



Wereldwijde Policy voor Gegevensbescherming van Klant-, Leverancier- en Zakenpartnergegevens

INFORMATIEBLAD

Doelgroep:

Alle klanten, leveranciers en zakenpartners van alle bedrijven (of bedrijfsonderdelen) waarvan ING de meerderheidsaandeelhouder is, bedrijven die onder controle van ING staan, en overkoepelende afdelingen.

Uitgegeven door:

ING Legal Department Bank (IT, Procurement & Privacy)

Versie:

1.0

Vervangt:

Deze ING Wereldwijde Policy voor Gegevensbescherming van Klant-, Leverancier- en Zakenpartnergegevens (de '**Policy**') vervangt elke policy en elke kennisgeving van ING inzake gegevensbescherming die bestaan op de Ingangsdatum voor zover zij dezelfde onderwerpen behandelen en niet in overeenstemming zijn met deze Policy.

Goedgekeurd door:

Bestuur Bank, ING Bank N.V. per 22 juli 2013

Ingangsdatum:

1 augustus 2013

Bij eventuele verschillen tussen de Engelse versie van deze Policy en deze vertaalde versie prevaleert het document in het Engels.

© ING Bank N.V. 2011

Dit document mag op geen enkele manier buiten ING verspreid worden zonder de voorafgaande schriftelijke toestemming van het ING Legal Department Bank (IT, Procurement & Privacy).

INHOUD

1. Inleiding
2. Doelstelling van deze Policy
3. Toepassingsgebied
4. Toepasselijkheid van lokaal recht en deze Policy
5. Implementatie
6. Doeleinden van de Verwerking van Persoonsgegevens
7. Gebruik voor andere Doeleinden
8. Verwerking van Bijzondere Gegevens
9. Kwantiteit en kwaliteit van Gegevens
10. Informatieverstrekking aan Betrokkenen
11. Recht op inzage, wijziging en verwijdering van Betrokkenen
12. Beveiligings- en vertrouwelijkheidsvereisten
13. Direct marketing
14. Automatische besluitvorming
15. Doorgifte van Persoonsgegevens aan Derden
16. Prevalerende Belangen
17. Toezicht en naleving
18. Verantwoordelijkheden
19. Policies en procedures
20. Opleiding
21. Monitoring van de naleving
22. Klachtenprocedure
23. Juridische kwesties
24. Sancties voor niet-naleving
25. Tegenstrijdigheden tussen deze Policy en toepasselijk lokaal recht
26. Wijzigingen in deze Policy
27. Overgangsperiodes

DEEL I ALGEMENE INLEIDING

1 Inleiding

1.1 Krachtens de Business Principles van ING worden alle werknemers geacht zorgvuldig om te springen met informatie. Met name de beveiliging en vertrouwelijkheid van de verwerking van alle aan ING toebehorende zakelijke informatie en gegevens, inclusief van vertrouwelijke persoonsgegevens, moet worden gewaarborgd in overeenstemming met de geldende wet- en regelgeving. Deze Policy legt uit dat de bescherming van persoonsgegevens het volgende inhoudt:

- Transparant zijn over wat ING doet met klant-, leverancier- en zakenpartnergegevens.
- Persoonsgegevens uitsluitend verwerken voor specifieke bedrijfsdoeleinden.
- Bijzondere gegevens worden alleen gebruikt wanneer nodig en wettelijk toegelaten.
- Erop toezien dat persoonsgegevens actueel, juist en nauwkeurig zijn.
- Klanten, leveranciers en zakenpartners worden geïnformeerd over de doeleinden waarvoor hun persoonsgegevens verwerkt worden en welke ING-vennootschap verantwoordelijk is voor de verwerking.
- Klanten, leveranciers en zakenpartners de mogelijkheid bieden een overzicht van hun persoonsgegevens te krijgen.
- Klanten, leveranciers en zakenpartners de mogelijkheid bieden hun persoonsgegevens te corrigeren, verwijderen of afschermen.
- De persoonsgegevens beschermen tegen onrechtmatig verlies, wijziging, bekendmaking of toegang.
- Persoonsgegevens enkel bekendmaken aan derden in overeenstemming met deze Policy.

Anders gezegd: de juiste **MENSEN** gebruiken de juiste **GEGEVENS** voor de juiste **DOELEINDEN**.

Voor de privacyregels die van toepassing zijn op persoonsgegevens van werknemers, verwijzen we naar de ING Wereldwijde Policy voor Gegevensbescherming van Werknemers (**'Policy Gegevensbescherming voor Werknemers'**). Deze Policy heeft uitsluitend betrekking op de persoonsgegevens van Betrokkenen die onze klant, leverancier of zakenpartner zijn en op hun werknemers. Deze Policy heeft geen betrekking op enige andere gegevens over bedrijven, instellingen of overheden die onze klant, leverancier of zakenpartner zijn, behalve waar lokaal recht anders bepaalt. De Policy gaat niet over verplichtingen die op ING van toepassing kunnen zijn krachtens lokaal bankgeheim en ander toepasselijk recht.

De termen die in deze Policy met hoofdletter worden geschreven, worden toegelicht in Bijlage 1. Uitvoeriger richtlijnen zijn beschikbaar in de Guidance Documenten die Medewerkers kunnen raadplegen via het intranet van ING.

2 Doelstelling van deze Policy

2.1 Deze Policy is bedoeld als duidelijke boodschap met betrekking tot de bescherming van Gegevens van Klanten, Leveranciers en Zakenpartners om een passend beschermingsniveau te bewerkstelligen voor alle Gegevens van Klanten, Leveranciers en Zakenpartners die door ING wereldwijd verwerkt worden.

3 Toepassingsgebied

- 3.1** Deze Policy behandelt de Verwerking van alle Persoonsgegevens van Klanten, Leveranciers en Zakenpartners door ING, of door een Derde namens ING wereldwijd in overeenstemming met Artikel 15. Deze Policy handelt niet over de Verwerking van Gegevens van Werknemers van ING.

Elektronische en papieren Verwerking

- 3.2** Deze Policy is van toepassing op de Verwerking van Persoonsgegevens langs elektronische weg en in systematisch raadpleegbare papieren archiefsystemen.

Advies van de Data Protection Executive

- 3.3** Medewerkers die vragen hebben over de toepasselijkheid van deze Policy, moeten het advies inwinnen van de bevoegde Data Protection Executive alvorens tot verwerking over te gaan.

Verantwoordelijkheid voor de naleving

- 3.4** Deze Policy is van kracht wanneer ING Verantwoordelijke is. De Data Protection Executive is verantwoordelijk voor de naleving van deze Policy door ING. Medewerkers moeten deze Policy naleven. De Policy is niet van toepassing wanneer ING Bewerker is.

4 Toepasselijkheid van lokaal recht en deze Policy

Betrokkenen behouden lokale rechten en rechtsmiddelen

- 4.1** Betrokkenen behouden alle rechten en rechtsmiddelen die zij krachtens toepasselijk lokaal recht hebben. Deze Policy is alleen van toepassing wanneer het aanvullende bescherming voor Persoonsgegevens biedt. Wanneer toepasselijk lokaal recht meer bescherming biedt dan deze Policy, is het lokale recht van toepassing. Wanneer deze Policy meer bescherming biedt dan toepasselijk lokaal recht of voorziet in aanvullende waarborgen, rechten of rechtsmiddelen voor Betrokkenen, is deze Policy van toepassing.

Minimumnormen en kennisgevingen

- 4.2** ING kan deze Policy aanvullen met minimumnormen of kennisgevingen die in overeenstemming zijn met deze Policy, zowel lokaal als door ING Bank N.V. Indien ING die minimumnormen of kennisgevingen van de Policy wijzigt en als gevolg daarvan wezenlijke wijzigingen aan de Policy nodig zijn, zal ING het Nederlandse College Bescherming Persoonsgegevens op de hoogte brengen van die wezenlijke wijzigingen aan de Policy in overeenstemming met Artikel 26.1.

5 Implementatie

Ingangsdatum

- 5.1** Deze Policy werd goedgekeurd door de Raad van Bestuur van ING Bank N.V. en treedt in werking op 1 augustus 2013 ('Ingangsdatum') en wordt gepubliceerd op de website en het intranet van ING en wordt tevens op aanvraag aan Betrokkenen verstrekt.

Policy vervangt eerdere policies

- 5.2** Deze Policy vervangt elke policy en elke kennisgeving van ING betreffende gegevensbescherming die bestaan op de Ingangsdatum voor zover zij dezelfde onderwerpen behandelen en niet in overeenstemming zijn met deze Policy of minder strenge eisen opleggen dan de Policy.

Implementatie

- 5.3** Deze Policy wordt geïmplementeerd in de organisatie van ING volgens het tijdschema vermeld in Artikel 27.

6 Doeleinden van de Verwerking van Persoonsgegevens

Beleidsbepaling

ING verzamelt, gebruikt of anderszins Verwerkt Persoonsgegevens met betrekking tot Klanten, Leveranciers en Zakenpartners alleen indien de Verwerking binnen het toepassingsgebied van een (of meer) hierna vermelde gerechtvaardigde Bedrijfsdoeleinden valt:

Gerechtvaardigde Bedrijfsdoeleinden

6.1 Persoonsgegevens worden verzameld, gebruikt, bewaard of anderszins Verwerkt wanneer nodig,

- in het kader van verantwoordelijke, efficiënte en doeltreffende bedrijfsvoering, in het bijzonder voor volgende activiteiten:
 - **de uitvoering van overeenkomsten:** evalueren en aanvaarden van Klanten, het aangaan en uitvoeren van overeenkomsten met Klanten, Zakenpartners en Leveranciers, het uitvoeren van betalingen en andere financiële transacties en het vastleggen en financieel afrekenen van aan door ING geleverde diensten, producten en materialen, met inbegrip van communicatie met Betrokkenen en andere partijen die bij contracten betrokken zijn (verzekerde personen, begunstigten, tussenpersonen) en antwoorden op verzoeken om (nadere) informatie van Klanten, Zakenpartners of Leveranciers, geschillen en rechtszaken afhandelen;
 - **relatiebeheer en marketing:** voor commerciële activiteiten, met inbegrip van de verwerking die nodig is voor de ontwikkeling en verbetering van producten en/of diensten van ING, klantenbeheer, dienstverlening aan klanten en de uitvoering van (gerichte) marketingactiviteiten teneinde een relatie aan te gaan met een Klant en/of een relatie met een Klant, Zakenpartner of Leverancier in stand te houden of uit te breiden, en om analyses te doen met betrekking tot persoonsgegevens voor statistische en wetenschappelijke doeleinden;
 - **de uitvoering van bedrijfsprocessen, intern beheer en managementrapportering:** activiteiten zoals de bedrijfsmiddelen beheren, interne audits en onderzoeken voeren, financieel beheer en boekhouding, implementeren van interne controlemechanismen op de bedrijfsvoering, centrale verwerkingsinfrastructuur ter beschikking stellen voor efficiëntie-doeleinden, fusies, overnames en afsplitsingen beheren, en Persoonsgegevens Verwerken voor managementrapportering en analyse;
 - **veiligheid en beveiliging:** dit doeleinde betreft activiteiten op het vlak van veiligheid en gezondheid, de bescherming van de activa van ING en Klanten, Leveranciers of Zakenpartners en de authenticatie van de status en toegangsrechten van Klanten, Leveranciers of Zakenpartners;
 - **de vitale belangen van Betrokkenen beschermen:** dit betreft Verwerking die nodig is om de vitale belangen van een Betrokkene te beschermen, bijvoorbeeld om dringende medische redenen;
 - **de naleving van wettelijke verplichtingen:** dit betreft de Verwerking van Persoonsgegevens die nodig is voor de naleving van wet- en regelgeving en sectorspecifieke richtlijnen die op ING van toepassing zijn.
- ter ondersteuning van de activiteiten om de veiligheid en integriteit van ING en/of de financiële sector te vrijwaren en garanderen, met inbegrip van volgende activiteiten:

- (i) activiteiten die een negatieve invloed kunnen hebben op financiële instellingen en ING identificeren, voorkomen en onderzoeken, met inbegrip van maar niet beperkt tot:
 - (i) misbruik van producten, diensten en faciliteiten van financiële instellingen;
 - (ii) (pogingen tot) strafbaar of anderszins negatief gedrag;
 - (iii) schendingen van (wettelijke) voorschriften;
- (ii) (pogingen tot) (strafbaar of ongewenst) gedrag ten opzichte van de financiële sector, ING Bank N.V., Groepsentiteiten, Klanten en Medewerkers afweren, voorkomen en opsporen;
- (iii) waarschuwingssystemen gebruiken en eraan deelnemen (inclusief sectorspecifieke waarschuwingssystemen);
- (iv) wettelijke bepalingen naleven, zoals de regelgeving inzake witwassen en de financiering van terrorisme.

Wanneer er onzekerheid bestaat of een Verwerking van Persoonsgegevens gebeurt voor een van de hiervoor genoemde Bedrijfsdoeleinden, moet het advies gevraagd worden van de bevoegde Data Protection Executive alvorens tot Verwerking over te gaan.

6.2 Toestemming van Betrokkenen

Indien geen Bedrijfsdoeleinde bestaat of indien toepasselijk lokaal recht dit vereist, zal ING Persoonsgegevens alleen Verwerken met de toestemming van de Betrokkene. Indien geen Bedrijfsdoeleinde bestaat en een specifieke Verwerking plaatsvindt op verzoek van een Betrokkene (bv. hij neemt een abonnement op een dienst of wil gebruikmaken van een benefit), wordt hij geacht zijn toestemming te hebben gegeven voor de Verwerking in kwestie.

De Betrokkene zal worden gewezen op:

- (a) De doeleinden van de Verwerking waarvoor toestemming gevraagd wordt of geacht wordt te zijn gegeven.
- (b) Andere relevante informatie die de Betrokkene nodig heeft om een bewuste beslissing over de Verwerking van zijn Persoonsgegevens te maken (bijvoorbeeld de aard en categorieën van de Verwerkte Gegevens, de categorieën van (eventuele) Derden aan wie de Gegevens worden bekendgemaakt en hoe Betrokkenen hun rechten kunnen uitoefenen).

Weigering of intrekking van toestemming

- 6.3 De Betrokkene kan te allen tijde zijn toestemming weigeren en intrekken.

Beperkingen op de Verwerking van Gegevens van Gezinsleden van Betrokkenen

- 6.4 ING Verwerkt Gegevens van Gezinsleden van een Betrokkene indien:

- (i) De Gegevens werden verstrekt met de toestemming van de Betrokkene of het Gezinslid; of
- (ii) De Verwerking van de Gegevens redelijkerwijs nodig is voor de uitvoering van een overeenkomst met de Betrokkene; of
- (iii) De Verwerking krachtens toepasselijk lokaal recht is verplicht of toegestaan.

7 Gebruik voor andere Doeleinden

Beleidsbepaling

ING gebruikt Persoonsgegevens in beginsel alleen voor de doeleinden waarvoor zij oorspronkelijk werden verzameld, maar kan de Gegevens ook gebruiken voor andere, aanverwante doeleinden volgens de voorwaarden uiteengezet in dit Artikel (7).

Gebruik van Gegevens voor Secundaire Doeleinden

- 7.1** Over het algemeen worden Persoonsgegevens alleen gebruikt voor de doeleinden waarvoor zij oorspronkelijk werden verzameld (**Oorspronkelijk Doeleinde**). Persoonsgegevens mogen alleen Verwerkt worden voor gerechtvaardigde doeleinden van ING die verschillen van het Oorspronkelijke Doeleinde (**Secundair Doeleinde**) als het Oorspronkelijke Doeleinde en het Secundaire Doeleinde nauw verband houden met elkaar én het gebruik van Gegevens voor Secundaire Doeleinden is toegestaan krachtens toepasselijk recht. Afhankelijk van de gevoeligheid van de Persoonsgegevens in kwestie en de vraag of het gebruik van de Gegevens voor het Secundaire Doeleinde potentieel negatieve gevolgen heeft voor de Betrokkene, kunnen voor het secundaire gebruik een of meer aanvullende maatregelen nodig zijn, zoals:
- (i) Toegang tot de Gegevens beperken
 - (ii) Aanvullende vertrouwelijkheidsvereisten opleggen
 - (iii) Aanvullende beveiligingsmaatregelen nemen
 - (iv) De Betrokkene informeren over het Secundaire Doeleinde
 - (v) De mogelijkheid tot opt-out bieden; of
 - (vi) Toestemming van de Betrokkene krijgen in overeenstemming met Artikel 6.2, indien dat krachtens toepasselijk recht verplicht is.

Over het algemeen toegestaan gebruik van Gegevens voor Secundaire Doeleinden

- 7.2** Het is over het algemeen toegelaten Persoonsgegevens te gebruiken voor de volgende Secundaire Doeleinden, op voorwaarde dat gepaste aanvullende maatregelen getroffen worden in overeenstemming met Artikel 7.1:
- (i) verplaatsen van de Gegevens naar een Archief; of
 - (ii) interne audits of onderzoeken; of
 - (iii) implementatie van interne controlemechanismen op de bedrijfsvoering; of
 - (iv) statistisch, historisch of wetenschappelijk onderzoek; of
 - (v) geschillen of rechtszaken afhandelen; of
 - (vi) juridisch of bedrijfsadvies; of
 - (vii) verzekeringsdoeleinden.

Advies van de Data Protection Executive

- 7.3** Alvorens Persoonsgegevens te Verwerken voor een Secundair Doeleinde, moeten Medewerkers het advies inwinnen van de bevoegde Data Protection Executive.

8 Verwerking van Bijzondere Gegevens

Beleidsbepaling

ING gebruikt Bijzondere Gegevens uitsluitend voor een van de doeleinden vermeld in dit Artikel (8), en alleen voor zover dat nodig is voor het Bedrijfsdoeleinde in kwestie, het Secundaire Doeleinde of de doeleinden waarvoor de Betrokkene zijn toestemming heeft gegeven in overeenstemming met Artikel 6.2, 6.3 of 7.1 ('de gerechtvaardigde doeleinden') en voor zover krachtens toepasselijk recht verplicht of toegelaten.

Specifieke doeleinden voor de Verwerking van Bijzondere Gegevens

- 8.1** Dit Artikel zet specifieke regels uiteen voor de Verwerking van Bijzondere Gegevens. ING Verwerkt alleen Bijzondere Gegevens voor zover dat nodig is voor de toepasselijke gerechtvaardigde doeleinden.

De volgende categorieën van Bijzondere Gegevens kunnen worden verzameld, gebruikt of anderszins Verwerkt voor een (of meer) van onderstaande doeleinden:

- (i) **Raciale of etnische gegevens** (met inbegrip van afbeeldingen en bewegende beelden van een Betrokkene): in sommige landen gelden foto's en videobeelden van Betrokkenen als raciale of etnische gegevens. ING kan foto's en videobeelden van Betrokkenen verwerken (i) voor opname in Klanten-, Leveranciers- en Zakenpartnerbestanden en (ii) voor toegang tot en beveiliging van locaties en (iii) om te voldoen aan wettelijke verplichtingen (bv. screening van klanten).
- (ii) **Gegevens over de fysieke of mentale gezondheid**; om Klanten te beoordelen en aanvaarden, een overeenkomst met een Klant aan te gaan en uit te voeren en om betalingen en andere financiële transacties uit te voeren.
- (iii) **Strafrechtelijke gegevens** (met inbegrip van gegevens inzake crimineel gedrag, strafrechtelijke gegevens of rechtszaken met betrekking tot strafbaar of onwettig gedrag); om de belangen van ING te beschermen ten opzichte van strafbare feiten die jegens ING of haar Werknemers zijn begaan of waarvan gezien de relevante omstandigheden vermoed worden dat ze zijn begaan.
- (iv) **Burgerservicenummer** (of andere identificatienummers, met inbegrip van paspoortnummers): om wettelijke verplichtingen na te leven, bv. inzake de identificatie en authenticatie van klanten.

Algemene Doeleinden voor de Verwerking van Bijzondere Gegevens

8.2 Naast de specifieke doeleinden vermeld in Artikel 8.1 hiervoor mogen alle categorieën van Bijzondere Gegevens uitsluitend worden verwerkt indien aan (een of meer van) volgende voorwaarden voldaan is:

- (i) De Betrokkene heeft zijn uitdrukkelijke toestemming gegeven voor de Verwerking ervan.
- (ii) De Verwerking is verplicht of toegelaten krachtens toepasselijk lokaal recht.
- (iii) De Verwerking is nodig om een rechtsvordering vast te stellen, uit te oefenen of te verdedigen.
- (iv) De Verwerking is nodig om een vitaal belang van een Betrokkene te beschermen, maar alleen wanneer het onmogelijk is eerst de toestemming van de Betrokkene te krijgen; of
- (v) De Verwerking is nodig om te voldoen aan een internationale publiekrechtelijke verplichting (bv. verdragen); of
- (vi) De Bijzondere Gegevens zijn overduidelijk publiek gemaakt werden door de Betrokkene.

Voorafgaande autorisatie van de Data Protection Executive

8.3 Wanneer Bijzondere Gegevens worden Verwerkt op grond van een andere wettelijke verplichting dan lokaal recht dat op de Verwerking van toepassing is, of op grond van de toestemming van de Betrokkene, is voor de Verwerking de voorafgaande toestemming van de bevoegde Data Protection Executive nodig.

Gebruik van Bijzondere Gegevens voor Secundaire Doeleinden

8.4 Naast de vereisten van dit Artikel (8) kunnen Bijzondere Gegevens van Betrokkenen Verwerkt worden voor Secundaire Doeleinden in overeenstemming met Artikel 7.

9 Kwantiteit en kwaliteit van Gegevens

Beleidsbepaling

ING Verwerkt geen Persoonsgegevens die niet redelijkerwijs nodig of anderszins relevant zijn voor de gerechtvaardigde doeleinden waarvoor ING Persoonsgegevens verwerkt. ING levert redelijke inspanningen om te waarborgen dat de Gegevens nauwkeurig, juist en actueel zijn. ING bewaart

Persoonsgegevens alleen voor de duur die voor de toepasselijke doeleinden nodig is of om wettelijke redenen.

Geen Bovenmatige Gegevens

- 9.1** ING beperkt de Verwerking van Persoonsgegevens tot die Gegevens die redelijkerwijs adequaat en relevant zijn voor de toepasselijke gerechtvaardigde doeleinden. ING neemt redelijke stappen om Persoonsgegevens die voor die gerechtvaardigde doeleinden niet nodig zijn, veilig te verwijderen.

Bewaartermijn

- 9.2** ING bewaart over het algemeen Persoonsgegevens alleen:
- (a) Voor de duur die nodig is voor de gerechtvaardigde doeleinden waarvoor de Persoonsgegevens worden Verwerkt; of
 - (b) Voor zover redelijkerwijs nodig is om te voldoen aan een toepasselijke wettelijke verplichting; of
 - (c) Zoals raadzaam is gelet op een toepasselijke verjaringstermijn.

ING kan (bijvoorbeeld in een minimumnorm, kennisgeving of regeling voor gegevensbewaring) een termijn stellen waarin bepaalde categorieën van Persoonsgegevens kunnen worden bewaard.

Prompt nadat de toepasselijke bewaartermijn is verstreken, geeft de Data Protection Executive de opdracht om de Gegevens:

- (i) Veilig te verwijderen of vernietigen in overeenstemming met de relevante Corporate ORM-policies.
- (ii) Te anonimiseren; of
- (iii) Te verplaatsen naar een Archief (tenzij dit krachtens wetgeving of een geldende regeling voor gegevensbewaring verboden is).

Gegevenskwaliteit

- 9.3** Persoonsgegevens moeten nauwkeurig, juist en actueel gehouden worden voor zover dat redelijkerwijs nodig is voor de toepasselijke gerechtvaardigde doeleinden waarvoor de Persoonsgegevens worden Verwerkt.

Nauwkeurige, juiste en actuele Gegevens

- 9.4** Het is de verantwoordelijkheid van ING om de Persoonsgegevens van Betrokkenen nauwkeurig, juist en actueel te houden. Het is de verantwoordelijkheid van Betrokkenen om ING te informeren over veranderingen van hun Persoonsgegevens.

10 Informatieverstrekking aan Betrokkenen

Beleidsbepaling

ING ziet erop toe dat Betrokkenen adequaat geïnformeerd worden over de Bedrijfsdoeleinden waarvoor hun Persoonsgegevens worden Verwerkt, en verstrekt de Betrokkenen alle andere eventueel vereiste informatie met betrekking tot de Verwerking in kwestie.

Informatievereisten

- 10.1** ING informeert Betrokkenen via een policy of kennisgeving inzake gegevensbescherming over:
- (i) De Bedrijfsdoeleinden waarvoor hun Gegevens worden Verwerkt.
 - (ii) Welke Groepentiteit verantwoordelijk is voor de Verwerking; en

- (iii) Andere relevante informatie (bv. de aard en categorieën van de Verwerkte Gegevens, de categorieën van (eventuele) Derden aan wie de Gegevens worden bekendgemaakt en hoe Betrokkenen hun rechten kunnen uitoefenen).

Persoonsgegevens niet verkregen van de Betrokkene

10.2 Indien toepasselijk lokaal recht dit vereist, verstrekt ING, wanneer Persoonsgegevens niet rechtstreeks van de Betrokkene werden verkregen, de Betrokkene de informatie vermeld in Artikel 10.1:

- (i) Op het ogenblik dat de Persoonsgegevens worden vastgelegd in een database van ING; of
- (ii) Op het ogenblik dat de Persoonsgegevens worden gebruikt voor een mailing, op voorwaarde dat die mailing gebeurt binnen zes maanden nadat de Persoonsgegevens werden vastgelegd in een database van ING.

Uitzonderingen

10.3 De verplichtingen uit Artikel 10.2 kunnen wegvallen indien:

- (i) Het onmogelijk is of een buitensporige inspanning zou vergen om de informatie aan Betrokkenen te verstrekken; of
- (ii) Zij leiden tot buitensporige kosten.

11 Recht op inzage, wijziging en verwijdering van Betrokkenen

Beleidsbepaling

Dit Artikel betreft bepaalde rechten van Betrokkenen van wie de Persoonsgegevens worden Verwerkt door ING in zijn rol als Verantwoordelijke.

Rechten van Betrokkenen

11.1 Iedere Betrokkene heeft het recht om een overzicht te vragen van zijn Persoonsgegevens die door of namens ING Verwerkt worden. Waar redelijkerwijs mogelijk bevat dit overzicht informatie over de bron, het type, het doeleinde en de categorieën van ontvangers van de Persoonsgegevens in kwestie. Indien de Persoonsgegevens onjuist of onvolledig zijn of niet Verwerkt worden in overeenstemming met toepasselijk recht of deze Policy, heeft de Betrokkene het recht om zijn Gegevens te laten corrigeren, verwijderen of afschermen (naargelang de situatie). Bovendien heeft de Betrokkene het recht om bezwaar aan te tekenen tegen de Verwerking van zijn Gegevens op grond van dwingende redenen met betrekking tot zijn individuele situatie.

Procedure

11.2 De Betrokkene moet zijn aanvraag sturen naar de contactpersoon of het aanspreekpunt dat is vermeld in de relevante privacyverklaring. Indien geen contactpersoon of aanspreekpunt wordt vermeld, kan de Betrokkene zijn aanvraag sturen naar de relevante Groepsentiteit met behulp van de contactgegevens in de algemene contactrubriek van de lokale ING-website.

Alvorens aan de aanvraag van de Betrokkene te voldoen, kan ING de Betrokkene vragen om:

- (i) Op te geven in welk type Persoonsgegevens hij inzage wenst.
- (ii) Voor zover redelijkerwijs mogelijk op te geven in welk gegevenssysteem de Gegevens waarschijnlijk bewaard worden.
- (iii) Op te geven onder welke omstandigheden ING de Persoonsgegevens heeft verworven; en
- (iv) Bewijs van zijn identiteit voor te leggen; en

- (v) In geval van een aanvraag tot correctie, verwijdering of afscherming, op te geven om welke redenen de Persoonsgegevens onjuist of onvolledig zijn of niet Verwerkt worden in overeenstemming met toepasselijk recht of deze Policy.

Antwoordtermijn

- 11.3** Binnen vier weken nadat ING de aanvraag heeft ontvangen, informeert de Data Protection Executive of enige andere verantwoordelijke functie vermeld in de toepasselijke lokale klachtenprocedures, de Betrokkene schriftelijk hetzij (i) over het standpunt van ING met betrekking tot de aanvraag en alle acties die ING als reactie daarop heeft ondernomen of zal ondernemen, hetzij (ii) over de uiterste datum waarop hij het standpunt van ING zal vernemen, met dien verstande dat die datum niet meer dan acht weken later zal vallen.

Klacht

- 11.4** Een Betrokkene kan een klacht indienen in overeenstemming met Artikel 22 indien:
- (i) Het antwoord op de aanvraag voor de Betrokkene ontoereikend is (bv. de aanvraag wordt geweigerd); of
 - (ii) De Betrokkene nog geen antwoord heeft ontvangen ingevolge Artikel 11.3; of
 - (iii) De termijn die aan de Betrokkene is meegedeeld ingevolge Artikel 11.3 gezien de relevante omstandigheden onredelijk lang is en de Betrokkene bezwaar heeft gemaakt maar geen kortere, redelijkere termijn heeft gekregen waarin hij een antwoord zal ontvangen.

Weigering van aanvragen

- 11.5** ING kan een aanvraag van een Betrokkene weigeren indien:
- (i) De aanvraag niet voldoet aan de voorschriften van Artikelen 11.1 en 11.2.
 - (ii) De aanvraag onvoldoende specifiek is.
 - (iii) De identiteit van de relevante Betrokkene niet met redelijke middelen kan worden vastgesteld; of
 - (iv) De aanvraag gebeurt binnen een onredelijke termijn na een eerdere aanvraag of anderszins misbruik van rechten vormt. Een termijn tussen aanvragen van 6 maanden of minder wordt over het algemeen geacht een onredelijke termijn te zijn.
 - (v) De aanvraag betrekking heeft op het corrigeren, afschermen of verwijderen van Persoonsgegevens waarvan de Verwerking wettelijk verplicht is.

12 Beveiligings- en vertrouwelijkheidsvereisten

Beleidsbepaling

ING treft gepaste maatregelen om de Gegevens te beschermen tegen onrechtmatige toegang en andere ongewenste of onwettige Verwerking, bv. verlies of vernietiging.

Gegevensbeveiliging

- 12.1** ING treft passende, commercieel redelijke technische, fysieke en organisatorische maatregelen om Persoonsgegevens te beschermen tegen misbruik of toevallige, onwettige of ongeoorloofde vernietiging, verlies, wijziging, bekendmaking, verwerving of toegang. Hiertoe heeft ING de ING CORM (Technology) Risk Standards en andere relevante policies met betrekking tot de beveiliging van Persoonsgegevens opgesteld en ingevoerd.

Toegang voor Medewerkers

- 12.2** Medewerkers krijgen uitsluitend toegang tot Persoonsgegevens voor zover dat nodig is voor de toepasselijke gerechtvaardigde doeleinden waarvoor de Gegevens door ING worden Verwerkt en voor de uitoefening van hun functie.
- 12.3** Medewerkers die toegang hebben tot Persoonsgegevens moeten zich houden aan hun vertrouwelijkheidsverplichtingen.

13 Direct marketing

Beleidsbepaling

Dit Artikel betreft de vereisten met betrekking tot de Verwerking van Persoonsgegevens voor direct marketingdoeleinden. ING moet de voorafgaande toestemming van de Betrokkene(n) krijgen indien dat krachtens toepasselijk recht verplicht is. In elk geval krijgen Betrokkenen de mogelijkheid om ervoor te kiezen deze communicaties niet te ontvangen (opt-out).

Direct marketing

- 13.1** Dit Artikel beschrijft de vereisten voor de Verwerking van Persoonsgegevens voor direct marketingdoeleinden (bijvoorbeeld contact opnemen met de Betrokkene per e-mail, fax, telefoon, sms of een ander kanaal, met het oog op commerciële, liefdadigheids- of idealistische doeleinden).

Toestemming voor direct marketing (opt-in)

- 13.2** Indien toepasselijk recht dit vereist, stuurt ING alleen ongevraagde commerciële communicatie (direct marketingcommunicatie) naar Betrokkenen mits de Betrokkene daar vooraf toestemming voor heeft gegeven (opt-in). In elke direct marketingcommunicatie aan de Betrokkene krijgt de Betrokkene de mogelijkheid aan te geven geen verdere direct marketingcommunicatie meer te willen ontvangen.

Verzet tegen direct marketing

- 13.3** Indien een Betrokkene zich verzet tegen de ontvangst van marketingcommunicatie van ING, of zijn toestemming om dergelijke materialen te ontvangen weer intrekt, treft ING maatregelen om geen verder marketingmateriaal meer te sturen, zoals uitdrukkelijk gevraagd door de Betrokkene. ING doet dit binnen de termijn die is voorzien in toepasselijk recht.

Derden en direct marketing

- 13.4** Er worden geen Gegevens verstrekt aan, gebruikt of anderszins Verwerkt namens Derden voor direct marketingdoeleinden van of voor Derden zonder de voorafgaande toestemming van de Betrokkene.

Persoonsgegevens van kinderen

- 13.5** ING gebruikt geen Persoonsgegevens van Betrokkenen jonger dan veertien (14) jaar voor direct marketing.

Registratie direct marketing

- 13.6** ING bewaart lokale registers van Betrokkenen die hebben gebruikgemaakt van hun recht op opt-in of opt-out en controleert regelmatig de relevante lokale openbare opt-out registers.

14 Automatische besluitvorming

Automatische besluiten

- 14.1** Er kan gebruikgemaakt worden van geautomatiseerde hulpmiddelen om beslissingen te nemen over Betrokkenen, maar beslissingen mogen niet uitsluitend gebaseerd zijn op de resultaten van het geautomatiseerde hulpmiddel. Die beperking is niet van toepassing als:
- (i) Het gebruik van geautomatiseerde hulpmiddelen wettelijk is verplicht of toegelaten.
 - (ii) ING de beslissing neemt om (a) een overeenkomst aan te gaan of uit te voeren of (b) de overeenkomst te beheren, op voorwaarde dat de onderliggende aanvraag die leidde tot een beslissing van ING werd ingediend door de Betrokkene (bv. wanneer geautomatiseerde hulpmiddelen worden gebruikt om antwoorden op promotionele spellen te filteren of bij de verstrekking van hypotheek en andere financiële producten); of
 - (iii) Passende maatregelen worden getroffen om de rechtmatige belangen van de Betrokkene te vrijwaren, bv. door de Betrokkene de mogelijkheid te bieden zijn standpunt te verwoorden.

15 Doorgifte van Persoonsgegevens aan Derden

Beleidsbepaling

ING ziet erop toe dat de vereisten voor de doorgifte van Persoonsgegevens aan Derden buiten ING, zoals vermeld in dit Artikel (15) worden nageleefd. Doorgifte van Persoonsgegevens kan ook situaties omvatten waarbij ING Persoonsgegevens deelt met Derden (bv. in het kader van corporate due diligence) of waarbij ING een Derde toegang op afstand verleent tot Persoonsgegevens. ING ziet er ook op toe dat aan de aanvullende voorschriften in dit Artikel is voldaan indien de Persoonsgegevens worden doorgegeven naar een Land zonder Passend Beschermingsniveau. In dit Artikel verwijst ING naar de betreffende Groepsentiteit.

Doorgifte van persoonsgegevens

- 15.1** ING geeft Persoonsgegevens door aan een Derde Verantwoordelijke voor zover dat nodig is voor het toepasselijke gerechtvaardigde doeleinde waarvoor de Persoonsgegevens worden Verwerkt.

Overeenkomsten met Derde Verantwoordelijken

- 15.2** Derde Verantwoordelijken (met uitzondering van overheidsinstellingen en andere overheidsorganen) mogen alleen Persoonsgegevens Verwerken indien zij een schriftelijke overeenkomst of een vergelijkbare overeenkomst (bv. elektronisch) met de betreffende Groepsentiteit hebben. In die overeenkomst streeft ING ernaar de belangen van de Betrokkenen inzake gegevensbescherming contractueel te beschermen. Alle dergelijke overeenkomsten worden opgesteld in overleg met of in overeenstemming met de richtlijnen van de bevoegde Data Protection Executive. Professionele Contactgegevens van de Betrokkene mogen worden doorgegeven aan een Derde Verantwoordelijke indien redelijkerwijs verwacht kan worden dat de Derde Verantwoordelijke die Professionele Contactgegevens zal gebruiken om contact op te nemen met de Betrokkene voor gerechtvaardigde bedrijfsdoeleinden met betrekking tot de professionele verantwoordelijkheden van de Betrokkene bij de betreffende Klant, Leverancier of Zakenpartner.

Overeenkomsten met Derde Bewerkers

- 15.3** Derde Bewerkers mogen alleen Persoonsgegevens Verwerken indien zij een schriftelijke overeenkomst of een vergelijkbare overeenkomst (bv. elektronisch) met ING hebben. Overeenkomsten met een Derde Bewerker die Persoonsgegevens zal verwerken moeten de volgende bepalingen bevatten:

- (i) De Bewerker Verwerkt de Persoonsgegevens uitsluitend in overeenstemming met de instructies van ING en voor de doeleinden waarvoor ING toestemming heeft verleend; en
- (ii) De Bewerker houdt de Persoonsgegevens vertrouwelijk; en
- (iii) De Bewerker treft gepaste technische, fysieke en organisatorische beveiligingsmaatregelen om de Persoonsgegevens te beschermen; en
- (iv) De Derde Bewerker verleent onderaannemers geen toestemming om Persoonsgegevens te Verwerken in verband met zijn verplichtingen jegens ING zonder voorafgaande schriftelijke toestemming van ING (of: de Bewerker waarborgt dat de onderaannemers zullen voldoen aan de voorwaarden van de overeenkomst die hij heeft met ING); en
- (v) ING heeft het recht om de beveiligingsmaatregelen van de Derde Bewerker te beoordelen, en de Derde Bewerker onderwerpt zijn betrokken infrastructuur voor gegevensverwerking aan audits en inspecties door ING of enige bevoegde overheidsinstantie; en
- (vi) De Derde Bewerker informeert ING onverwijld over elk feitelijke of vermoedelijke datalek waar Persoonsgegevens bij betrokken zijn; en
- (vii) De Derde Bewerker treft zo snel mogelijk gepaste herstelmaatregelen en verstrekt ING onverwijld alle relevante informatie en ondersteuning waar ING om verzoekt met betrekking tot het datalek.

Doorgifte van Gegevens naar een Land zonder Passend Beschermingsniveau

15.4 Dit Artikel zet aanvullende regels uiteen ten aanzien van de grensoverschrijdende doorgifte van Persoonsgegevens naar een Derde gevestigd in een Land zonder Passend Beschermingsniveau, die moeten worden nageleefd bovenop de overige vereisten uit deze Policy. Persoonsgegevens mogen alleen worden doorgegeven aan een Derde in een Land zonder Passend Beschermingsniveau indien:

- (i) De doorgifte noodzakelijk is voor de uitvoering van een overeenkomst met de Betrokkene, voor het beheer van een overeenkomst met de Betrokkene of om op verzoek van de Betrokkene benodigde stappen te ondernemen alvorens een overeenkomst aan te gaan, bv. voor de verwerking van orders; of
- (ii) ING en de betreffende Derde een overeenkomst zijn aangegaan die voorziet in waarborgen met een vergelijkbaar beschermingsniveau als deze Policy, of indien die overeenkomst in overeenstemming is met een eventuele modelovereenkomst krachtens toepasselijk lokaal recht; of
- (iii) De doorgifte noodzakelijk is voor het tot stand komen of uitvoeren van een overeenkomst in het belang van de Betrokkene tussen ING en een Derde; of
- (iv) De Derde is gecertificeerd onder het United States Safe Harbor Program of een vergelijkbaar programma waarvan wordt erkend dat het een 'adequaat' niveau van gegevensbescherming biedt; of
- (v) De Derde binding corporate rules of een vergelijkbaar controlemechanisme op doorgifte heeft ingevoerd, die afdoende waarborgen bieden onder toepasselijk recht. Een kopie van de binding corporate rules of bewijs van het controlemechanisme op doorgifte moet aan ING worden verstrekt voordat de doorgifte plaatsvindt; of
- (vi) De doorgifte nodig is om een vitaal belang van de Betrokkene te beschermen; of
- (vii) De doorgifte nodig is in verband met rechtszaken, juridisch advies of rechten; of
- (viii) de doorgifte nodig is om te voldoen aan een dwingende noodzaak om een zwaarwegend algemeen belang te beschermen; of
- (ix) De doorgifte verplicht is krachtens wet- of regelgeving die op het betreffende Groepsentiteit van toepassing is; of
- (x) De door te geven Gegevens zijn opgenomen in een openbaar register.

Onderdelen (viii) en (ix) hierboven vereisen:

- (i) De voorafgaande goedkeuring van de bevoegde Data Protection Executive; en
- (ii) Dat geschikte maatregelen worden getroffen om de rechtmatige belangen van de Betrokkene te vrijwaren (die onder andere kunnen bestaan uit overleg met het Nederlandse College Bescherming Persoonsgegevens).

Toestemming voor doorgifte

15.5 Indien geen van de in Artikel 15.4 vermelde gronden van toepassing zijn of indien toepasselijk recht dat vereist, vraagt ING (ook) toestemming van de Betrokkene voor de doorgifte naar een Derde gevestigd in een Land zonder Passend Beschermingsniveau. Alvorens om toestemming wordt gevraagd, krijgt de Betrokkene de volgende informatie:

- (i) Het doeleinde van de doorgifte; en
- (ii) De identiteit van de Groepsentiteit die de doorgifte uitvoert; en
- (iii) De identiteit of categorieën van Derden aan wie de Gegevens worden doorgegeven; en
- (iv) De categorieën van Gegevens die worden doorgegeven; en
- (v) Het land naar waar de Gegevens worden doorgegeven; en
- (vi) Het feit dat de Gegevens worden doorgegeven naar een Land zonder Passend Beschermingsniveau.

Artikel 6.4 is van toepassing op de verlening, weigering of intrekking van de toestemming.

Doorgifte tussen Landen zonder Passend Beschermingsniveau

15.6 Dit Artikel zet aanvullende regels uiteen voor de grensoverschrijdende doorgifte van Persoonsgegevens die werden verzameld in het kader van de activiteiten van een Groepsentiteit gevestigd in een Land zonder Passend Beschermingsniveau naar een Derde die eveneens is gevestigd in een Land zonder Passend Beschermingsniveau. Bovenop de gronden vermeld in Artikel 15.4 is deze doorgifte toegestaan indien:

- (i) Nodig om te voldoen aan een wettelijke verplichting die op de betreffende Groepsentiteit van toepassing is.
- (ii) Nodig in het kader van het openbare belang; of
- (iii) Nodig voor het gerechtvaardigde doeleinde waarvoor de Gegevens worden Verwerkt.

16 Prevalerende Belangen

Beleidsbepaling

Er kunnen omstandigheden zijn waarin ING kan beslissen sommige van de verplichtingen van ING of rechten van Betrokkenen krachtens deze Policy niet te laten prevaleren, maar alleen onder de voorwaarden uiteengezet in dit Artikel en voor zover dat mogelijk is krachtens toepasselijk lokaal recht.

Prevalerende Belangen

16.1 Enkele van de verplichtingen van ING of rechten van Betrokkenen krachtens deze Policy hoeven niet te prevaleren indien, gelet op de specifieke omstandigheden van het geval, een dwingende noodzaak bestaat die het belang van de Betrokkene overtreft (**Prevalerend Belang**). Er is sprake van een Prevalerend Belang indien de noodzaak bestaat om:

- (i) De rechtmatige bedrijfsbelangen van ING te beschermen, met inbegrip van maar niet beperkt tot:
 - (a) de gezondheid, veiligheid of bescherming van Werknemers of Betrokkenen; of
 - (b) de intellectuele eigendomsrechten, bedrijfsgeheimen of reputatie van ING; of
 - (c) de continuïteit van de bedrijfsvoering van ING; of

- (d) het behoud van de vertrouwelijkheid in een voorgestelde verkoop, fusie of overname van een bedrijf; of
 - (e) de betrokkenheid van vertrouwde adviseurs of consultants voor bedrijfs-, juridische, fiscale of verzekeringsdoeleinden.
- (ii) Vermoedelijke of feitelijke wetsovertredingen te voorkomen of onderzoeken (met inbegrip van samenwerking met wetshandhavende instanties); of
 - (iii) De rechten of vrijheden van ING, Werknemers van ING of andere personen anderszins te beschermen of verdedigen.

Uitzonderingen in het geval van Prevalerende Belangen

16.2 Indien een Prevalerend Belang bestaat, kunnen een of meer van volgende verplichtingen van ING of rechten van de Betrokkene terzijde geschoven worden:

- (i) Artikel 7.1 (Verwerking van Persoonsgegevens voor nauw verbonden doeleinden); en
- (ii) Artikel 10.1 en 10.2 (informatie verstrekt aan Betrokkenen, Persoonsgegevens niet verkregen van de Betrokkenen); en
- (iii) Artikel 11.1 (rechten van Betrokkenen); en
- (iv) Artikelen 12.2 en 12.3 (toegangsbeperkingen en vertrouwelijkheidsplicht van Medewerkers); en
- (v) Artikelen 15.2, 15.3 en 15.4 (ii) (overeenkomsten met Derden).

Bijzondere Gegevens

16.3 De vereisten van Artikelen 8.1 en 8.2 (Bijzondere Gegevens) mogen alleen terzijde geschoven worden voor de Prevalerende Belangen vermeld in Artikel 16.1 (i) (a), (c) en (e), (ii) en (iii).

Voorafgaande goedkeuring van de Data Protection Executive

16.4 Verplichtingen van ING of rechten van Betrokkenen kunnen slechts terzijde geschoven worden op grond van een Prevalerend Belang na voorafgaande goedkeuring van de bevoegde Data Protection Executive.

Informatieverstrekking aan de Betrokkene

16.5 Op verzoek van een Betrokkene informeert ING de Betrokkene over het Prevalerende Belang waarvoor verplichtingen van ING of rechten van de Betrokkene terzijde werden geschoven, tenzij het specifieke Prevalerende Belang de vereisten van Artikelen 11.1 of 12.1 terzijde schuift, in welk geval het verzoek wordt geweigerd.

DEEL III TOEZICHT, NALEVING EN JURIDISCHE KWESTIES

17 Toezicht en naleving

- 17.1 Het management van het bedrijf is verantwoordelijk voor de naleving van de Policy in elk Bedrijfsonderdeel.

Bank Data Protection Executive (Bank DPE)

- 17.2 De Bank Data Protection Executive houdt toezicht op de implementatie en naleving van de Policy in elk Bedrijfsonderdeel, hetgeen de verantwoordelijkheden en activiteiten omvat die nader omschreven staan in Artikel 18 van deze Policy. De rol van Bank Data Protection Executive wordt vervuld door de vicevoorzitter van de Bank.

Bank Data Protection Officer (Bank DPO)

- 17.3 De Bank Data Protection Officer is verantwoordelijk voor het toezicht op de algemene naleving van de Policy en verstrekt advies bij de invoering en interpretatie ervan in heel ING, wat de verantwoordelijkheden en activiteiten omvat die nader omschreven staan in Artikel 18. De rol van Bank Data Protection Officer wordt vervuld door een functionaris van de Bank uit Tier 2.

BU Data Protection Executive (BU DPE)

- 17.4 Het management van het bedrijf stelt voldoende BU Data Protection Executives aan om de naleving van deze Policy in hun respectieve Bedrijfsonderdelen in goede banen te leiden. De Data Protection Executive neemt zijn functie waar zoals nader omschreven in Artikel 18.

BU Data Protection Officer (BU DPO)

- 17.5 Het management van het bedrijf stelt voldoende BU Data Protection Officers aan om de naleving van deze Policy in hun respectieve Bedrijfsonderdelen in goede banen te leiden. De Data Protection Officer neemt zijn functie waar zoals nader omschreven in Artikel 18. De rol van BU Data Protection wordt vervuld door de gepaste tweedelijnsfunctionaris.

Data Protection Officer met een wettelijke positie

- 17.6 Wanneer een Data Protection Officer zijn positie bekleedt krachtens de wet, voert hij zijn functieverantwoordelijkheden uit voor zover die niet strijdig zijn met zijn wettelijke positie.

18. Verantwoordelijkheden

Wie	Verantwoordelijkheden
Data Protection Executive (DPE)	De BU Data Protection Executive is vanuit zakelijk oogpunt verantwoordelijk voor de naleving en invoering van de Policy in een Bedrijfsonderdeel. De Data Protection Executive beslist over, stelt de middelen beschikbaar voor en faciliteert de afhandeling van alle kwesties met betrekking tot gegevensbescherming in het betreffende Bedrijfsonderdeel. De Data Protection Executive: • Ziet erop toe dat zijn Bedrijfsonderdeel Persoonsgegevens verwerkt in overeenstemming met deze Policy.

Wie	Verantwoordelijkheden
	• Voert in zijn Bedrijfsonderdeel de veranderingen in die nodig zijn om tot naleving te komen. • Werkt samen met de DPO's binnen zijn Bedrijfsonderdeel en faciliteert hun werk om een kader neer te zetten en in stand te houden voor het ontwikkelen, invoeren en actueel houden van lokale policies en procedures met betrekking tot gegevensbescherming (inclusief opleiding en voorlichting). • Ziet erop toe dat de Medewerkers in zijn Bedrijfsonderdeel de verplichte opleiding volgen. • Vult vragenlijsten in het kader van audits en Data Protection Impact Assessments naar behoren in en valideert deze. • Brengt de DPO's in zijn Bedrijfsonderdeel op de hoogte van en wint hun advies in over alle risico's en incidenten met betrekking tot gegevensbescherming, nalevingskwesties of vragen in het Bedrijfsonderdeel waarin hij verantwoordelijk is voor de naleving van het privacybeleid. • Escaleert naar de Bank DPE indien nodig. • Brengt verslag uit, naar behoefte maar ten minste elk kwartaal, aan de Bank DPE over risico's in verband met gegevensbescherming en nalevingskwesties.
Bank Data Protection Executive (Bank DPE)	De Bank Data Protection Executive is verantwoordelijk voor het toezicht op de algemene naleving en invoering van de Policy binnen heel ING. De Bank Data Protection Executive: • Overlegt met de Bank DPO over alle risico's, incidenten, nalevingskwesties of vragen inzake gegevensbescherming die naar de Bank DPE zijn geëscaleerd. • Brengt ten minste eenmaal per jaar en vaker indien nodig verslag uit aan de Bank DPO en de Bank NFRC over risico's en nalevingskwesties inzake gegevensbescherming.
Data Protection Officer (DPO)	De BU Data Protection Officer is verantwoordelijk voor het toezicht op de naleving van de Policy in de relevante Bedrijfsonderdelen en verstrekt advies aan de relevante DPE. De relevante Data Protection Officer: • Beschikt over voldoende expertise met betrekking tot het recht en de praktijk inzake gegevensbescherming. • Adviseert de relevante DPE op diens verzoek over alle risico's en incidenten met betrekking tot gegevensbescherming, nalevingskwesties of vragen in het Bedrijfsonderdeel. • Werkt samen met de DPE om een kader neer te zetten en in stand te houden voor het ontwikkelen, invoeren en actueel houden van lokale policies en procedures met betrekking tot gegevensbescherming om toe te kunnen zien op en ondersteuning te kunnen bieden aan de invoering en inbedding

Wie	Verantwoordelijkheden
	van de Policy in zijn Bedrijfsonderdeel. • Adviseert over en ondersteunt door middel van communicatie aan en opleiding van de Medewerkers de correcte invoering van de Policy; • Is in staat om onafhankelijk van de business en het (senior) management kunnen werken zonder belangenverstremgeling met zijn andere professionele taken.. • Heeft controle- en toezichtsbevoegdheden (het recht om intern onderzoek te doen en recht op toegang tot informatie). • Brengt ten minste eenmaal per kwartaal en vaker indien nodig verslag uit aan de Bank DPO over risico's en nalevingskwesaties inzake gegevensbescherming.
Bank Data Protection Officer (Bank DPO)	De Bank DPO is verantwoordelijk voor het toezicht op de algemene naleving van de Policy in heel ING. De Bank DPO: • Coördineert samen met de relevante DPO's officiële onderzoeken naar de Gegevensverwerking door een overheidsinstantie. • Begeleidt waar mogelijk de DPO's bij de interpretatie van de Policy ten opzichte van lokale gegevensbeschermingskwesaties en ziet erop toe dat de Policy wordt bijgewerkt wanneer nodig. • Brengt ten minste eenmaal per jaar en vaker indien nodig verslag uit aan de Bank DPE en de Bank NFRC over risico's en nalevingskwesaties inzake gegevensbescherming.
Medewerkers die met Persoonsgegevens in aanraking komen	Medewerkers die in het kader van hun functie toegang hebben tot Persoonsgegevens, moeten deze Policy naleven. Medewerkers: • Mogen Persoonsgegevens alleen gebruiken voor zover nodig voor het toepasselijke gerechtvaardigde doeleinde waarvoor ING Persoonsgegevens verwerkt en om hun werk uit te voeren. • Moeten elk (mogelijk) incident of kwestie met betrekking tot Persoonsgegevens melden aan hun manager of aan de relevante DPE of via de Klokkenluidersregeling.

19 Policies en procedures

- 19.1** ING ontwikkelt en implementeert policies, minimumnormen en procedures om deze Policy na te leven. Deze Policy hangt samen met enkele andere policies in het ING Bank Policy House. In de regel vormt deze Policy het uitgangspunt voor andere, meer gedetailleerde policies. Onderstaande grafiek toont de belangrijkste samenhangen.



Documentatie van de informatiesystemen

- 19.2** ING houdt documentatie in stand (bv. Data Protection (Privacy) Impact Assessments, Control Framework/Register, Operational Security Guidelines) met betrekking tot de structuur, werking, beveiliging en controle van zijn informatietechnologiesystemen die Persoonsgegevens Verwerken.

20 Opleiding

Opleiding van Medewerkers

- 20.1** ING zorgt ervoor dat Medewerkers die toegang hebben tot Persoonsgegevens bekend zijn met deze Policy en de aanverwante vertrouwelijkheidsplichten. Specifieke functies, en in elk geval de Data Protection Executives en Data Protection Officers, krijgen doorlopend diepgaande trainingen. Meer gedetailleerde trainingen gefocust op specifieke lokale voorschriften die van belang zijn voor de naleving van deze Policy worden lokaal of regionaal geregeld. Al deze trainingen kunnen aangeboden worden via het wereldwijde ING Learning Center en op regionale of lokale basis.

21 Monitoring van de naleving

Audits

- 21.1** Corporate Audit Services zal bedrijfsprocessen en -procedures waarbij sprake is van de Verwerking van Persoonsgegevens toetsen op de naleving van deze Policy. De audits zullen worden uitgevoerd in de loop van de normale activiteiten van Corporate Audit Services of op verzoek van de Bank Data Protection Executive. De Bank Data Protection Executive kan ook verzoeken dat een audit zoals uiteengezet in dit Artikel 21.1 wordt uitgevoerd door een externe auditor. Bij het uitvoeren van een audit moeten de geldende beroepsnormen ten aanzien van onafhankelijkheid, integriteit en vertrouwelijkheid in acht genomen worden. De Bank Data Protection Executive wordt op de hoogte gebracht van de resultaten van de audits. De Bank Data Protection Executive verstrekt een kopie van de auditresultaten aan de betreffende Data

Protection Executive(s) en aan de Bank Data Protection Officer. Op verzoek wordt een kopie van de auditresultaten verstrekt aan het Nederlandse College Bescherming Persoonsgegevens.

Mitigerende maatregelen

- 21.2** ING zal, waar dat nodig blijkt, ervoor zorgen dat passende maatregelen worden genomen om schendingen van deze Policy die worden geconstateerd tijdens regulier onderzoek van of een audit naar de naleving onder dit Artikel 21 aan te pakken.

22 Klachtenprocedure

Klacht naar BU Data Protection Executive

- 22.1** Onverminderd de rechten en rechtsmiddelen waarover de Betrokkenen in hun lokale rechtsgebied beschikken zoals uiteengezet in Artikel 23.1, kunnen Betrokkenen een klacht indienen met betrekking tot de naleving van deze Policy of een schending van hun rechten krachtens deze Policy of krachtens toepasselijk lokaal recht in overeenstemming met de lokale klachtenprocedure uiteengezet in het toepasselijke privacybeleid of overeenkomst of zoals anderszins meegedeeld aan de Betrokkene. De lokale klachtenprocedure zorgt ervoor dat een onderzoek naar de klacht wordt begonnen en zorgt ervoor dat de relevante BU Data Protection Executive daarbij wordt betrokken.

- 22.2** De BU Data Protection Executive:

- (a) Ondersteunt het onderzoek; en
- (b) Wint altijd advies in van de relevante BU Data Protection Officer over de gepaste maatregelen met het oog op naleving; en
- (c) Adviseert de business in overeenstemming met het advies van de relevante BU Data Protection Officer over passende maatregelen met het oog op naleving en ziet tot aan de voltooiing toe op stappen bedoeld om tot naleving te komen; en
- (d) Licht de Bank Data Protection Officer indien nodig in.

De verantwoordelijke Data Protection Officer kan met elke overheidsinstantie die voor een bepaalde aangelegenheid bevoegd is, overleggen over de te treffen maatregelen.

Antwoord aan Betrokkene

- 22.3** Binnen vier weken nadat ING een klacht heeft ontvangen, informeert ING de Betrokkene schriftelijk of (i) over het standpunt van ING met betrekking tot de klacht en alle acties die ING als reactie daarop heeft ondernomen of zal ondernemen, of (ii) wanneer hij in kennis zal worden gesteld van het standpunt van ING, met dien verstande dat die datum niet meer dan vier weken later zal vallen. De verantwoordelijke BU Data Protection Executive stuurt een kopie van de klacht en het schriftelijke antwoord van ING naar de relevante BU Data Protection Officer en de Bank Data Protection Officer, indien die werd ingelicht ingevolge Artikel 22.2 (d).

Klacht aan Bank Data Protection Officer

- 22.4** Een Betrokkene kan een klacht escaleren naar de Bank Data Protection Officer indien:
- (i) De afhandeling van de klacht door het Bedrijfsonderdeel in kwestie voor de Betrokkene onbevredigend is (bijvoorbeeld de klacht wordt afgewezen).
 - (ii) De Betrokkene nog geen antwoord heeft ontvangen zoals voorgeschreven door Artikel 22.3.
 - (iii) De termijn die aan de Betrokkene is meegedeeld ingevolge Artikel 22.3 gezien de relevante omstandigheden onredelijk lang is en de Betrokkene bezwaar heeft gemaakt

- maar geen kortere, redelijkere termijn heeft gekregen waarin hij een antwoord zal ontvangen; of
- (iv) Een van de gebeurtenissen vermeld in Artikel 11.4 zich voordoet.

De procedure beschreven in Artikelen 22.1 tot en met 22.3 is van toepassing op klachten die worden geëscaleerd naar de Bank Data Protection Officer in overeenstemming met Artikel 22.4. De Bank Data Protection Officer licht de Bank Data Protection Executive in over de geëscaleerde klacht, indien relevant.

23 Juridische kwesties

Lokaal recht en bevoegde rechtbanken

- 23.1** Elke Verwerking van Persoonsgegevens door ING wordt beheerst door toepasselijk lokaal recht. Betrokkenen behouden hun rechten en rechtsmiddelen zoals die hen ter beschikking staan in hun lokale jurisdicties, bv. het recht om een klacht in te dienen bij de lokale autoriteit voor gegevens-bescherming of om een zaak aanhangig te maken bij de lokale rechtbank. Lokale overheidsinstanties die bevoegd zijn in de relevante kwestie behouden hun bevoegdheid.

Aanvullende bescherming geboden door deze Policy

- 23.2** Deze Policy wordt beheerst en geïnterpreteerd volgens het Nederlandse recht. Deze Policy is alleen van toepassing wanneer het aanvullende bescherming voor Persoonsgegevens biedt. Wanneer toepasselijk lokaal recht meer bescherming biedt dan deze Policy, is lokaal recht van toepassing. Wanneer deze Policy meer bescherming biedt dan toepasselijk lokaal recht of voorziet in aanvullende waarborgen, rechten of rechtsmiddelen voor Betrokkenen, is deze Policy van toepassing.

Primaire instantie voor toezicht op de regels

- 23.3** Op de naleving van deze Policy wordt uitsluitend toegezien door het Nederlandse College Bescherming Persoonsgegevens, dat ook te allen tijde als enige bevoegd is om ING Bank N.V. te adviseren over de toepassing van deze Policy. Het Nederlandse College Bescherming Persoonsgegevens heeft de onderzoeksbevoegdheden toegekend op grond van de Nederlandse Wet Bescherming Persoonsgegevens. Voor zover het Nederlandse College Bescherming Persoonsgegevens discretionaire bevoegdheden heeft met betrekking tot de handhaving van de Nederlandse Wet Bescherming Persoonsgegevens, heeft het dezelfde discretionaire bevoegdheden voor de handhaving van deze Policy.

Exclusieve bevoegdheid krachtens de Policy

- 23.4** Alle klachten of vorderingen van Betrokkenen met betrekking tot aanvullende rechten die de Betrokkene mogelijk krachtens deze Policy heeft, mogen uitsluitend worden gericht aan ING Bank N.V. en zullen worden voorgelegd aan het Nederlandse College bescherming persoonsgegevens of de bevoegde rechtbank in Amsterdam, Nederland. Het Nederlandse College bescherming persoonsgegevens en de rechtbanken van Amsterdam, Nederland, zijn als enige bevoegd over alle aanvullende rechten die deze Policy verleent. Klachten en vorderingen zijn alleen ontvankelijk indien de Betrokkene eerst de klachtenprocedure heeft gevolgd zoals uiteengezet in Artikel 22 van deze Policy.

Policy uitsluitend afdwingbaar jegens ING Bank N.V.

- 23.5** Alle aanvullende waarborgen, rechten of rechtsmiddelen die krachtens deze Policy aan Betrokkenen worden verleend, zijn alleen verleend door en jegens ING Bank N.V. afdwingbaar in Nederland.

Beschikbare rechtsmiddelen, beperking van schadevergoedingen en bewijslast

- 23.6** In aanvulling op alle rechtsmiddelen waarover Betrokkenen beschikken krachtens hun toepasselijke lokale recht, kunnen Betrokkenen op grond van deze Policy alleen aanspraak maken op rechtsmiddelen die beschikbaar zijn voor betrokkenen krachtens de Nederlandse Wet Bescherming Persoonsgegevens, het Nederlandse Burgerlijk Wetboek en het Nederlandse Wetboek van Burgerlijke Rechtsvordering. ING Bank N.V. zal echter slechts aansprakelijk zijn voor directe schade geleden door een Betrokkene als gevolg van een schending van deze Policy. Op voorwaarde dat een Natuurlijk Persoon kan aantonen dat hij schade geleden heeft en feiten aanvoert waaruit blijkt dat aannemelijk is dat de schade is ontstaan vanwege een schending van deze Policy, zal ING Bank N.V. moeten bewijzen dat de schade die de Betrokkene heeft geleden als gevolg van een schending van de Policy, niet toe te schrijven is aan de betreffende Groepsentiteit.

Onderlinge bijstand en herstel

- 23.7** Alle Groepsentiteiten zullen voor zover redelijkerwijs mogelijk samenwerken en elkaar bijstaan bij de behandeling van:
- (i) een aanvraag, klacht of vordering van een Betrokkene; of
 - (ii) een wettig onderzoek door een bevoegde overheidsinstantie.

De Groepsentiteit die een aanvraag, klacht of vordering ontvangt van een Betrokkene, is verantwoordelijk voor alle communicatie met de Betrokkene met betrekking tot zijn aanvraag, klacht of vordering, tenzij dit door de gegeven omstandigheden niet kan.

De Groepsentiteit die verantwoordelijk is voor de Verwerking waarop de aanvraag, klacht of vordering betrekking heeft, draagt alle gemaakte kosten en betaalt ING Bank N.V. terug op eerste verzoek van ING Bank N.V.

24 Sancties voor niet-naleving

Niet-naleving

- 24.1** Niet-naleving van deze Policy door Medewerkers kan beschouwd worden als een ernstige schending van het vertrouwen dat ING in zijn Werknemers en andere Medewerkers moet kunnen hebben. Niet-naleving door een Werknemer kan dan ook leiden tot een sanctie, zoals een schorsing of andere disciplinaire maatregelen of maatregelen krachtens het arbeidsrecht, tot en met ontslag op staande voet. Niet-naleving door Medewerkers die geen Werknemers zijn kan leiden tot de beëindiging van de betreffende overeenkomst met deze Medewerker. Medewerkers zullen niet bestraft worden voor het signaleren van problemen met betrekking tot de naleving van deze Policy. De Klokkenluidersregeling van ING is van toepassing.

25 Tegenstrijdigheden tussen deze Policy en toepasselijk lokaal recht

Wetsconflict bij de doorgifte van Gegevens

- 25.1** In het geval een wettelijke verplichting om Persoonsgegevens door te geven in strijd is met het recht van de Lidstaten van de EER of het recht van Zwitserland, is voor de doorgifte de voorafgaande goedkeuring van de Bank Data Protection Executive vereist. De Bank Data Protection Executive zal advies inwinnen bij de Bank Data Protection Officer. De Bank Data Protection Officer kan advies inwinnen bij het Nederlandse College bescherming persoonsgegevens of een andere bevoegde overheidsinstantie.

Tegenstrijdigheid tussen deze Policy en de wet

- 25.2 In alle andere gevallen waarin er tegenstrijdigheid is tussen toepasselijk lokaal recht en de Policy, moet de betreffende Data Protection Executive of de manager van de Werknemers of Medewerkers die het probleem signaleerden, overleggen met de Bank Data Protection Executive om te bepalen hoe deze Policy kan worden nageleefd en de tegenstrijdigheid op redelijkerwijs uitvoerbare wijze kan worden opgelost gelet op de wettelijke verplichtingen die op het betreffende Groepsentiteit van toepassing zijn.

Nieuwe tegenstrijdige wettelijke verplichtingen

- 25.3 De betreffende Data Protection Executive moet de Bank Data Protection Executive onverwijld op de hoogte brengen van alle nieuwe wettelijke verplichtingen die het naleven van deze Policy door ING kunnen belemmeren.

26 Wijzigingen aan de Policy

- 26.1 Voor alle wijzigingen aan deze Policy is de voorafgaande goedkeuring van de General Legal Counsel vereist. De General Legal Counsel zal overleggen met de Bank Data Protection Officer alvorens dergelijke wijzigingen goed te keuren. ING Bank N.V. zal het Nederlandse College bescherming persoonsgegevens jaarlijks op de hoogte brengen van wezenlijke wijzigingen aan de Policy, of eerder indien de aard van de wezenlijke wijziging dit vereist.
- 26.2 Deze Policy kan worden gewijzigd zonder toestemming van de Betrokkenen, ook als een wijziging betrekking heeft op een aan Betrokkenen toegekend recht.
- 26.3 Elke wijziging treedt pas in werking nadat ze is goedgekeurd door de General Legal Counsel en is gepubliceerd op het intranet van ING en de website(s) van ING.
- 26.4 Elke aanvraag, klacht of vordering van een Betrokkene met betrekking tot deze Policy zal worden afgewogen tegen de versie van de Policy die van kracht is op het moment waarop de aanvraag, klacht of vordering wordt ingediend.

27 Overgangsperiodes

Algemene overgangsperiode

- 27.1 Tenzij hieronder anders vermeld, geldt een overgangsperiode van twee jaar om te gaan voldoen aan deze Policy. Dienovereenkomstig zullen, tenzij anders vermeld, alle Persoonsgegevens binnen twee jaar na de Ingangsdatum verwerkt worden in overeenstemming met de Policy. Tijdens elke overgangsperiode streeft ING ernaar te voldoen aan de Policy.

Overgangsperiode voor nieuwe Groepsentiteiten

- 27.2 Elke entiteit die een Groepsentiteit wordt na de Ingangsdatum, zal binnen twee jaar nadat zij een Groepsentiteit is geworden voldoen aan deze Policy.

Overgangsperiode voor IT-systemen

- 27.3 In het geval de implementatie van deze Policy updates of wijzigingen van informatietechnologie-systemen vereist (met inbegrip van de vervanging van systemen), bedraagt de overgangsperiode vier jaar vanaf de Ingangsdatum of vanaf de datum waarop een entiteit een Groepsentiteit wordt, of elke langere periode die redelijkerwijs nodig is om de update, aanpassing of vervanging te voltooien.

Overgangsperiode voor bestaande overeenkomsten

- 27.4** In het geval bestaande overeenkomsten met Derden gevolgen ondervinden van deze Policy, zullen de bepalingen van de overeenkomsten prevaleren tot de overeenkomsten worden verlengd in het kader van de normale bedrijfsvoering.

Overgangsperiode voor lokale systemen voor lokale gegevens

- 27.5** De Verwerking van Persoonsgegevens die werden verzameld in het kader van de activiteiten van een Groepsentiteit gevestigd in een Land zonder Passend Beschermingsniveau, zullen binnen drie jaar na de Ingangsdatum in overeenstemming worden gebracht met deze Policy.

Contactgegevens

Data Protection Officer ING Bank

p/a ING Bank N.V.

E-mailadres: DPO.office@ing.nl

Telefoonnummer: +31 (0) 20 430 8015

BIJLAGE 1 DEFINITIES EN INTERPRETATIE

Definities

Archief betekent een verzameling Persoonsgegevens die niet langer nodig zijn om de doeleinden te verwezenlijken waarvoor de Gegevens oorspronkelijk werden verzameld of die niet langer gebruikt worden voor algemene bedrijfsactiviteiten, maar alleen gebruikt worden voor historische, wetenschappelijke of statistische doeleinden, het afhandelen van geschillen, rechtszaken, onderzoeken of algemene archiefdoeleinden. Een archief omvat alle datasets die niet langer toegankelijk zijn voor andere Werknemers dan de systeembeheerder.

Artikel betekent een artikel in deze Policy.

Bank Data Protection Executive (Bank DPE) betekent de functionaris zoals omschreven in Artikel 17.2.

Bank Data Protection Officer (Bank DPO) betekent de functionaris zoals omschreven in Artikel 17.3.

Bank NFRC betekent het Non-Financial Risk Committee van de Bank.

Bedrijfsdoeleinde betekent een doeleinde voor de Verwerking van Persoonsgegevens zoals omschreven in Artikel 6 of 7 of voor de Verwerking van Bijzondere Gegevens zoals omschreven in Artikel 7 of 8.

Bedrijfsonderdeel betekent een Groepsentiteit die een lokale, regionale of algemene bank is. Voor de toepassing van deze Policy worden corporate en andere stafafdelingen beschouwd als Bedrijfsonderdelen en hebben zij dezelfde verantwoordelijkheden.

Betrokkene betekent iedere Klant, Leverancier of Zakenpartner die een natuurlijke persoon is of iedere werknemer of iedere persoon die werkt voor een Klant, Leverancier of Zakenpartner, met inbegrip van personen van wie ING de persoonsgegevens Verwerkt op grond van een wettelijke of contractuele verplichting jegens een derde (bv. begunstigen, gemandateerden of wettelijke vertegenwoordigers).

Bewerker betekent de partij die de Persoonsgegevens Verwerkt namens en op aanwijzen van de Verantwoordelijke die niet onder het rechtstreekse gezag van de Verantwoordelijke staat.

Bijzondere Gegevens betekent Persoonsgegevens waaruit de raciale of etnische afkomst, politieke opvattingen of lidmaatschap van politieke partijen of vergelijkbare organisaties, godsdienstige of levensbeschouwelijke overtuiging, lidmaatschap van een beroeps- of vakvereniging of vakbond, fysieke of mentale gezondheid inclusief iedere mening daarover, invaliditeit, genetische code, verslavingen, seksuele geaardheid, strafbare feiten, strafrechtelijke veroordelingen, rechtszaken met betrekking tot strafbaar of onwettig gedrag, of door de overheid verstrekte socialezekerheidsnummers, of enige andere soort Gegevens die krachtens toepasselijk lokaal recht als Bijzondere Gegevens worden beschouwd.

BU Data Protection Executive (BU DPE) of Data Protection Executive (DPE) betekent de eerstelijns Data Protection Executive voor een Bedrijfsonderdeel die is aangesteld krachtens Artikel 17.4, dat wil zeggen iemand in het lokale bedrijfsmanagement met primaire budgetverantwoordelijkheid die verantwoordelijk gesteld kan worden voor de effectieve implementatie en naleving van de Policy, van wie de functie nader omschreven is in Artikel 18.

BU Data Protection Officer (BU DPO) of Data Protection Officer (DPO) betekent de tweedelijs Data Protection Officer voor een Bedrijfs onderdeel die is aangesteld krachtens Artikel 17.5, van wie de functie nader omschreven is in Artikel 18.

Derde betekent elke persoon, privaatrechtelijke organisatie of overheidsorgaan buiten ING.

Derde Bewerker betekent een Derde die Persoonsgegevens Verwerkt namens en op aanwijzen van ING die niet onder het rechtstreekse gezag van ING staat.

Derde Verantwoordelijke betekent een Derde die Persoonsgegevens Verwerkt en de doeleinden en middelen van dergelijke Verwerking bepaalt.

EER of Europese Economische Ruimte betekent alle Lidstaten van de Europese Unie plus Noorwegen, IJsland en Liechtenstein.

EU-Richtlijn voor Gegevensbescherming betekent Richtlijn 95/46/EG van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

Gegevens van Werknemers betekent alle informatie met betrekking tot een geïdentificeerde of identificeerbare Werknemer.

General Legal Counsel betekent het hoofd Juridische Zaken van ING Bank N.V.

Gezinslid betekent de echtgenoot of echtgenote, de partner of het kind die deel uitmaken van het huishouden van de Betrokkene.

Groepsentiteit betekent ING Groep N.V. en ING Bank N.V. en elk bedrijf of elke rechtspersoon, inclusief *branches* en *representative offices*, waarin ING Bank N.V. direct of indirect meer dan 50% van het uitgegeven aandelenkapitaal bezit, 50% of meer van de stemmen op algemene aandeelhoudersvergaderingen heeft, de meerderheid van de leden van de raad van bestuur of een vergelijkbaar bestuursorgaan kan benoemen of ontslaan, of de meerderheid van de stemmen uit kan brengen op vergaderingen van de raad van bestuur of een vergelijkbaar bestuursorgaan.

Guidance Documenten betekent de documenten met aanvullende informatie over en een toelichting op de adequate normen in deze Policy.

ING betekent ING Bank N.V. en de Groepsentiteiten.

Ingangsdatum betekent de datum waarop deze Policy in werking treedt, zoals bepaald in Artikel 5.1.

ING Bank N.V. betekent ING Bank N.V., gevestigd te Amsterdam, Nederland.

Klant betekent elke Derde die een product of dienst van ING aanschaft, kan aanschaffen of heeft aangeschaft.

Land zonder Passend Beschermingsniveau betekent een land dat krachtens toepasselijk lokaal recht (zoals Artikel 25 van de EU-Richtlijn voor Gegevensbescherming) geacht wordt geen 'passend' niveau van gegevensbescherming te bieden. Een lijst van Landen met Passend Beschermingsniveau is beschikbaar op de website van ING.

Leverancier betekent elke Derde die goederen of diensten verstrekt aan ING (bv. een agent, consultant, tussenpersoon of verkoper).

Medewerkers betekent alle Werknemers en andere personen die Persoonsgegevens Verwerken in het kader van hun taken of verantwoordelijkheden met behulp van de informatietechnologiesystemen van ING of die hoofdzakelijk werken vanuit de gebouwen van ING.

Oorspronkelijk Doeleinde betekent het doeleinde waarvoor Persoonsgegevens oorspronkelijk werden verzameld.

Persoonsgegevens of **Gegevens** betekent alle informatie met betrekking tot een geïdentificeerde of identificeerbare Betrokkene.

Policy of **GDP Policy Gegevensbescherming voor Klanten** betekent deze ING Wereldwijde Policy voor Gegevensbescherming van Klant-, Leverancier- en Zakenpartnergegevens.

Prevalerend Belang betekent de dwingende belangen omschreven in Artikel 16.1 op grond waarvan de verplichtingen van ING of rechten van Betrokkenen uiteengezet in Artikel 16.2 en 16.3 in specifieke omstandigheden terzijde kunnen worden geschoven indien dit dwingende belang het belang van de Betrokkene overtreft.

Professionele Contactgegevens betekent alle gegevens die typisch vermeld worden op een visitekaartje en door de Betrokkene gebruikt worden in zijn contacten met ING.

Secundair Doeleinde betekent elk ander doeleinde dan het Oorspronkelijke Doeleinde waarvoor Persoonsgegevens verder Verwerkt worden.

Verantwoordelijke betekent de partij bij de verwerking van de Persoonsgegevens die de middelen en het doeleinde van de Verwerking bepaalt.

Verwerking of **Verwerken** betekent elke bewerking met betrekking tot persoonsgegevens, al dan niet uitgevoerd met behulp van geautomatiseerde procedés, zoals het verzamelen, vastleggen, bewaren, ordenen, wijzigen, gebruiken, verstrekken (met inbegrip van het verlenen van toegang op afstand), doorzending of verwijderen van Persoonsgegevens.

Werknemer betekent een werknemer, een sollicitant of vroegere werknemer van ING. Deze term omvat niet de personen die bij ING werken als externe consultants of werknemers van Derden die diensten verlenen aan ING.

Zakenpartner betekent elke Derde die geen Klant of Leverancier is en een zakenrelatie of strategische alliantie met ING heeft of had (bv. gezamenlijke marketingpartner, joint venture of gezamenlijke ontwikkelingspartner).

Interpretaties

Interpretatie van deze policy:

- (i) Tenzij uit de context anders blijkt, zijn alle verwijzingen naar een bepaald Artikel of een bepaalde Bijlage verwijzingen naar dat Artikel of die Bijlage in of bij dit document, zoals die van tijd tot tijd gewijzigd kunnen worden.

- (ii) Koppen zijn slechts voor het leescomfort opgenomen en kunnen niet gebruikt worden voor het uitleggen van enige bepaling van deze Policy.
- (iii) Indien een woord of zin is gedefinieerd, hebben de andere grammaticale vormen daarvan een overeenkomstige betekenis.
- (iii) De mannelijke vorm verwijst eveneens naar de vrouwelijke vorm (en vice versa).
- (iv) De woorden 'inclusief', 'omvatten' en 'met inbegrip van' en alle woorden die erop volgen moeten worden uitgelegd zonder het algemene karakter van alle voorafgaande woorden of concepten te beperken en vice versa; en
- (v) Een verwijzing naar een document (inclusief, en niet beperkt tot, een verwijzing naar deze Policy) is naar het document zoals gewijzigd, aangepast, aangevuld of vervangen, behalve voor zover verboden door deze Policy of dat andere document.