PRIVACYVERKLARING MEDEWERKERS ABN AMRO

Deze privacyverklaring is gewijzigd op 24 februari 2023

1. Algemeen

Dit is de privacyverklaring voor alle medewerkers van ABN AMRO. Onder ‘medewerkers’ verstaan wij in deze privacyverklaring medewerkers die in dienst zijn van ABN AMRO Bank N.V. en werken voor ABN AMRO of één van de dochterondernemingen. Ook voor externe medewerkers die door de bank zijn ingehuurd zoals via een uitzendbureau of detachering geldt deze privacyverklaring. Voor het gemak spreken we in de rest van deze privacyverklaring over ‘de Bank’ en over ‘medewerkers’.

Graag verwijzen we ook naar de Personal Data Policy waarin de regels zijn opgenomen die zien op interne regels voor het verwerken van persoonsgegevens van klanten, werknemers en andere individuen waarvan de Bank persoonsgegevens verwerkt.

1.1 Wie is er verantwoordelijk voor jouw gegevens?

De Bank is als jouw werkgever verantwoordelijk voor jouw gegevens. Met de Bank wordt bedoeld:

ABN AMRO Bank N.V

Gustav Mahlerlaan 10

1082 PP Amsterdam

Handelsregister KvK Amsterdam, nummer 34334259

1.2 Functionaris voor de gegevensbescherming

De Bank heeft een functionaris voor de gegevensbescherming. De functionaris voor de gegevensbescherming houdt binnen de organisatie van ABN AMRO toezicht op de toepassing en naleving van de AVG. Deze functie is belegd binnen het Privacy Office.

1.3 Wat zijn ‘persoonsgegevens’?

Deze privacyverklaring gaat over het gebruik van jouw persoonsgegevens door de Bank. Maar wat zijn persoonsgegevens precies? De bekendste persoonsgegevens zijn naam, adres, leeftijd en geboortedatum. Ook zakelijke e-mailadressen, telefoonnummers, bankrekeningnummers en je BSN zijn persoonsgegevens. Een speciaal soort persoonsgegevens zijn de zogenaamde bijzondere persoonsgegevens. Dit zijn gegevens die zo gevoelig zijn dat het gebruik ervan de privacy van een individu ernstig kan beïnvloeden. Hieronder vallen o.a. gegevens over je gezondheid, seksuele geaardheid, je culturele achtergrond of lidmaatschap van een vakbond. Biometrische gegevens vallen ook onder bijzondere persoonsgegevens. Dit is een verzameling van technieken om lichaamskenmerken van een individu te meten en vast te stellen, zoals vingerafdrukken (bijvoorbeeld om toegang te

verlenen tot beveiligde ruimtes). De privacywetgeving stelt strenge eisen aan het gebruik van deze bijzondere persoonsgegevens.

2. Grondslag en doeleinden

2.1 Op basis waarvan verwerkt de Bank jouw gegevens?

Iedereen die gegevens van jou krijgt en gebruikt moet daarvoor een reden hebben. De wet noemt dat 'een grondslag voor de verwerking' van jouw persoonsgegevens. Als werkgever gebruikt de Bank jouw gegevens voor één of meer van de volgende wettelijke grondslagen.

- **Overeenkomst**
  De Bank gebruikt jouw gegevens die noodzakelijk zijn om de arbeidsovereenkomst met jou na te kunnen komen.

- **Wettelijke verplichting**
  De Bank verwerkt jouw gegevens ook omdat ze dat moet doen op grond van verschillende wet- en regelgeving.

- **Gerechtvaardigd belang**
  De Bank of een andere partij mag jouw gegevens ook gebruiken als ze daar zelf een belang bij heeft. Dat heet 'gerechtvaardigd belang'. Het belang van de Bank of een andere partij om jouw gegevens te gebruiken moet wel zwaarder wegen dan jouw recht op privacy. De Bank weegt daarbij alle belangen dus af. Voorbeelden waarbij de Bank een gerechtvaardigd belang heeft om jouw gegevens te gebruiken zijn onder andere voor de bescherming van de integriteit en veiligheid van de bank en voor het uitvoeren van een verantwoordelijk, effectief en efficiënt HR-beleid.

- **Vitaal belang**
  Het kan voorkomen dat de Bank jouw gegevens gebruikt omdat dit noodzakelijk is om jouw leven of dat van iemand anders te beschermen. Denk aan een (nood)situatie waarin de Bank gegevens van jou moet doorgeven aan een ziekenhuis.

2.2 Het gebruik van gegevens met jouw toestemming

De Bank zal alleen in uitzonderlijke gevallen om toestemming vragen voor het gebruik van jouw gegevens. Heb je toestemming gegeven? Dan kun je deze altijd intrekken. Het intrekken van je toestemming kan wel gevolgen hebben. Heb je bijvoorbeeld in een app je toestemming gegeven voor het gebruik van jouw locatiegegevens waardoor de app beter werkt? Dan kan deze werking anders zijn op het moment dat je jouw toestemming intrekt.

2.3 Gebruikt de Bank ook gegevens van jou die zij niet van jou zelf heeft gekregen?

Ja, de Bank gebruikt ook gegevens van jou die zij niet van jou zelf heeft gekregen. Denk aan de volgende bronnen:

- Een uitzend- of recruitmentbureau, bijvoorbeeld jouw NAW gegevens ten behoeve van een detacheringsovereenkomst
- Openbare registers waarin jouw gegevens staan, zoals het Handelsregister van de Kamer van Koophandel en het Kadaster
- Het UWV
- De arbodienst
- Een extern bureau dat wordt ingeschakeld in het kader van re-integratie of loopbaanbegeleiding
- In het kader van in-employment screening (zie punt 2.4 onder **Waarvoor gebruikt de Bank jouw gegevens**?) kunnen we referenties opvragen bij oud-werkgevers die jij hebt opgegeven en kan de Bank gebruik maken van openbare bronnen zoals zoekmachines en gedeelten van sociale media die niet privé zijn.
- Het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen. Onder 2.4.3 volgt een korte een toelichting over hoe dit waarschuwingssysteem werkt. Op de site van de NVB lees je meer over dit waarschuwingssysteem en hoe dit werkt: Website NVB.

2.4 Waarvoor gebruikt de Bank jouw gegevens?

De Bank gebruikt als werkgever jouw gegevens voor de volgende doelen.

2.4.1 Verplichting op grond van wet- en regelgeving

De Bank gebruikt gegevens van medewerkers om aan geldende wet- en regelgeving te kunnen voldoen. Denk aan:

- Mifid II. De Bank moet gesprekken die gaan over beleggen tussen adviseurs en klanten vastleggen. Voor meer informatie verwijzen wij naar het Voice Logging & Video Reglement.
- Belastingwetgeving. Op grond van de wet moet de Bank bepaalde informatie over haar medewerkers doorgeven aan de Belastingdienst. Zo worden bijvoorbeeld de BSN, geboortedatum, NAW en nationaliteit verwerkt in de aangifte Loonheffingen.
- Wetboek van Burgerlijke Rechtsvordering. Wordt door iemand beslag gelegd op jouw loon? Dan is de Bank als werkgever wettelijke verplicht hieraan mee te werken en informatie over jou aan de deurwaarder te verstrekken.
- Financieel toezichtregelgeving. Het kan voorkomen dat de Bank verplicht is gegevens van medewerkers te verstrekken aan een toezichthouder in het kader van een toezichtrechtelijk onderzoek of een vergunningaanvraag.
- Wetboek van Strafrecht. Het kan zijn dat de Bank verplicht is gegevens van medewerkers te verstrekken aan opsporingsdiensten in het kader van een strafrechtelijk onderzoek.
- Tuchtrecht Banken. Ben je betrokken bij een incident, dan kan het zijn dat de Bank verplicht is dit te melden bij de Stichting Tuchtrecht Banken.
- Soms moet de Bank persoonsgegevens verstrekken in het kader van een procedure voor de rechter of naar aanleiding van een verzoek van bevoegde autoriteiten (nationaal en internationaal).
- Sociaal zekerheidsrecht. Soms moet de Bank informatie doorgeven aan het UWV, bijvoorbeeld als je langere tijd ziek bent of als je zwanger bent.

2.4.2 Arbeidsovereenkomst

De Bank heeft jouw gegevens nodig om met jou een arbeidsovereenkomst te kunnen sluiten en uitvoeren. De Bank verwerkt je gegevens in dit kader bijvoorbeeld:

- om je salaris uit te betalen;
- je ingezette Employee Benefits te verwerken;
- voor verzuimregistratie;
- voor de training en beoordeling van medewerkers waaronder het Together & Better programma van de Bank;
- in het kader van de pensioenregeling.

2.4.3 Bescherming integriteit en veiligheid

De Bank gebruikt gegevens om de Bank, haar eigendommen, haar gegevens en haar medewerkers zo goed mogelijk te beschermen tegen allerlei vormen van inbreuken en schade. Denk aan:

- Beveiligingscamera's in en rond de gebouwen van de Bank. Lees meer over het gebruik van cameratoezicht binnen de Bank in het Reglement Cameratoezicht.
- Sommige gebouwen en ruimtes van de Bank zijn extra beveiligd, zoals de Computer Centra in Amstelveen: om toegang te verkrijgen tot bepaalde zalen in dit gebouw zal een scan van je vingeraderpatroon worden verwerkt. Omdat het hier om beveiliging gaat die noodzakelijk is voor de Bank, kunnen deze biometrische gegevens worden gebruikt op basis van een gerechtvaardigd belang van de Bank.
- Als je met je mobiele apparaat toegang wil tot het ABN AMRO netwerk wordt je apparaat gescand met een beveiligingstool (Defender MTD). Doel is om onze (klant)gegevens ook via telefoons/tablets zo goed mogelijk te beschermen tegen cybercriminaliteit. Je vindt meer informatie over Defender MTD en het gebruik van persoonsgegevens op intranet.
- Ben je betrokken geweest bij een incident of bestaat daarvan een vermoeden? Dan zal de Bank onderzoek doen en kunnen jouw gegevens daarin worden gebruikt. Bij een incident kun je denken aan ongewenste omgangsvormen (zoals (seksuele) intimidatie, discriminatie, pesten) of ongeoorloofd gebruik van systemen van de Bank. SIM is het centrale aanspreekpunt voor incidenten op het gebied van criminaliteit en veiligheid die de integriteit en het functioneren van de Bank, onze klanten en onze medewerkers kunnen aantasten. De Bank heeft gedragsregels opgesteld waar je je als medewerker aan moet houden. Deze zijn te vinden op General rules of conduct (sharepoint.com).
- De Bank doet aan in-employment screening. Dat betekent dat je niet alleen bij binnenkomst als medewerker wordt gescreend, maar ook als je wisselt naar een functie waarvoor een andere (zwaardere) screening geldt. Hierbij kunnen ook gegevens worden gebruikt die afkomstig zijn uit openbare bronnen.
- De Bank kan in het kader van de veiligheid de activiteit op jouw computer monitoren, waaronder jouw e-mailverkeer van het zakelijk e-mailadres van ABN AMRO.
- Chat jij in het kader van jouw functie met Bloomberg & Reuters of valt jouw functie onder Mifid II regelgeving? Dan kan de Bank jouw chatverkeer monitoren. Zie ook de uitleg onder 2.5.1 Monitoren. In dit kader raden wij je aan het volgende document te lezen: het Reglement e-mail en chat monitoring.

- De Bank kan in het kader van veiligheid en integriteit van de Bank en van onze sector je gegevens gebruiken voor het Interne- en Externe Verwijzingsregister. Zie hieronder een nadere toelichting over deze waarschuwingssystemen.

Het waarschuwingssysteem van de Bank

Stel: een klant of een medewerker is betrokken bij de beschadiging of vermissing van onze eigendommen, er is een vermoeden dat een klant of medewerker fraude pleegt of de overheid of de politie doet onderzoek naar een klant of medewerker.

Dit zijn voorbeelden van voorvallen die de bijzondere aandacht behoeven van de Bank. De Bank moet deze kunnen vastleggen en onthouden zodat ze adequate maatregelen of vervolgstappen kan nemen. De Bank heeft hiervoor een gerechtvaardigd belang.

Dit soort voorvallen noemen we “gebeurtenissen”. Deze worden opgenomen in een speciale interne administratie van de Bank, in het algemeen genoemd “Gebeurtenissenadministratie”, die slechts toegankelijk is voor bevoegde medewerkers. Dit geldt zowel voor klanten als voor medewerkers. Hier lees je verder hoe dit werkt voor medewerkers.

Het Interne Verwijzingsregister (IVR)

Aan de Gebeurtenissenadministratie is een Intern Verwijzingsregister (IVR) gekoppeld. Het IVR zorgt ervoor dat, als wij vinden dat de betrokkenheid van een medewerker bij een gebeurtenis serieus genoeg is, wij onze relevante afdelingen kunnen waarschuwen. Dit geldt ook voor onze groepsmaatschappijen. Deze waarschuwing heeft alleen interne werking (binnen onze organisatie). Of een gebeurtenis via het IVR binnen onze organisatie kan worden gedeeld wordt getoetst aan de AVG regels. In dat geval informeren we onder meer expliciet over de redenen voor opname, de gevolgen van de opname voor de medewerker en zijn of haar relatie met ons en met onze groepsmaatschappijen. Ook informeren we over de duur van de opname en de rechten van de medewerker, bijvoorbeeld het recht van bezwaar.

Het Externe Verwijzingsregister (EVR)

Aanvullend hebben financiële instellingen in Nederland, waaronder ABN AMRO, een waarschuwingssysteem ontwikkeld die, anders dan de Gebeurtenissenadministratie en het IVR externe werking heeft.

Hiermee kunnen zij toetsen of iemand:

- ooit fraudeerde,
- probeerde te frauderen,
- of op een andere manier een bedreiging vormt voor de veiligheid van de bankensector. Dit systeem geldt ook voor klanten. Andere banken aangesloten bij de NVB maken ook hier gebruik van. Vandaar dat je op de Website van de NVB en de Website van de AP meer kan lezen over dit waarschuwingssysteem en hoe dit werkt. De regels die bepalen hoe de banken, en dus ook ABN AMRO, gebruik kunnen maken van het externe waarschuwingssysteem zijn goedgekeurd door de Autoriteit Persoonsgegevens. Je kunt deze regels ook op de site van de NVB lezen. Als je opgenomen wordt in dit externe waarschuwingssysteem word je conform deze regels geïnformeerd over de registratie en hoe je je (privacy)rechten kan uitoefenen.

Het IVR en EVR toetsen wij als je bij ons wil komen werken. Alleen degenen die zich bezighouden met klant-, product- en medewerkersacceptatie mogen een toets doen op deze lijsten. Deze medewerkers krijgen slechts een signaal als je geregistreerd bent. Alleen een beperkt aantal bevoegde medewerkers hebben de details over de redenen van opname op de lijsten. Er wordt altijd overwogen aan de hand van deze informatie of de Bank deze medewerker kan accepteren en zo ja - onder welke voorwaarden.

2.4.4 Efficiënt en optimaal gebruik van faciliteiten, zoals IT, werkplekken en gebouwen

De Bank gebruikt persoonsgegevens om de medewerkers zo goed mogelijk te kunnen voorzien van de benodigde faciliteiten. Voorbeelden zijn:

- Verspreiding over de verschillende ruimtes en gebouwen. Denk onder andere aan het reserveren van vergaderkamers, parkeerplekken of het vinden van een vrije werkplek. Zo kan op grond van wifi signalen de bezetting van de verschillende werkruimtes worden bijgehouden. Denk verder aan jouw toegangspas waarmee de Bank jouw aanwezigheid in het gebouw bijhoudt en de bezetting analyseert. Middels analyses wordt gekeken of het beoogde gebruik en het daadwerkelijke gebruik van het pand op elkaar aansluit.
- Monitoring van het gebruik van IT-appratuur, zoals video conferencing equipment en printers, of het gebruik van softwarepakketen op de ABN AMRO laptops.

De gebruikersdata van de faciliteiten kan naast monitoring ook gebruikt worden voor (statistische) onderzoeken naar de impact van (het gebruik van) specifieke faciliteiten en gerelateerd beleid op medewerkers en bedrijfsdoelstellingen. Denk hierbij aan onderzoek welke faciliteiten bijdragen aan een verbeterde dienstverlening van ABN AMRO, of hoe bepaalde faciliteiten bedragen aan de Employee Experience. De uitkomsten van dergelijke onderzoeken zijn nooit herleidbaar tot individuen.

2.4.5 HR Management

De Bank gebruikt persoonsgegevens om een verantwoordelijk, effectief en efficiënt HR-beleid te kunnen uitvoeren. Denk hierbij aan activiteiten als:

- Personeelsplanning en het beleid rond in- en uitstroom.
- Beleid rondom ziekteverzuim en re-integratie.
- Subsidieaanvraag voor medewerkers met een afstand tot de arbeidsmarkt.
- De producten die vanuit HR worden aangeboden, zoals opleidingen en trainingen.
- Het meten van experience en engagement van medewerkers.
- Analyses op basis van data (geavanceerde) statistische methoden
    - Beleidsanalyses: onderzoeken die worden uitgevoerd om de impact van HR-strategie en -beleid op medewerkers- en bedrijfsdoelstellingen te duiden. Voorbeelden van onderzoeksvragen zijn ‘Welke trainingen hebben invloed op onze klanttevredenheid?’ en ‘Wat zijn belangrijke drijfveren voor de betrokkenheid van medewerkers bij de organisatie?’ Een beperkt aantal medewerkers hebben vanuit hun functie toegang tot deze gegevens. De resultaten van dergelijke onderzoeken en bijbehorende adviezen zijn nooit herleidbaar tot individuele medewerkers.
    - Persoonlijke analyses: Binnen de dienstverlening van HR kan data ingezet worden om medewerkers van persoonlijk advies te voorzien. Denk hierbij aan het (vrijblijvend)

aanbevelen van specifieke vacatures of trainingen. Zie ook de 'Module Gepersonaliseerde HR Dienstverlening' voor meer informatie onder welke voorwaarden dit plaats kan vinden.

- Het diversiteitsbeleid van de Bank. De Bank streeft naar het bankbreed weerspiegelen van de groeiende diversiteit binnen de samenleving. Zij wil daarom graag monitoren hoe de diversiteit binnen de verschillende (functie)lagen van de organisatie ervoor staat, zodat zij indien nodig interventies kan ontwikkelen. De Bank gebruikt hiervoor gegevens over geslacht, leeftijden land van herkomst van haar medewerkers. Een beperkt aantal medewerkers hebben vanuit hun functie toegang tot deze gegevens. Verder gebruikt de bank deze gegevens op geaggregeerd niveau. 'Geaggregeerd' betekent dat de gegevens niet op persoonsniveau worden verwerkt. De Bank gebruikt wat betreft land van herkomst alleen gegevens van medewerkers die deze zelf vrijwillig voor dit doel hebben ingevuld: in MyHR kun je invullen wat jouw geboorteland of dat van je vader of moeder is. Deze gegevens kun je altijd aanpassen of verwijderen.
- Het inlcusiebeleid van de bank: de Bank gebruikt bijvoorbeeld gezondheidsgegevens van medewerkers op vrijwillige basis voor het aanvragen en behouden van een keurmerk dat van toegevoegde waarde is voor de Bank en de medewerker. De medewerker beslist zelf of hij of zij de gezondheidsgegevens beschikbaar stelt voor dit doel.

2.4.6 Verbetering en vernieuwing dienstverlening

- Maak je gebruik van een telefoon van de Bank (voor zakelijk gebruik) voor jouw klantcontact? Dan kan de Bank telefoongesprekken of (video) chats van jou met klanten opnemen (loggen) om de kwaliteit van deze gesprekken te verbeteren. Denk aan de werkzaamheden in het Contact Center. Zie ook de uitleg onder 2.5.1 Loggen.
- Om interne processen te verbeteren kan gebruik worden gemaakt van rapportages / dashboards. Het is niet toegestaan de dashboards te gebruiken voor beoordeling van medewerkers, tenzij dit specifiek is opgenomen in een door de Raad van Medewerkers goedgekeurd Reglement. Zie voor meer informatie het Memo Persoonsgegevens in (online) dashboards en rapportages binnen ABN AMRO.
- Innovatie. Het kan zijn dat medewerkers die zelf actief betrokken zijn bij de ontwikkelingen van nieuwe technieken (DevOps, Ciso) de tool in ontwikkeling zelf testen. Voorwaarde voor deelname is dat privacyrechten zijn gewaarborgd voor betrokken medewerkers. Dit wordt per geval beoordeeld.
- Toepassing van geavanceerde technologieën, zoals Artificial Intelligence worden gebruikt om medewerkers te ondersteunen bij de uitvoering van hun werkzaamheden.

2.5 Logging & Monitoring

Zoals je hierboven al hebt kunnen lezen maakt de Bank gebruik van verschillende loggings- en monitoringstechnieken. Wat bedoelen we met loggen en monitoren?

2.5.1 Loggen

Als de Bank logt, legt zij de gegevens vast zodat zij later – bijvoorbeeld als de toezichthouder onderzoek doet – deze gegevens kan raadplegen. Bepaalde logs kunnen vervolgens worden gebruikt om te monitoren (zie voor verdere uitleg over monitoren paragraaf 2.5.2 Monitoren). Voorbeelden van loggen zijn:

- Vastleggen wie wanneer toegang heeft gehad tot een bepaalde ruimte (bijvoorbeeld gebruik toegangspas).
- Het opnemen van telefoongesprekken van medewerkers van het Contact Center en de Dealing Room om de kwaliteit van deze gesprekken te verbeteren.
- Het vastleggen en opnemen van video-opnames voor interne informatievoorziening, voor meer informatie zie Hoofdstuk 2 van het Voice Logging & Video Reglement.
- Vastleggen van wie wanneer toegang heeft gehad tot applicaties met vertrouwelijke medewerker-, klant- en of productinformatie en wie wat wanneer waar gezien en gewijzigd heeft in deze applicaties (zie voor meer informatie: Audit Trail on employee and client data (Policy nummer: S07-400)).
- Ook moet de Bank op grond van Europese regelgeving telefoongesprekken die gaan over beleggen tussen adviseurs en klanten vastleggen.

Lees meer over 'logging' in het Voice Logging & Video Reglement.

Wij raden je aan de volgende documenten te lezen voor meer informatie over dit onderwerp:

- De gedragsregels voor het zakelijk gebruik van e-mail, intranet en internet: Use of email, intranet and internet (sharepoint.com).
- De Information Security Awareness & Secure Behaviour Policy
- De Standard for Audit Trail on employee and client data

2.5.2 Monitoren

Monitoren betekent iets anders dan loggen. Als de Bank monitort, houdt zij actief bij wat er op een bepaalde plek of binnen een bepaald kanaal (o.a. e-mailverkeer) gebeurt en grijpt ze in als er iets verkeerd gaat. Meer hierover lees je in het Reglement Personeelsvolgsystemen.

De Bank monitort haar medewerkers voor verschillende doelen. We maken daarbij geen gebruik van geautomatiseerde besluitvorming.

- **Veiligheid**: denk aan het monitoren van mail- en chatverkeer, maar ook fax-, scan- en printverkeer of documenten opslaan op een USB stick (dit betekent dat de Bank kan monitoren dat interne documenten op een externe device worden opgeslagen).
- **Voldoen aan wettelijke verplichtingen**: zo monitort de Bank effectentransacties van medewerkers afhankelijk van hun compliance status.
- Efficiënt en optimaal gebruik van faciliteiten, zoals IT, werkplekken en gebouwen: wifi-tracking, sensoren, pasjes data, reserveringsdata. Dit bekijken we niet op persoonsniveau.
- Het voorkomen van **ongeoorloofd rekeningkijken** door medewerkers.

2.6 Gebruik voor andere doelen dan waarvoor de Bank jouw gegevens eerst had verkregen

De Bank mag jouw gegevens ook gebruiken voor andere doelen dan waarvoor je ze oorspronkelijk had gegeven. Daarbij geldt wel dat dat nieuwe doel moet passen bij het doel waarvoor je jouw gegevens in eerste instantie aan de Bank had gegeven. Om te bepalen of dit het geval is, kijkt de Bank in ieder geval naar de volgende punten.

- Is er een duidelijk verband bij het doel waarvoor je de gegevens eerder gaf? Past het nieuwe doel daarbij?
- Hoe zijn de gegevens ooit van jou verkregen? Zijn de gegevens van jouzelf gekregen of op een andere manier?
- Om wat voor soort gegevens gaat het precies? Heel gevoelige gegevens? Of minder gevoelige gegevens?
- Wat zijn de gevolgen voor jou als de Bank de gegevens op een andere manier gebruikt? Is dat in jouw voordeel, jouw nadeel of maakt het niet uit?
- Wat kan de Bank doen om jouw gegevens zo goed mogelijk te beschermen als zij deze opnieuw gebruikt? Denk aan anonimiseren of versleutelen.

2.7 Profilering

De Bank maakt gebruik van profilering. Hieronder verstaan we het indelen van mensen in groepen (profielen). Op basis hiervan kan de Bank persoonlijke aspecten evalueren en analyseren en voorspellingen doen. Hieronder lees je waarvoor en wanneer de Bank dat doet met persoonsgegevens van medewerkers.

- **Voorkomen van ongeoorloofde transacties**
  De Bank monitort effectentransacties van medewerkers afhankelijk van hun compliance status. Het doel hiervan is om ongeoorloofde transacties, zoals handel met voorkennis, te voorkomen. De Bank gebruikt hierbij profielen. Een profiel bestaat uit kenmerken waaraan de Bank ongeoorloofde transacties kan herkennen. De Bank doet onderzoek als er mogelijke ongeoorloofde transacties worden gezien. Als wordt vastgesteld dat je daadwerkelijk een ongeoorloofde transactie hebt uitgevoerd kun je op staande voet worden ontslagen.
- **Gepersonaliseerde HR-dienstverlening**
  De Bank kan analyses uitvoeren om haar dienstverlening te personaliseren, (zie punt 2.4.5 en de ‘Module Gepersonaliseerde HR Dienstverlening’).

Je hebt het recht om bezwaar te maken tegen het gebruik van jouw persoonsgegevens voor profileringsdoeleinden. Jouw bezwaar kun je indienen via Contact HR (via de medewerkerspagina op intranet).

De Bank hoeft jouw verzoek niet altijd te honoreren.

3. Het delen van je gegevens met derden en doorgifte buiten de EU

3.1 Geeft de Bank jouw gegevens ook aan anderen?

Ja, soms zal de Bank jouw gegevens ook met anderen moeten delen.

- **Pensioenfonds en verzekeraars**
  Bijvoorbeeld aan ABN AMRO Pensioenfonds om jouw pensioen te kunnen regelen. Of aan een verzekeraar, bijvoorbeeld als er een verzekering is afgesloten voor een aanvulling op de WIA-uitkering bij arbeidsongeschiktheid.

- **Arbodienst**
  Meld je je ziek? Dan komt deze melding ook terecht bij Beter, de arbodienst (en dochteronderneming) van de Bank. In deze melding staat niet wat de reden van de ziekte/het verzuim is.
- **Nationale en Internationale Overheidsinstanties**
  De Bank moet soms op grond van de wet jouw gegevens geven aan overheidsinstanties zoals de Belastingdienst en het UWV en soms ook bevoegde internationale overheidsinstanties. Ook onze toezichthouders kunnen gegevens opvragen. Als de wet hiertoe verplicht, moet de Bank gegevens met hen delen waar ook jouw gegevens bij kunnen zitten. Het kan voorkomen dat de politie in verband met een incident camerabeelden opvraagt waar jij ook op voorkomt. Als de Bank hiertoe verplicht is, zal zij deze beelden doorgeven aan de politie.
- **Stichting Tuchtrecht Banken**
  Werknemers in de financiële sector zijn gebonden aan het Tuchtrecht Banken. In het kader van een tuchtrechtzaak kan het zijn dat persoonsgegevens verstrekt worden aan de Stichting Tuchtrecht Banken.
- **Andere bedrijven**
  De Bank werkt samen met andere bedrijven. Het kan zijn dat die bedrijven ook jouw gegevens nodig hebben om hun werk voor de Bank goed te kunnen doen. Denk aan KPN, voor de afwikkeling van de telefoonabonnementen van medewerkers, de ABM AMRO Alert app (Everbridge) of Pronk Geschenken voor het Thumbs Up programma. De Bank kiest de bedrijven waarmee zij werkt zorgvuldig uit. De Bank maakt duidelijke afspraken in een contract over hoe zij met jouw gegevens omgaan. De Bank blijft zelf verantwoordelijk als zij een ander bedrijf inschakelt dat voor haar werkt.

3.2 Worden je gegevens ook buiten Europa verwerkt?

De Bank en haar groepsmaatschappijen kunnen soms persoonsgegevens met elkaar delen. Ook wanneer deze groepsmaatschappijen zich buiten Europa zich bevinden. Denk bijvoorbeeld aan de situatie dat je als expat werkzaamheden voor de vestiging in Sydney zou verrichten. De Bank zou dan gegevens van jou doorgeven aan die vestiging, zodat je kan worden opgenomen in de systemen daar. De Bank moet zich hierbij aan de lokale regelgeving houden.

Het delen van persoonsgegevens met groepsmaatschappijen buiten Europa doet de Bank op basis van haar wereldwijde interne beleid, de Binding Corporate Rules (BCRs). Dit beleid is door de Autoriteit Persoonsgegevens goedgekeurd.

Het kan ook zijn dat de Bank gebruik maakt van IT leveranciers die buiten Europa zijn gevestigd, of die hun dienstverlening ook vanuit landen buiten Europa aanbieden. Als dit het geval is zal de Bank ervoor zorgen dat deze doorgifte gebeurt in lijn met de privacywetgeving.

4. Beveiliging en bewaartermijnen

4.1 Beveiliging van je gegevens

De Bank doet haar uiterste best om de gegevens van haar medewerkers zoveel mogelijk te beschermen. De Bank investeert daarvoor veel in haar mensen, systemen en procedures. De manier van werken

wordt steeds afgestemd op de gevoeligheid van de gegevens. Medewerkers worden getraind om veilig om te gaan met de gegevens.

Juist vanwege jouw veiligheid kunnen we niet in detail treden over de precieze maatregelen die we in verband met gegevensbeveiliging nemen. Onder punt 2.4.3 van Waarvoor gebruikt de Bank jouw gegevens? vind je voorbeelden van maatregelen waarmee de Bank de gegevens van medewerkers beveiligt. Andere veiligheidsmaatregelen waarmee je misschien wel eens te maken hebt gehad zijn:

- toegang tot banksystemen met inlogcodes of zelfs een dubbele verificatie;
- beperking toegang tot gegevens: alleen de personen die hiertoe bevoegd zijn krijgen toegang tot gegevens;
- eisen aan het versturen van vertrouwelijke documenten.

4.2 Hoe bepaalt de Bank hoe lang jouw gegevens worden bewaard?

De Bank bewaart gegevens van jou: denk aan jouw HR dossier (waaronder jouw arbeidsovereenkomst en officiële beoordelingen), e-mails, chat-historie en door jou opgestelde documenten (ook die niet zien op klantcontact).

Bij het bepalen van de verschillende bewaartermijnen voor deze gegevens, hanteert de Bank het uitgangspunt dat ze in elk geval worden bewaard zolang dat nodig is voor het bereiken van het doel waarvoor ze zijn gekregen. Verder is hierbij het volgende van belang.

- De privacywetgeving kent geen concrete bewaartermijnen voor persoonsgegevens. In andere wetten kunnen wél minimale bewaartermijnen staan. Dan moeten die gegevens dus ook zo lang worden bewaard. Denk bijvoorbeeld aan het Burgerlijk Wetboek, belastingwetgeving of financiële wetgeving zoals Mifid II en de Wwft.
- Het kan zijn dat de Bank betrokken raakt bij een rechtszaak of andere procedure. In Nederland of in het buitenland. Om te kunnen bewijzen hoe de zaak in elkaar zit, kan het zijn dat de Bank gegevens gebruikt waar gegevens van jou bij zitten (zoals e-mails van jou over het geschil). De Bank kan gegevens in een archief bewaren totdat een eventuele claim verjaard is en zij niet meer betrokken kan worden bij een procedure.

In de Local Retention Schedule (een bijlage bij de Data Retention Policy van de Bank) heeft de Bank voor een aantal categorieën persoonsgegevens de bewaartermijnen geformuleerd.

5. Welke rechten heb je?

- **Inzage en rectificatie**
  Je hebt het recht inzage te krijgen in de persoonsgegevens die de Bank van jou verwerkt. Ook kun je de Bank vragen jouw gegevens te verbeteren als deze niet kloppen. Veel van jouw gegevens kun je zelf inzien en wijzigen via MyHR, My Compliance, My Learning, Sharepoint en Talent2Grow. Heb je een aanvullend verzoek? Dan kun je jouw verzoek indienen bij Contact HR (via de medewerkerspagina op intranet).
- **Vergetelheid**
  In sommige gevallen kun je de Bank ook vragen jouw gegevens te wissen. De Bank hoeft een verzoek om jouw gegevens te wissen niet altijd te honoreren. Bijvoorbeeld niet als zij op grond van de wet jouw gegevens nog langer moet bewaren.

- **Bezwaar**
  Je kunt bezwaar maken tegen het gebruik van jouw persoonsgegevens die worden verwerkt op grond van het gerechtvaardigd belang van de bank. De Bank hoeft de verwerking niet altijd te staken. Bijvoorbeeld niet als zij een belang heeft dat zwaarder weegt dan het belang van de medewerker.
- **Beperking**
  Je kunt de Bank ook vragen tijdelijk het gebruik van jouw persoonsgegevens te beperken. Dat kan in de volgende gevallen:
  - Je denkt dat jouw persoonsgegevens niet juist zijn;
  - De Bank maakt ten onrechte gebruik van jouw persoonsgegevens;
  - De Bank wil jouw persoonsgegevens vernietigen (bijvoorbeeld na de bewaartermijn) maar je hebt ze nog nodig.

Ook een bezwaar, verzoek tot het wissen of beperken van je gegevens kun je indienen via Contact HR. Geef hierbij altijd duidelijk aan wat de reden is van je verzoek.

Voor meer informatie over jouw rechten en hoe je een verzoek kunt doen kun je terecht bij Contact HR. Op de intranetpagina van Contact HR kun je gebruikmaken van het contactformulier. Je kunt ook bellen naar 020 - 343 6000 (op werkdagen van 9:00 tot 17:00 uur).

- **Recht op dataportabiliteit** (overdraagbaarheid van gegevens)
  De Bank kan er voor zorgen dat jij jouw gegevens krijgt die je haar hebt gegeven en die geautomatiseerd worden opgeslagen. Dit geldt alleen als de Bank jouw gegevens verwerkt op basis van toestemming of de (arbeids)overeenkomst die zij met jou heeft gesloten. Dat heet ‘data portabiliteit’. Je mag de Bank ook vragen jouw gegevens rechtstreeks aan een andere partij te geven zoals een opvolgend werkgever.

Een verzoek om jouw gegevens te ontvangen of aan een ander te geven kun je doen via Contact HR.

Let op de veiligheid van jouw gegevens Controleer of de partij aan wie je jouw gegevens wilt geven, te vertrouwen is en net zo veilig met uw gegevens omgaat als de Bank. Als jij jouw gegevens zelf wilt ontvangen, let er dan op dat je eigen apparatuur veilig genoeg is en bijvoorbeeld niet is- of kan worden gehackt.

Heb je een vraag, Is er is iets onduidelijk of heb je een klacht?

Neem dan contact op met HR via Contact HR. Ben je niet tevreden over de afhandeling? Dan is het mogelijk contact op te nemen met de Functionaris Gegevensbescherming via privacy.office@nl.abnamro.com. Ook heb je het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.

6. Wijziging van de Privacyverklaring

Het kan zijn dat er in de loop van de tijd veranderingen in het gebruik van persoonsgegevens plaatsvinden door wijziging van wet- en regelgeving of wijziging van interne procedures of systemen die rechtstreeks gevolgen hebben op het gebruik van jouw persoonsgegevens door de Bank. In dat geval wordt de privacyverklaring aangepast en zal de Bank jou daarover informeren. Je ziet dan een

aankondiging van de wijziging op Intranet. Ex-medewerkers kunnen contact opnemen met Contact HR om kennis te nemen van de privacyverklaring. Je kunt ook bellen naar 020 - 343 6000 (op werkdagen van 9:00 tot 17:00 uur).