming.
- Een rechtspersoon of natuurlijk persoon kan rechtstreeks of middellijk (indirect) ten minste 10% van de stemrechten in uw onderneming uitoefenen of heeft een daarmee vergelijkbare zeggenschap.

Bij het bepalen van het aantal stemrechten dat iemand in een onderneming heeft, moeten de stemmen waarover hij beschikt of geacht wordt te beschikken worden meegerekend. De met stemrechten vergelijkbare zeggenschap kan bestaan uit bijvoorbeeld bijzondere rechten bij benoeming, ontslag of schorsing van het bestuur of de raad van commissarissen van uw onderneming.

Separaat vvgb-proces

Alvorens een vergunning aan uw onderneming kan worden verstrekt, dienen alle gekwalificeerde deelnemingen door DNB te zijn goedgekeurd door afgifte van de vereiste vvgb's. Voor een verklaring van geen bezwaar ten aanzien van gekwalificeerde deelneming(en), heeft DNB relevante gegevens nodig van de kwalificeerde aandeelhouder(s).

Let op: de betreffende aandeelhouders dienen deze informatie in een apart formulier via het Digitaal Loket Toezicht bij DNB aan te leveren. Het vvgb-proces loopt parallel aan de vergunningaanvraag. Bij complexe aandeelhoudersstructuren, bijvoorbeeld in het geval er meerdere partijen gelijktijdig vvgb-aanvragen moeten indienen, adviseren wij u om vooraf contact op te nemen met DNB om het proces te stroomlijnen. U kunt daarvoor een e-mail sturen naar: markttoegang@dnb.nl

Termijnen

De wettelijke beslistermijn voor een aanvraag van een vvgb bedraagt 62 werkdagen. Deze termijn kan met maximaal twintig of dertig werkdagen worden opgeschort indien DNB voor de behandeling van een vvgb-aanvraag additionele informatie nodig heeft. De beslistermijn vangt aan op de eerste werkdag nadat DNB een volledige vvgb-aanvraag (alle vereiste gegevens) heeft ontvangen.

Kosten

Aan een aanvraag van een vvgb zijn kosten verbonden. De tarieven zijn opgenomen in Bijlage I bij de Wet bekostiging financieel toezicht. De hoogte van de kosten is afhankelijk van het aantal bestede uren aan de behandeling van de aanvraag.

De kosten voor de vvgb-aanvraag worden in rekening gebracht bij degene die de gekwalificeerde deelneming verwerft of vergroot, ongeacht of de vvgb door DNB wordt verleend of afgewezen, of de vvgb-aanvraag door de aanvrager tussentijds wordt ingetrokken of door DNB tussentijds buiten behandeling wordt gesteld.

9 Zekerstelling van gelden van betaaldienstgebruikers

44

Dit onderdeel is niet op u van toepassing als u uitsluitend betaaldienst 7 en/of 8 aanbiedt.

Het is belangrijk dat uw onderneming bij het verlenen van betaaldiensten 1 t/m 6 waarborgt dat de gelden van betaaldienstgebruikers niet worden vermengd met het eigen vermogen van de onderneming. Op deze wijze voorkomt u dat schuldeisers van de onderneming (bijvoorbeeld in het geval van faillissement) beslag kunnen leggen op gelden van de betaaldienstgebruikers. De onderneming kan kiezen tussen twee methoden om derdengelden zeker te stellen.

Methode 1: stichting derdengelden

De gelden worden op een afzonderlijke rekening gestort die vervolgens niet door andere schuldeisers van uw onderneming kunnen worden aangesproken. In de praktijk betekent dit dat er een afgescheiden, onafhankelijke, bewaarder moet worden ingesteld die de desbetreffende gelden van betaaldienstgebruikers onder zicht houdt: een stichting derdengelden. Om de onafhankelijkheid van de stichting derdengelden en de afscheiding van de gelden zo goed mogelijk te borgen, is het van belang dat de stichting voldoet aan de volgende voorwaarden.

- **Betrouwbaarheid van de bestuurders van de stichting derdengelden:** De betrouwbaarheid van de bestuurders van de stichting derdengelden staat buiten twijfel.
- **Passende en beperkte doelomschrijving:** in de statuten van de stichting derdengelden is het doel van de stichting, namelijk het ontvangen, beheren en doorbetalen van derdengelden, concreet en ondubbelzinnig omschreven.
- **Geen commerciële activiteiten:** In het verlengde van de doelstelling van de stichting derdengelden, mag de stichting geen eigen commerciële activiteiten verrichten, leningen verstrekken of andersoortige financiële verplichtingen aangaan. Op deze wijze wordt voorkomen dat er vorderingen van derden op de stichting kunnen ontstaan.
- **Prudente omgang met de liquide middelen van betaaldienstgebruikers:** voor zover middelen gedurende de bewaarperiode worden belegd, dienen deze te worden belegd in veilige en liquide assets met een lage risicograad. De onderneming moet tevens waarborgen dat de liquide middelen van de stichting op elk moment ten minste gelijk zijn aan de verplichtingen van de Onderneming ten opzichte van de betaaldienstgebruikers (reconciliatie). Tot slot mag geen sprake zijn van voorfinanciering door de stichting, bijvoorbeeld wanneer de stichting gelden uitbetaalt aan de gebruiker vóórdat deze gelden zijn ontvangen.

DNB vindt het van groot belang dat sprake is van adequate functiescheiding en dat geen belangenverstrengeling mogelijk is tussen de betaalinstantie en de stichting derdengelden. Daartoe is het onder meer van belang om te voorkomen dat degenen die ten behoeve van de stichting derdengelden (bestuurs)werkzaamheden verrichten tevens werkzaam zijn voor het bedrijfsdeel van de financiële onderneming dat betalingstransacties verricht, of daarvoor (eind) verantwoordelijkheid dragen.

Als u voor deze methode kiest, verwachten wij van u een verklaring in hoeverre voldaan aan artikel 10 van PSD2. Daarnaast verwachten een beschrijving van het aantal personen dat toegang heeft tot de afgeschermdere rekeningen en de functies van deze personen. Ook verwachten een beschrijving van het administratie- en afstemmingsproces waarmee wordt gewaarborgd dat geldmiddelen van gebruikers van de betalingsdienst in het belang van de betalingsdienstgebruikers zijn gevrijwaard tegen de vorderingen van andere schuldeisers van de betaalinstantie, in het bijzonder in het geval van insolventie.

Methode 2: verzekeringspolis of vergelijkbare garantie

Als u voor deze methode kiest, verwachten wij een verklaring dat de geldmiddelen worden gedekt door een verzekeringspolis of een vergelijkbare garantie van een verzekeraar of bank die niet tot dezelfde groep behoort als uw onderneming. De polis of garantie beschermt tegen het risico dat de betaalonderneming niet in staat is haar verplichtingen met betrekking tot de geldmiddelen na te komen. Daarnaast verwachten we ook een gedetailleerde beschrijving van het afstemmingsproces waaruit blijkt dat verzekeringspolis of een vergelijkbare garantie van een verzekeraar of bank van voldoende dekking en kwaliteit is om de verplichting tot veiligstelling van uw onderneming te allen tijde te voldoen. [Link naar Open Boek?](#)

10 Minimum eigen vermogen en solvabiliteit

46

10.1 Minimum eigen vermogen

Dit vereiste is niet op uw onderneming van toepassing indien u uitsluitend dienst 8 aanbiedt.

Uw onderneming beschikt bij vergunningverlening over een aanvangskapitaal ter hoogte van de hoogste uitkomst die volgt uit de volgende berekeningen:

Het aanvangskapitaal van uw onderneming bedraagt:

EUR 125.000, bij het verlenen van betaaldienst:

- 1 t/m 5; of
- 1 t/m 5 in combinatie met 6, 7 en/of 8;

EUR 50.000, bij het verlenen van betaaldienst:

- 7; of
- 7 in combinatie met dienst 6 en/of in combinatie met dienst 8;

EUR 20.000, bij het verlenen van betaaldienst:

- 6; of
- 6 in combinatie met dienst 8.

Het eigen vermogen van uw onderneming mag niet kleiner worden dan het bedrag van het hierboven bedoelde aanvangskapitaal. Wij verwachten dat u bij de aanvraag gedetailleerde informatie over de positie van het eigen vermogen van uw onderneming aanlevert zoals vermeld op het aanvraagformulier.

Let op: bij de berekening van het eigen vermogen dient u rekening te houden met de voor het eigen vermogen kwalificerende kapitaalinstrumenten. Dit zijn kapitaalinstrumenten zoals bedoeld in artikel 26 van de Capital Requirements Regulation (CRR).

10.2 Aan te houden toetsingsvermogen (eigen vermogen in het kader van solvabiliteit)

Dit vereiste is niet op uw onderneming van toepassing indien u uitsluitend dienst 7 en/of 8 aanbiedt.

Uw onderneming moet beschikken over voldoende eigen vermogen in het kader van solvabiliteit. Het aan te houden eigen vermogen in het kader van solvabiliteit wordt uitgedrukt in toetsingsvermogen. De methode voor de berekening van de minimumomvang van het

toetsingsvermogen wordt bepaald op basis van de betaaldiensten die uw onderneming uitvoert. De minimumomvang van dit toetsingsvermogen wordt doorgaans berekend volgens 'methode B'. Bij methode B is het toetsingsvermogen van de onderneming afhankelijk van het betalingsvolume. Wij vragen u echter berekeningen conform alle drie de methodes (A, B en C) aan te leveren.

Op de statistiek-pagina van DNB (<https://www.dnb.nl/statistiek/digitaal-loket-rapportages/toezicht-rapportages/betaalinstellingen-en-elektronischgeldinstellingen/index.jsp#>) vindt u informatie over de prudentiële rapportages. In de prudentiële rapportages is de berekening en controle van het toetsingsvermogen opgenomen. Onder het kopje gebruikersdocumentatie vindt u de 'invoer templates' voor de prudentiële rapportages. Wij vragen u de prudentiële rapportages (invoer templates) voor de komende drie jaren (en in lijn met uw financiële prognoses, zie hoofdstuk 3) in te vullen.

Let op: bij de berekening van het toetsingsvermogen dient u rekening te houden met een aantal aftrekposten. Dit zijn aftrekposten zoals bedoeld in artikel 36 e.v. van de Capital Requirements Regulation (CRR). Bijvoorbeeld: immateriële vaste activa. Deze activa worden gezien als 'zachte' activa die in tijden van stress nauwelijks een buffer voor verliezen bieden. Maar ook onder meer winsten van het lopende boekjaar die nog niet door een accountantscontrole zijn bevestigd en uitgestelde belastingvorderingen die op toekomstige winstgevendheid berusten. Wij vragen uw verscherpte aandacht hiervoor. Onze ervaring leert, dat dit vaak over het hoofd wordt gezien.

Zie voor meer informatie de Handleiding prudentiële rapportage.

11 Aansprakelijkheidsverzekering

48

Dit vereiste is uitsluitend op uw onderneming van toepassing indien u dienst 7 en/of 8 aanbiedt.

Let op: indien uw onderneming ook een vergunning heeft of heeft aangevraagd voor dienst 1 t/m 6, dan geldt de eis van de aansprakelijkheidsverzekering bovenop de eisen ten aanzien van het minimum eigen vermogen en aan te houden toetsingsvermogen.

Indien uw onderneming betaalinitiatiediensten en/of rekeninginformatiediensten gaat aanbieden, dient u te beschikken over een beroepsaansprakelijkheidsverzekering of een vergelijkbare waarborg. Meer informatie over de vergelijkbare waarborg is te vinden op Open Boek Toezicht: <http://www.toezicht.dnb.nl/3/50-237165.jsp>

De te verzekeren aansprakelijkheid en de hoogte van de dekking van deze verzekering zijn afhankelijk van het type dienstverlening. Zo dient er bij het aanbieden van betaalinitiatiediensten (dienst 7) bijvoorbeeld voldoende dekking te zijn in het geval van aansprakelijkheid voor niet-toegestane betalingstransacties, voor de niet-uitvoering, gebrekkige uitvoering of niet-tijdige uitvoering van betalingstransacties. En dient er bij het aanbieden van rekeninginformatiediensten (dienst 8) bijvoorbeeld voldoende dekking te zijn voor aansprakelijkheid jegens de rekeninghoudende betaaldienstverlener voor niet-geautoriseerd of frauduleus gebruik van rekeninginformatie.

Minimale dekking

De minimale hoogte van de dekking wordt berekend aan de hand van de volgende formule:

Minimale dekking = het bedrag passend bij het risicoprofiel + het bedrag passend bij het type activiteiten + het bedrag passend bij de omvang van de activiteiten.

Risicoprofiel

Het bedrag passend bij het risicoprofiel kan worden berekend door te kijken naar de totale waarde van de verzoeken tot terugstorten door de betaaldienstgebruiker en/of rekeninghoudende betaalinstantie in de afgelopen 12 maanden. Zijn er geen verzoeken ingediend in de afgelopen 12 maanden en was uw onderneming al wel actief in deze periode, dan kunt u hier als waarde 0 gebruiken. Indien er nog geen diensten zijn verleend in de afgelopen 12 maanden, kan er gekeken worden naar de waarde van het voorspelde aantal verzoeken tot terugstorten. Wordt er geen opgave gedaan of is de voorspelde waarde lager dan EUR 50.000, dan gaat DNB uit van een fictieve waarde van EUR 50.000.

Onderdeel van het risicoprofiel is het aantal geïnitieerde transacties of het aantal bekeken rekeningen in de afgelopen 12 maanden. Voor betaalinitiatiedienstverleners wordt dit als volgt berekend:

- 40% van de eerste 10.000 geïnitieerde transacties;
- plus 25% van het aantal tussen 10.000 en 100.000 geïnitieerde transacties;
- plus 10% van het aantal tussen 100.000 en 1 miljoen geïnitieerde transacties;
- plus 5% van het aantal tussen 1 en 10 miljoen geïnitieerde transacties;
- plus 0,025% van het aantal boven 10 miljoen geïnitieerde transacties.

Mocht uw onderneming nog niet actief zijn, dan kan gekeken worden naar het aantal voorspelde geïnitieerde transacties. Is er niets ingevuld of is het aantal lager dan 50.000, dan gaat DNB uit van 50.000 transacties.

Eenzelfde manier van berekenen wordt toegepast ten aanzien van het aantal bekeken rekeningen door een rekeninginformatiedienst. Waarbij het aantal geïnitieerde transacties kan worden gelezen als het aantal bekeken rekeningen in de afgelopen 12 maanden.

Type activiteit

Het bedrag dat past bij het type activiteiten wordt als volgt gewaardeerd: indien enkel een vergunning voor dienst 7 ofwel dienst 8 aanvraagt, kan hiervoor het getal 0 worden gebruikt. Indien uw onderneming ook een vergunning heeft of heeft aangevraagd voor dienst 1 t/m 6, dan geldt de eis van de aansprakelijkheidsverzekering bovenop de eisen ten aanzien van startkapitaal en minimum eigen vermogen. Indien uw onderneming ook andere zakelijke activiteiten ontplooit dan het aanbieden van betaaldiensten zoals bedoeld in bijlage 1 van de betaalrichtlijn, dan wordt er EUR 50.000 aan waarde toegevoegd aan de formule, tenzij uw onderneming kan aantonen dat de risico's geen invloed hebben dienstverlening hetzij doormiddel van een garantie hetzij omdat de betaaldienstverleningsactiviteiten zijn ondergebracht in een separate entiteit.

Omvang van de activiteiten

Het bedrag dat in de formule ingevuld dient te worden voor de omvang van de activiteiten van een betaalinitiatiedienstverlener berekent u als volgt:

- 40% van het gedeelte van de totale waarde van alle transacties in de afgelopen 12 maanden (N), tussen de 0 en 500.000 euro;
- Plus 25% van het gedeelte van N tussen EUR 500.000 en 1.000.000;
- Plus 10% van het gedeelte van N tussen EUR 1.000.000 en 5.000.000;
- Plus 5% van het gedeelte van N tussen EUR 5.000.000 en 10.000.000;
- Plus 0,025% van het gedeelte van N boven EUR 10.000.000.

50 Voor het bedrag dat in de formule ingevuld dient te worden indien uw onderneming rekeninginformatiediensten aanbiedt, geldt de volgende berekening:

- 40% van het gedeelte van het totaal aantal gebruikers in de afgelopen 12 maanden (N) tussen de 1 en 100;
- Plus 25% van het gedeelte van N tussen 100 en 10.000 gebruikers;
- Plus 10% van het gedeelte van N tussen 10.000 en 100.000 gebruikers;
- Plus 5% van het gedeelte van N tussen 100.000 en 1.000.000 gebruikers;
- Plus 0,025% van het gedeelte van N boven de 1.000.000 gebruikers.

Indien de diensten in de afgelopen 12 maanden nog niet werden aangeboden dient uitgegaan te worden van de voorspelde waarde en/of aantallen. Indien er geen prognose beschikbaar is of de waarde en/of aantallen lager zijn dan 50.000, dan dient 50.000 te worden gehanteerd.

Bovenstaande berekeningen zijn gebaseerd op de door de EBA opgestelde '*Final Guidelines on Personal Indemnity Insurance under PSD2*', die gepubliceerd zijn op de website van de EBA.

Bijlage

Overzicht van de documenten die in het aanvraagformulier worden opgevraagd

Mocht u nog niet beschikken over e-herkenning en daardoor nog geen toegang hebben tot het Digitaal loket toezicht (DLT) dan geeft onderstaand overzicht u beeld van de verschillende bijlagen waar in aanvraagformulier om wordt verzocht. Dit overzicht bevat echter geen limitatieve opsomming/ gedetailleerd overzicht van alle vragen en motiveringen die in het aanvraagformulier staan opgenomen. Wij raden u dan ook aan om zo snel mogelijk e-herkenning aan te vragen zodat u het inkijkexemplaar van het aanvraagformulier erbij kan houden.

51

Plannen

- Programma van werkzaamheden en bedrijfsplan
- Herstel- en exitplan met scenarioanalyses
- Marketingplan

Overzichten

- Organogram
- Structuuroverzicht

Analyses

- Algemene risicoanalyse
- Systematische analyse van integriteitsrisico's (SIRA)
- Business Impact Analyse
- Analyse de identificatie en classificatie van bedrijfsfuncties, processen en resources met aandacht voor de Beschikbaarheid, de Integriteit en de Vertrouwelijkheid (CIA) van systemen, infrastructuur, data en processen
- Ingevulde exceltemplate FIN&CO REP betaalinstantellingen voor de komende 3 jaren (geldt niet voor dienst 7 en 8)

Overeenkomsten

- Kopie van de opdrachtovereenkomst met de accountant / het auditkantoor (geldt niet voor dienst 8)
- Kopie(ën) vanuitbestedingsovereenkomst(en)

Beleid

- Risicobeheerskingskader
- Compliance + charter voor de compliancefunctie
- Interne controlefunctie + charter voor de interne controlefunctie
- Uitbesteding
- Incidenten
- Business continuity management
- Beloningsbeleid
- Tegengaan van verstremgeling van privébelangen
- Integriteitsgevoelige functies

- Clientonderzoek
- Sanctieregelgeving
- Transactiemonitoring en melding ongebruikelijke transacties
- Opleidingsplan

Overig

- Uittreksel uit het Handelsregister van de KvK van de onderneming
- Een gewaarmerkt afschrift van de statuten van de onderneming
- Een kopie van actuele aandeelhoudersregister van de onderneming
- Stroomschema gelden (geldt niet voor dienst 7 en 8)
- Lijst van uitbestede activiteiten
- Procedurehandboek (uitwerking van beleid in procedures en maatregelen)
- Aansprakelijkheidsverzekering (eventueel)
- Gecertificeerde jaarrekening(en) of verklaring van accountant dat aan minimum eigen vermogens-eis en/of solvabiliteits-eis wordt voldaan
- Indien sprake van Stichting derdengelden: 1) Uittreksel van uit het Handelsregister van de KvK van de stichting derdengelden 2) Een gewaarmerkt afschrift van de statuten van de stichting derdengelden 3) Een beschrijving van de tussen de onderneming en de stichting derdengelden gemaakte afspraken of een kopie van de overeenkomst tussen de stichting derdengelden en de onderneming 4) Een verklaring waarin de onderneming bevestigt dat de stichting derdengelden aan een aantal voorwaarden voldoet. (geldt niet voor dienst 7 en 8)
- Indien sprake van verzekeringspolis of vergelijkbare garantie: kopie van de polis of garantie (geldt niet voor dienst 7 en 8)
- Documentatie waaruit het eigen vermogen van de onderneming blijkt: Bijv. gecertificeerde jaarrekening (goedgekeurd door accountant), oprichtingsakte, bankafschrift waaruit de storting van een bepaald kapitaalbedrag blijkt (geldt niet voor dienst 8)
- In het geval van een bestaande onderneming ontvangen wij graag gecertificeerde jaarrekeningen tot drie jaar terug of voor zover beschikbaar een overzicht van de financiële situatie indien de onderneming nog geen jaarrekeningen heeft voortgebracht (geldt niet voor dienst 7 en 8)
- Verzekeringspolis of vergelijkbare garantie (inclusief voorwaarden) (geldt niet voor dienst 1 t/m 6)
- Berekening waaruit blijkt dat de minimale omvang dekking in overeenstemming is met EBA Guideline CB/2016/12 (geldt niet voor dienst 1 t/m 6)

Let op: Separaat dient u in het kader van de vergunningaanvraag tevens de volgende aanvragen via het DLT in te dienen.

Toetsing op betrouwbaarheid en geschiktheid per te toetsen persoon:

53

- Aanvraagformulier Aanvangstoetsing
- Aanvraagformulier Betrouwbaarheidsonderzoek (verplicht indien niet eerder getoetst op betrouwbaarheid)(nog niet beschikbaar via het DLT, zie Open Boek Toezicht <http://www.toezicht.dnb.nl/4/2/16/50-229347.jsp>)

Verklaring van geen bezwaar per aandeelhouder (gekwalificeerde deelnemer):

- Aanvraag voor een verklaring van geen bezwaar – artikel 3:95 Wft

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl