

Europa, Midden-Oosten en Afrika (EMEA)

Wells Fargo Internationale Privacykennisgeving Contingente Hulpbronnen

Deze kennisgeving is van toepassing voor het Verenigd Koninkrijk ("**UK**"), landen in de Europese Unie ("**EU**") en het Dubai Internationaal Financieel Centrum ("**DIFC**") (verenigd "**EMEA**").

Ingangsdatum: 9 dec 2022

"**Wij**," "**onze**," "**ons**" of "**Bedrijf**" verwijst naar de Wells Fargo-entiteit die het bedrijf dat u inhuurt, of waarvoor u anderszins werkt (de "**Leverancier**"), om bepaalde diensten voor ons uit te voeren. In het kader van deze verbintenis verleent u ons namens de Leverancier bepaalde diensten en treden wij op als verwerkingsverantwoordelijke voor de verwerking van informatie die op u betrekking heeft ("**Persoonsgegevens**"). U dient bij de leverancier te informeren welke Wells Fargo-entiteit de verwerkingsverantwoordelijke van uw Persoonsgegevens is. Als u een aanbieder van aannemers bent, zal die entiteit een van de in Sectie 11 genoemde entiteiten zijn die in hetzelfde land als de leverancier zijn gevestigd. Als u een externe adviseur bent, zal die entiteit waarschijnlijk een van de in Sectie 11 genoemde entiteiten zijn. De Leverancier kan u het adres en het e-mailadres van de betrokken Wells Fargo-entiteit verstrekken.

Dit document wordt de "**Kennisgeving**" genoemd.

Wells Fargo is een van de grootste financiële instellingen die wereldwijd actief zijn. Wij hebben wereldwijd gelieerde ondernemingen, onder andere in de Verenigde Staten ("**Gelieerde Entiteiten**"). Zoals beschreven in Sectie 2 moeten wij, om uw verbintenis bij ons te beheren, bepaalde Persoonsgegevens verwerken, zoals hieronder beschreven.

Naam van groep moedermaatschappij: Wells Fargo & Company

Locatie hoofdkantoor: 420 Montgomery Street; San Francisco, CA 94104 USA

De contactgegevens van onze EMEA Regionale Privacyfunctionaris staan vermeld in Sectie 9. Wells Fargo & Company en haar filialen en dochterondernemingen zijn gezamenlijk "Wells Fargo".

1. Welke Persoonsgegevens verzamelen we?

Het is mogelijk dat we de volgende categorieën Persoonsgegevens verzamelen:

- **Algemene gegevens:** voor-, tussen- en achternaam (inclusief eerder gebruikte namen); persoonlijke contactgegevens (vaste en mobiele telefoonnummers, e-mailadressen en huisadres); geboortedatum en plaats; nationaliteit; burgerlijke staat; geslacht; en veteraan-/militaire status.
- **Positie of aanwerving / werkbeschrijving:** aanwervende entiteit; titel; functie; duur van dienstverband en werkvergunningstatus.

- **Identificatie- en authenticatiegegevens:** nationaal of overheidsidentificatie zoals paspoort of nationale identiteitskaart; rijbewijs; nationaal verzekeringsnummer of fiscaal en/of sociaal verzekeringsnummer; informatie vereist voor belastingaangifte; woonadres en telefoonnummer; documenten die adres verifiëren; geboortedatum; land van domicilie; documenten die werkstatus verifiëren; en handtekeningautorisatie of informatie die we gebruiken om u te identificeren en authentifieren, bv. uw handtekening of eventuele extra gegevens die we nodig hebben voor naleving die we van externe bronnen verkrijgen.
- **Financiële gegevens en betalingsgegevens:** salaris en andere inkomsten; bankrekeninggegevens en financiële betrekkingen.
- **Achtergrond- of kredietcontrolegegevens:** Voor zover vereist of toegestaan door de lokale wetgeving, informatie over krediet- en achtergrondcontroles, waaronder krediet- en strafrechtelijke controles en onderzoeken; arbeidsgeschiedenis; huidige en voormalige bestuursfuncties van uzelf of van leden van uw directe familie; gegevens in verband met de verificatie van politiek prominente personen; onderwijsgeschiedenis; professionele lidmaatschappen en beoordelingen; professionele of persoonlijke verwijzingen; en andere informatie in uw curriculum vitae of cv.
- **Kwalificatiegegevens:** informatie over eventuele kwalificaties waarover u beschikt, bv. universitaire opleiding, beroepscertificaten.
- **Visum- en werkvergunninggegevens:** kopieën van uw paspoort; geboorteakte; nationale identiteitskaart; bestaande en verlopen visum(s) en andere vergunninggegevens; en alle informatie over relevante leden van uw gezin (zoals uw ouders, echtgenote, inwonende/geregistreerde partner, kinderen en/of andere afhankelijke personen), indien legitiem vereist.
- **Contactgegevens voor noodgevallen:** voor- en achternaam, en contactgegevens van een familielid waar in geval van nood contact mee opgenomen kan worden.
- **Contactgegevens werk:** werkadres; telefoon- en faxnummers; en e-mailadres van het werk.
- **Contractgegevens:** algemene voorwaarden van uw contract; loon en wijzigingen in de algemene voorwaarden van uw tewerkstelling of arbeidsrelatie.
- **Organisatorische gegevens:** titel; baanpositie; functie; werknemer-ID; afdeling; bedrijfsonderdeel; namen leidinggevende en top-leidinggevenden; kostenplaats; tekenbevoegdheid; vaardigheden; werkervaring bij het Bedrijf; gebruikers-ID; IT-toegangsrechten (zoals gebruikers- en systeem-ID's en wachtwoorden); en elektronische inhoud die u produceert als u gebruikt van bedrijfssystemen.
- **Werkgerelateerde gegevens:** informatie op urenlijsten voor uw werk (voor zover dit op u van toepassing is), alle gegevens die in het kader van contractuele diensten kunnen worden verzameld, waaronder zakenreizen; zakelijke uitgaven; thuiswerken (indien van toepassing); gebruik van bedrijfsfaciliteiten; opleidingsactiviteiten; en aanwezigheid op kantoor en bij bedrijfsevenementen.
- **Toegang of systeemgebruiksgegevens:** informatie gegeven door het invullen van formulieren en enquêtes, en gegevens over uw gebruik van onze toepassingssystemen, met inbegrip van authenticatieinloggegevens zoals gebruikersnamen of ID's en wachtwoorden om in te loggen op portalen; locatiegegevens; gebruikersweergavenaam en identificatie; andere website- of producttoegang informatie.
- **Computergebruiksgegevens:** gegevens over uw gebruik van (bijvoorbeeld hoe, wanneer en waar u gebruik maakt van en omgaat met) apparatuur, elektronische communicatiesystemen en eigendommen, zoals computers, mobiele toestellen, e-mail, chatberichten, internet, intranet SharePoint sites, gedeelde schijven en andere gegevensopslagplaatsen, en voicemail.
- **Marktgegevens:** informatie uit marktonderzoek, alle verkregen gegevens en geuite meningen bij deelname aan eventuele enquêtes.
- **Geografische gegevens:** informatie over uw locatie, bv. over eventuele controle van de werklocatie voor nalevings- en andere doeleinden.

- **Prestatiegegevens:** informatie over de kwaliteit en de efficiëntie van de diensten die u levert, in vergelijking met de overeengekomen criteria tussen de onderneming en de Leverancier of uzelf (naargelang het geval) en andere soortgelijke prestatiebeoordelingen.
- **Disciplinaire gegevens:** informatie over gedrag, disciplinaire en klachtenonderzoek en disciplinaire en klachtzaken.
- **Afwezigheidsgegevens:** data van afwezigheden redenen voor afwezigheid (zoals medisch verlof), voor zover deze op u van toepassing zijn.
- **Onderzoeksgegevens:** gegevens verzameld voor Wells Fargo onderzoekproces (indien toegepast) bv. due diligence controles, fraude, sancties en anti-witwascontroles, externe inlichtingenrapporten, en inhoud en metagegevens in verband met relevante uitwisselingen van informatie tussen personen, organisaties, inclusief, e-mails, live chat, videogesprekken, voicemail enz.
- **Klachtgegevens:** gegevens verzameld voor de verwerking in verband met eventuele klachtenprocedures van Wells Fargo.
- **Reglementaire gegevens:** informatie die we nodig hebben om onze reglementaire verplichtingen na te komen.
- **Gegevens van derden:** de naam, titel, inhuurbedrijf/werkgever, contactgegevens en locatie van elke persoon met wie u verwant bent of een nauwe persoonlijke relatie mee hebt, en die: (i) u een functie/persoonlijke referentie heeft gegeven; (ii) een VS of niet-VS overheidsfunctionaris is; of (iii) beslissingsbevoegdheid/bevoegdheid heeft over zaken die het Bedrijf betreffen.
- **Gevoelige Persoonsgegevens:** Het Bedrijf kan ook bepaalde soorten Gevoelige Persoonsgegevens verzamelen zoals toegestaan en/of vereist door de lokale wetgeving, zoals gezondheids- of medische informatie (bv. gezondheids- en ziektedossiers), invaliditeitsstatus (gezamenlijk "**Gevoelige Persoonsgegevens**"). We verzamelen deze informatie voor specifieke doeleinden, zoals gezondheids-/medische informatie om een invaliditeit of ziekte op te vangen en om bepaalde werkvoorzieningen aan te bieden (zoals flexibele thuiswerkregelingen). Zoals in Sectie 2 nader wordt uitgelegd, zullen we dergelijke gevoelige informatie alleen voor die doeleinden gebruiken en zoals legitiem is toegestaan.

2. Voor welke doeleinden gebruiken we Persoonsgegevens?

Het Bedrijf gebruikt Persoonsgegevens voor de hieronder vermelde doeleinden op basis van een of meer van de volgende legitieme bases:

- omdat de lokale wetgeving ons daartoe verplicht;
- omdat die informatie nodig is om het contract uit te voeren;
- omdat deze informatie nodig is om de vitale belangen van een persoon te beschermen;
- omdat deze informatie nodig is voor de uitvoering van algemeen belang (bv. ter voorkoming of opsporing van criminaliteit of fraude); omdat u deze informatie vrijwillig verstrekt en ons toestemming geeft om deze te verwerken;
- omdat we een specifiek legitiem belang hebben om deze te verwerken of als we onze legitieme belangen moeten nastreven. In dergelijke gevallen hebben we een legitiem belang bij de verwerking van Persoonsgegevens, bijvoorbeeld (i) om ervoor te zorgen dat onze netwerken en informatie veilig zijn; en (ii) om zaken binnen het Bedrijf en in de hele organisatie te beheren en in het algemeen uit te voeren;
- om een legitieme verplichting na te komen;
- om onze legitieme rechten vast te stellen, te gebruiken en te verdedigen;
- voor verzekeringsdoeleinden.

Het Bedrijf gebruikt Persoonsgegevens om u in staat te stellen diensten aan ons te verlenen op basis van onze verbintenis met de Leverancier, met inbegrip van het gebruik en de verwerking van de bovengenoemde categorieën van Persoonsgegevens voor de volgende doeleinden ("**Verbintenisdoeleinden**").

- **Onderhouden en verbeteren van een doeltreffende administratie van onze verbintenismet de Leverancier**, waaronder toewijzen van projecten en taken, uitvoeren van analyse en planning van middelen, registreren van projectkosten en schattingen, beheren van werkactiviteiten en geven van trainingen over naleving. Het Bedrijf kan voor deze doeleinden algemene gegevens, functie/tewerkstellingsomschrijving, organisatorische gegevens, identificatie- en authenticatiegegevens, toegangsgegevens of systeemgegevens, financiële gegevens en betalingsgegevens, werkcontactgegevens, contractgegevens, prestatiegegevens, werkgerelateerde gegevens, geografische gegevens, kwalificatiegegevens, gegevens van derden, klachtengegevens, onderzoeksgegevens, reglementaire gegevens, afwezigheidsgegevens en disciplinaire gegevens verwerken. We verwerken dergelijke gegevens omdat deze nodig zijn om een overeenkomst die we met u hebben uit te voeren; omdat we een specifiek legitiem belang hebben om deze te verwerken of als we onze legitieme belangen moeten nastreven; om te voldoen aan een legitieme verplichting; om onze legitieme rechten vast te stellen, te gebruiken en te verdedigen; of, indien van toepassing, omdat u deze informatie vrijwillig verstrekt en ons toestemming geeft om deze te verwerken.
- **Het onderhouden en verbeteren van een effectieve administratie van het personeelsbestand en de Bedrijfsfaciliteiten**, waaronder: het toewijzen van projecten en taken; het regelen van zakenreizen; het beheren van zakelijke uitgaven en vergoedingen; het beheren en administreren van vakantietijd, kantoortijd en (ziekte)verlof; het uitvoeren van personeelsevaluatie en -planning; het beheren van projectkosten en schattingen; het beheren van werkactiviteiten; het beheren van overplaatsingen; het geven van prestatie-evaluaties; het beheren van leren en ontwikkeling (inclusief het benaderen van u om specifieke training voor te stellen); het geven van verwijzingen zoals gevraagd (indien toegestaan door het Bedrijfsbeleid); en het bieden van faciliteitenbeheer en beveiliging op de werkplek. Het Bedrijf kan voor deze doeleinden algemene gegevens, functie/tewerkstellingsomschrijving, organisatorische gegevens, identificatie- en authenticatiegegevens, gegevens over toegang of systeemgebruik, gegevens over achtergrond- of kredietcontroles, gegevens over visa en werkvergunningen, financiële gegevens en betalingsgegevens, gegevens over werkcontacten, contactinformatie voor noodgevallen, contractgegevens, prestatiegegevens, afwezigheidsgegevens, werkgerelateerde gegevens, geografische gegevens, kwalificatiegegevens, gegevens van derden, marktgegevens, klachtengegevens, reglementaire gegevens, onderzoeksgegevens en disciplinaire gegevens verwerken. We verwerken dergelijke gegevens omdat deze nodig zijn om een overeenkomst die we met u hebben uit te voeren; omdat we een specifiek legitiem belang hebben om deze gegevens te verwerken of als we onze legitieme belangen moeten nastreven; om te voldoen aan een legitieme verplichting; om onze legitieme rechten vast te stellen, te gebruiken en te verdedigen; of, indien van toepassing, omdat u deze informatie vrijwillig verstrekt en ons toestemming geeft om deze te verwerken.
- **Om te voldoen aan andere werkgerelateerde legitieme vereisten**, waaronder het bevestigen van iemands recht om te werken of flexibele thuiswerkregelingen, en het verifiëren van de identiteit voor beveiligingsdoeleinden, vergoedingsverlening en belastingberekeningen. Het Bedrijf kan voor deze doeleinden algemene gegevens, functie/tewerkstellingsomschrijving, organisatorische gegevens, identificatie- en authenticatiegegevens, gegevens over toegang of systeemgebruik, gegevens over werkcontacten, financiële gegevens en betalingsgegevens, contractgegevens, werkgerelateerde gegevens, prestatiegegevens, afwezigheidsgegevens, geografische gegevens, kwalificatiegegevens, gegevens van derden, gegevens over visa en werkvergunningen verwerken. We verwerken dergelijke gegevens omdat deze nodig zijn om een overeenkomst die we met u hebben uit te voeren; omdat we een specifiek legitiem belang hebben om deze gegevens te verwerken of als we onze legitieme belangen moeten nastreven; om te voldoen aan een legitieme verplichting; om onze legitieme rechten vast te stellen, te gebruiken en te verdedigen; of, indien van toepassing, omdat u deze informatie vrijwillig verstrekt en ons toestemming geeft om deze te verwerken.
- **Het bijhouden van een zakelijke adressenlijst en het mogelijk maken van personeelscommunicatie**, met inbegrip van het invullen en beschikbaar stellen van contactgegevens en/of een intranetwebsite (toegankelijk voor werknemers van het Bedrijf en geautoriseerde contingente hulpbronnen) om de communicatie met u of

het delen van informatie intern te verbeteren. Het Bedrijf kan voor deze doeleinden algemene gegevens, contactgegevens van het werk, functie/tewerkstellingsomschrijving, organisatorische gegevens en andere gegevens die u vrijwillig verstrekt, zoals foto's, verwerken. We verwerken dergelijke gegevens omdat we een specifiek legitiem belang hebben om ze te verwerken of als we onze legitieme belangen moeten nastreven.

- **Om de bedrijfsvoering te beheren en voor contractuele en procesgerelateerde doeleinden**, waaronder het inleiden of verdedigen van claims, uitvoering en service van contracten, het bijhouden van dossiers met betrekking tot bedrijfsactiviteiten, budgettering, financieel beheer en rapportage, bedrijfscontinuïteit, communicatie, beheer van fusies, overnames enz. Het Bedrijf kan voor deze doeleinden algemene gegevens, functie/tewerkstellingsomschrijving, werkcontactgegevens, organisatorische gegevens, contractgegevens, werkgerelateerde gegevens, gegevens van derden, toegangsgegevens of gegevens over systeemgebruik, gegevens over computergebruik (met inbegrip van het bedenken en uitvoeren van methodologieën zoals risicobeoordelingen), geografische gegevens, klachtgegevens, reglementaire gegevens, onderzoeksgegevens en disciplinaire gegevens en alle andere relevante gegevenstypen verwerken. We verwerken dergelijke gegevens omdat dergelijke gegevens nodig zijn om een overeenkomst die we met u hebben uit te voeren; omdat we een specifiek legitiem belang hebben om ze te verwerken of als we onze legitieme belangen moeten nastreven; om te voldoen aan een legitieme verplichting; of om onze legitieme rechten vast te stellen, te gebruiken en te verdedigen.
- **Om informatietechnologiesystemen ("IT") te onderhouden en voor eventuele analytische doeleinden**, waaronder het uitvoeren, onderhouden en gebruiken van IT- en communicatiesystemen; het verlenen van IT-ondersteuning en activabeheer; het onderhouden van plannen en processen voor bedrijfscontinuïteit en crisisbeheer; het beheren van beveiligingsdiensten en toegangsrechten van werknemers; het samenstellen van audittrails en andere rapportage-instrumenten; en het vaststellen van patronen, het vaststellen en uitvoeren van risicoclassificatie instrumenten bij het gebruik van technologische systemen en informatie die aan ons zijn toevertrouwd om mensen, activa en eigendommen van het Bedrijf te beschermen en om te voldoen aan alle reglementaire vereisten of eisen. Het Bedrijf kan voor deze doeleinden algemene gegevens, functie/tewerkstellingsomschrijving, werkcontactgegevens, organisatorische gegevens, contractgegevens, werkgerelateerde gegevens, toegangsgegevens of gegevens over systeemgebruik, gegevens over computergebruik (met inbegrip van het bedenken en uitvoeren van methodologieën zoals risicobeoordelingen), geografische gegevens, klachtgegevens, reglementaire gegevens, onderzoeksgegevens, disciplinaire gegevens en alle andere relevante gegevenstypen voor deze doeleinden verwerken.
- **Het verstrekken van prestatiecijfers** aan de Leverancier (als uw werkgever of agentschap), met inbegrip van de beoordeling van de kwaliteit en kwantiteit van de diensten die op basis van onze overeenkomst met de Leverancier worden verleend. Het Bedrijf kan voor deze doeleinden algemene gegevens, functie/tewerkstellingsomschrijving, werkcontactgegevens, organisatorische gegevens, contractgegevens, werkgerelateerde gegevens, identificatie- en authenticatiegegevens, toegangsgegevens of gegevens over systeemgebruik, gegevens over computergebruik (met inbegrip van het bedenken en uitvoeren van methodologieën zoals risicobeoordelingen), geografische gegevens, prestatiegegevens, klachtgegevens, reglementaire gegevens, onderzoeksgegevens en disciplinaire gegevens verwerken. We verwerken dergelijke gegevens omdat dergelijke gegevens nodig zijn om een overeenkomst die we met u hebben uit te voeren; omdat we een specifiek legitiem belang hebben om ze te verwerken of als we onze legitieme belangen moeten nastreven; om te voldoen aan een legitieme verplichting; of om onze legitieme rechten vast te stellen, te gebruiken en te verdedigen.
- **Om te bepalen of u geschikt bent om in dienst te worden genomen** op het moment dat de Leverancier u aanwijst om diensten aan Wells Fargo te verlenen waarvoor toegang tot het netwerk van Wells Fargo nodig is, of om te bepalen of u op de "Niet Opnieuw tewerk stellen" of "Niet Opnieuw in dienst nemen" lijsten van Wells Fargo staat. Het Bedrijf kan voor deze doeleinden algemene gegevens, functie/tewerkstellingsomschrijving, werkcontactgegevens, organisatorische gegevens, contractgegevens, werkgerelateerde gegevens, kwalificatiegegevens, gegevens van derden, identificatie- en

authenticatiegegevens, toegangsgegevens of gegevens over systeemgebruik, gegevens over computergebruik (met inbegrip van het bedenken en uitvoeren van methodologieën zoals risicobeoordelingen), geografische gegevens, prestatiegegevens, klachtengegevens, reglementaire gegevens, onderzoeksgegevens en disciplinaire gegevens als Gevoelige Persoonlijke Gegevens voor deze doeleinden.. We verwerken dergelijke gegevens omdat deze nodig zijn om een overeenkomst die we met u hebben uit te voeren; omdat we een specifiek legitiem belang hebben om deze gegevens te verwerken of als we onze legitieme belangen moeten nastreven; om te voldoen aan een legitieme verplichting; om onze legitieme rechten vast te stellen, te gebruiken en te verdedigen; of, indien van toepassing, omdat u deze informatie vrijwillig verstrekt en ons toestemming geeft om deze te verwerken.

- **Toezien op en verzekeren van naleving van Wells Fargo's Code of Ethics en Business Conduct, andere beleidslijnen en procedures, en toepasselijke wetgeving**, met inbegrip van bedrijfsbeleidslijnen en procedures met betrekking tot toezicht op telefoon, instant message, e-mail, video, internet en andere bedrijfsmiddelen, en andere toezichtactiviteiten zoals toegestaan door de lokale wetgeving; het voldoen aan legitieme en andere vereisten die van toepassing zijn op onze bedrijven in alle landen waar we actief zijn, zoals verplichtingen inzake het bijhouden van administratieve rapportage; het uitvoeren van audits; het uitvoeren van achtergrondcontroles het opsporen of voorkomen van mogelijk verlies of ongeoorloofde toegang tot of verwerking van gegevens van klanten, werknemers, vertrouwelijke of beperkte gegevens; het beschermen van gegevens en activa van het Bedrijf en andere partijen, het uitvoeren van interne onderzoeken, met inbegrip van het melden door werknemers van beschuldigingen van wanpraktijken van beleidschendingenschendingen, fraude of financiële rapportage; en het naleven van interne beleidslijnen en procedures; het afhandelen van mogelijke of andere claims; en het voeren van disciplinaire acties, grieven en beëindigingen; en indien Wells Fargo naar eigen goeddunken verneemt of vaststelt dat u een misdrijf hebt gepleegd waarbij diefstal, fraude of oneerlijkheid in het spel is, of een overtreding hebt begaan van de gedragscode of het informatiebeveiligingsbeleid van Wells Fargo, om uw Persoonsgegevens op de "Niet Opnieuw te werk stellen" of "Niet Opnieuw in dienst nemen" lijsten van Wells Fargo te plaatsen. Het Bedrijf kan algemene gegevens, functie/tewerkstellingsomschrijving, werkcontactgegevens, organisatorische gegevens, contractgegevens, werkgerelateerde gegevens, toegangsgegevens of gegevens over systeemgebruik, gegevens over computergebruik (inclusief het bedenken en uitvoeren van methodologieën zoals risicobeoordelingen), geografische gegevens, afwezigheidsgegevens, identificatie- en authenticatiegegevens, gegevens over achtergrond- of kredietcontroles, gegevens van derden, Gevoelige Persoonsgegevens, prestatiegegevens, klachtengegevens, reglementaire gegevens, onderzoeksgegevens, disciplinaire gegevens en alle andere relevante gegevens verwerken zoals nodig voor deze doeleinden. We verwerken dergelijke gegevens omdat we een specifiek legitiem belang hebben om ze te verwerken of als we onze legitieme belangen moeten nastreven; om te voldoen aan een legitieme verplichting; of om onze legitieme rechten vast te stellen, te gebruiken en te verdedigen.
- **Het reageren op verzoeken en legitieme eisen van rechtbanken, regelgevende instanties of andere autoriteiten**, inclusief het voldoen aan inspecties en andere verzoeken van regelgevende instanties of andere autoriteiten in uw eigen land of andere rechtsgebieden, zoals beslagleggingsbevelen, en het deelnemen aan en reageren op juridische procedures, met inbegrip van binnenlandse en grensoverschrijdende rechtszaken, dagvaardingen waarmee legitieme rechten en rechtsmiddelen worden nagestreefd, het verdedigen van rechtszaken, en het beheren van eventuele interne klachten of aanspraken en ontdekkingsprocedures (met inbegrip van juridische procedures die zich buiten uw rechtsgebied van verblijf kunnen voordoen). Het Bedrijf kan algemene gegevens, functie/tewerkstellingsomschrijving, werkcontactgegevens, organisatorische gegevens, contractgegevens, werkgerelateerde gegevens, toegangsgegevens of gegevens over systeemgebruik, gegevens over computergebruik (inclusief het bedenken en uitvoeren van methodologieën zoals risicobeoordelingen), geografische gegevens, afwezigheidsgegevens, identificatie- en authenticatiegegevens, gegevens over achtergrond- of kredietcontroles, gegevens van derden, Gevoelige Persoonsgegevens, prestatiegegevens, klachtengegevens, reglementaire gegevens, onderzoeksgegevens, disciplinaire gegevens en alle andere belangrijke gegevens verwerken zoals nodig voor deze doeleinden. We verwerken dergelijke gegevens omdat dergelijke gegevens nodig zijn om een overeenkomst die we met u hebben uit te voeren; omdat we een specifiek legitiem belang hebben om ze te verwerken of als we onze

legitieme belangen moeten nastreven; om te voldoen aan een legitieme verplichting; of om onze legitieme rechten vast te stellen, te gebruiken en te verdedigen.

- **Het reageren op noodsituaties, inclusief het contact opnemen met u of uw familie of contactpersonen in geval van nood**, bescherming van de gezondheid en zekerheid/beveiliging van werknemers en anderen, en bescherming van kantoorapparatuur, activa, faciliteiten en andere eigendommen. Het Bedrijf kan algemene gegevens, werkcontactgegevens, contactinformatie voor noodgevallen, organisatorische gegevens en andere gegevens die u vrijwillig verstrekt voor deze doeleinden verwerken. We verwerken dergelijke gegevens omdat we een specifiek legitiem belang hebben om ze te verwerken of als we onze legitieme belangen moeten nastreven.
- **Het uitvoeren van bepaalde beperkte activiteiten met betrekking tot Gevoelige Persoonsgegevens**, zoals vereist of toegestaan onder lokale wetgeving, zoals het berekenen van het aantal ziekte- of afwezigheidsdagen, het melden van bedrijfsongevallen, het voldoen aan verplichtingen om redelijke aanpassingen te doen voor eventuele handicaps of gezondheidsproblemen. Het Bedrijf kan voor deze doeleinden algemene gegevens en Gevoelige Persoonsgegevens verwerken. We verwerken dergelijke gegevens omdat we een specifiek legitiem belang hebben om ze te verwerken of als we onze legitieme belangen moeten nastreven; om te voldoen aan een legitieme verplichting; of, indien van toepassing, u deze informatie vrijwillig verstrekt en ons toestemming geeft om ze te verwerken.

3. Aan wie maken we Persoonsgegevens bekend?

Wells Fargo is wereldwijd actief en we kunnen Persoonsgegevens voor wervingsdoeleinden overdragen aan Wells Fargo-entiteiten buiten het VK, de EU en/of DIFC. Grensoverschrijdende overdrachten kunnen ook plaatsvinden wanneer we derden inschakelen om ons te helpen bij bepaalde activiteiten en werkzaamheden indien deze in verschillende landen zijn gevestigd, waaronder landen buiten het VK, de EU en het DIFC.

De landen waar wij actief zijn, zijn aangegeven op deze kaart www.wellsfargo.com/com/international/locations. Wij kunnen Persoonsgegevens ook doorgeven aan andere landen waar onze externe dienstverleners gevestigd zijn.

Openbaarmaking van en toegang tot Persoonsgegevens binnen het Bedrijf zal beperkt zijn tot diegenen die de informatie moeten kennen voor wervingsdoeleinden en zal bestaan uit uw managers en de door hen aangewezen personen, en personeel van HR, IT, Compliance, Legal, Finance en Accounting, en Internal Audit.

Al het personeel binnen het Bedrijf heeft over het algemeen toegang tot uw zakelijke contactgegevens zoals naam, functie, telefoonnummer, postadres en e-mailadres.

Het Bedrijf kan Persoonsgegevens voor doeleinden van de verbintenis overdragen aan de volgende ontvangers:

- **Wells Fargo U.S.** Omdat de verantwoordelijkheid voor management, human resources, legal en audit gedeeltelijk berust bij Wells Fargo & Company als de moedermaatschappij van de groep in de Verenigde Staten ("**Wells Fargo & Company**") en bij Wells Fargo Bank, N. A. activiteiten in de Verenigde Staten ("**Wells Fargo Bank, N.A.**") (gezamenlijk "**Wells Fargo U.S.**"), kan het Bedrijf Persoonsgegevens ter beschikking stellen aan, of anderszins toegang verlenen tot deze gegevens door, Wells Fargo U.S., die de gegevens kan verwerken voor de volgende doeleinden: het onderhouden en verbeteren van een effectieve administratie van het personeelsbestand; het onderhouden van een zakelijke adressenlijst; het onderhouden van IT-systemen; het controleren en waarborgen van de naleving van Wells Fargo's Ethische en Zakelijke Gedragscode, andere beleidslijnen en procedures, en toepasselijke wetgeving; en het reageren op verzoeken en legitieme eisen van regelgevende instanties andere autoriteiten, waaronder dergelijke autoriteiten in de Verenigde Staten. In bepaalde omstandigheden kan Wells Fargo & Company of Wells Fargo Bank, N.A. optreden als een onafhankelijke verwerkingsverantwoordelijke van uw Persoonsgegevens. Als u vragen hebt, kunt u contact opnemen met onze Regionale Functionaris Gegevensbescherming voor EMEA, via de contactgegevens in Sectie 10.

- **Gelieerde Entiteiten.** Voor zover de verantwoordelijkheid voor het management of human resources van uw verbintenis gedeeltelijk berust bij verschillende Gelieerde Entiteiten, kan het Bedrijf ook Persoonsgegevens ter beschikking stellen aan, of anderszins toegang verlenen tot, relevante Gelieerde Entiteiten, die de gegevens kunnen verwerken voor de volgende doeleinden het onderhouden en verbeteren van een effectieve administratie van het personeelsbestand; het onderhouden van een zakelijke adressenlijst; het onderhouden van IT-systemen; het controleren en verzekeren van de naleving van Wells Fargo's Ethische en Zakelijke Gedragscode, andere beleidslijnen en procedures, en toepasselijke wetten; en het reageren op verzoeken en legitieme eisen van regelgevende instanties en andere autoriteiten, met inbegrip van autoriteiten in de rechtsgebieden waar de Gelieerde Entiteiten zijn gevestigd. Als u vragen hebt, kunt u contact opnemen met onze EMEA Regionale Functionaris Gegevensbescherming via de contactgegevens in Sectie 10.
- **Klanten en prospecten.** Voor zover nodig en in verband met de doeleinden van de Verbintenis, kunnen Persoonsgegevens worden doorgegeven aan klanten en andere derden zoals toegestaan door de toepasselijke wetgeving.
- **Regelgevende instanties, publieke en overheidsinstanties.** Indien nodig en in verband met de hierboven beschreven doeleinden van de Verbintenis kunnen Persoonsgegevens worden doorgegeven aan regelgevende instanties; rechtbanken; andere autoriteiten (bijv. belasting- en wetshandhavingsautoriteiten), met inbegrip van autoriteiten buiten het land waar u woont.
- **Dienstverleners.** Voor zover nodig en in verband met de hierboven beschreven doeleinden van de Verbintenis kunnen Persoonsgegevens worden gedeeld met een of meer al dan niet gelieerde partijen om Persoonsgegevens te verwerken volgens passende instructies ("**Verwerkers**"). Deze Verwerkers kunnen instructies uitvoeren in verband met IT-systeemondersteuning, opleiding, naleving, toezicht en andere activiteiten, en zijn onderworpen aan contractuele verplichtingen om passende technische en organisatorische beveiligingsmaatregelen te nemen om Persoonsgegevens te beschermen en Persoonsgegevens alleen volgens de instructies te verwerken.
- **Professionele Adviseurs.** Deze categorie omvat accountants, bedrijfsrevisoren, advocaten, verzekeraars, bankiers en andere externe professionele adviseurs in alle landen waar wij actief zijn. Voor zover nodig en in verband met de hierboven beschreven Doeleinden van de Verbintenis kunnen Persoonsgegevens worden gedeeld met een of meer professionele adviseurs.

Overdracht van uw gegevens naar het buitenland: Het is mogelijk dat we uw gegevens op deze manier moeten overdragen voor verschillende doeleinden, zoals het uitvoeren van onze overeenkomst met u, om aan onze legitieme verplichting te voldoen, om het algemeen belang te beschermen en/of voor onze legitieme belangen. De ontvangers van Persoonsgegevens die in dit Sectie worden genoemd, kunnen zich in de Verenigde Staten en andere rechtsgebieden bevinden. Sommige van deze landen worden door de EU, het VK of het DIFC respectievelijk erkend als landen die volgens hun respectieve normen een passend beschermingsniveau bieden (de volledige lijst van deze volgens het EU-recht erkende landen is bijvoorbeeld beschikbaar op https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en). Met betrekking tot overdrachten vanuit de EU, het VK of het DIFC naar landen die door de relevante Gegevensbeschermingsautoriteit niet als adequaat worden beschouwd, hebben we waarborgen en adequate maatregelen getroffen om Persoonsgegevens te beschermen, zoals standaardcontractbepalingen die door de EU, het VK of het DIFC respectievelijk zijn vastgesteld. Voor een kopie van deze waarborgen en maatregelen kunt u contact opnemen met onze regionale privacyfunctionaris voor de EMEA via de contactgegevens in Sectie 10.

4. Van welke andere bronnen ontvangen we Persoonsgegevens?

Naast de Persoonsgegevens die wij direct of indirect van u ontvangen, kunnen wij uw Persoonsgegevens ook uit bepaalde andere bronnen ontvangen. Van onder anderen:

- Collega's;

- Beheerders;
- Voormalige werkgevers of scholen;
- Klanten;
- De Leverancier;
- Overheidsdatabanken;
- Kredietinformatiebureaus;
- Strafregisters; en
- Antecedentenonderzoekslieferanciers.

Voor specifieke functies met een hoog risico binnen Wells Fargo kunnen we een uitgebreid antecedentenonderzoek uitvoeren en deze functies zullen als zodanig worden aangeduid. Dit zal worden uitgevoerd tijdens de aanwerving en periodiek gedurende uw dienstverband, in overeenstemming met de beleidslijnen en de procedures van Wells Fargo.

5. Hoelang bewaren we Persoonsgegevens?

Wij bewaren Persoonsgegevens zo lang als nodig of toegestaan is in het licht van het doeleinde of de doeleinden waarvoor de gegevens zijn verkregen en in overeenstemming met de toepasselijke wetgeving. De criteria die worden gebruikt om onze bewaartermijnen te bepalen omvatten, maar zijn niet beperkt tot:

- De tijdsduur dat we een lopende verbintenis met u hebben;
- Of er een legitieme verplichting bestaat waaraan we zijn onderworpen (bepaalde wetten vereisen bijvoorbeeld dat we uw activiteiten gedurende een bepaalde periode na beëindiging van de verbintenis registreren);
- Of bewaring raadzaam is in het licht van onze juridische positie (zoals met betrekking tot toepasselijke verjaringstermijnen, rechtszaken of regelgevende onderzoeken); en/of
- Of het voor onze operationele behoeften noodzakelijk is uw Persoonsgegevens te bewaren (bijvoorbeeld voor de interne audit van de bankverrichtingen, het bijhouden van de voorkeuren voor verzoeken (ook voor voormalige klanten en niet-klanten), systeemadministratie, of voor fraudepreventie).

6. Welke beveiligingsmaatregelen passen we toe?

Het Bedrijf heeft passende technische, fysieke en organisatorische beveiligingsmaatregelen toegepast om voor de bescherming van Persoonsgegevens in overeenstemming met het Informatiebeveiligingsbeleidsnormen van Wells Fargo. Houd er rekening mee dat indien u als gevolg van uw verbintenis toegang hebt tot Persoonsgegevens van het Bedrijf of Persoonsgegevens van een van zijn controlerende of Gelieerde Entiteiten, zijn klanten en/of Verwerkers, of derden, u verplicht bent tot geheimhouding van die Persoonsgegevens. Bovendien is het niet toegestaan deze Persoonsgegevens met derden te delen zonder toestemming van het Bedrijf of de personen. Deze verplichting blijft ook bestaan na beëindiging van uw verbintenis met ons.

7. Wat zijn uw rechten met betrekking tot Persoonsgegevens?

Indien u wenst te verzoeken om toegang tot, correctie, bijwerking, terugname, beperking of verwijdering van uw Persoonsgegevens, om bezwaar te maken tegen of af te zien van de verwerking van uw Persoonsgegevens, of indien u wenst te verzoeken om een kopie van uw Persoonsgegevens te ontvangen voor overdracht aan een ander bedrijf (voor zover deze rechten u door de toepasselijke wetgeving worden verleend), kunt u contact opnemen met onze Regionale Functionaris Gegevensbescherming EMEA met de contactgegevens in Sectie 10. Wij zullen op uw verzoek reageren in overeenstemming met de toepasselijke wetgeving.

Naast onze in Sectie 10 genoemde Regionale Functionaris Gegevensbescherming EMEA heeft het Bedrijf een contactpersoon ("Contactpersoon") aangewezen om uw vragen en klachten te beantwoorden. De contactpersoon is

doorgaans de Manager Personeelszaken van het Bedrijf of, indien er geen Manager Personeelszaken is, de Filiaalmanager of de Landmanager voor die locatie.

U kunt ook een klacht indienen bij een Gegevensbescherming Autoriteit voor uw land of regio of in de plaats van het vermeende wangedrag. Contactinformatie voor de Gegevensbescherming Autoriteit vindt u door op onderstaande link(s) te klikken:

Verenigd Koninkrijk	Information Commissioner's Office (ICO)
Europese Unie	Onze leden Europees Comité voor gegevensbescherming (europa.eu)
DIFC	Gegevensbescherming DIFC

8. Onder welke omstandigheden worden apparatuur, elektronische communicatiesystemen en eigendommen aan monitoringonderworpen?

Voor zover toegestaan door de plaatselijke wetgeving, en onder voorbehoud van andere plaatselijke mededelingen of beleidslijnen, behoudt het Bedrijf zich het recht voor het gebruik van apparatuur, elektronische communicatiesystemen en eigendommen te controleren, met inbegrip van originele en reservekopieën van e-mail, instant messaging, sms, voicemail, internetgebruik, computergebruiksactiviteit, en CCTV. Voor meer informatie kunt u de Ethische en Zakelijke Gedragscode raadplegen (<https://portal.teamworks.wellsfargo.net/1/Ethics/Pages/COE.aspx>) en de verbintenis tussen het Bedrijf en het bedrijf waar u werkt of waarvoor u anders werkt.

Bovendien kan het Bedrijf dergelijke activiteiten uitvoeren om IT-toegang te beheren, IT-ondersteuning te verlenen, beveiligingsdiensten en toegangscontrole autorisaties te beheren, en om de naleving van Wells Fargo's Ethische en Zakelijke Gedragscode en andere beleidslijnen en procedures van het Bedrijf en disciplinaire of klachtenonderzoek te controleren en te verzekeren. Er wordt niet verwacht dat u geen privacy verwachten in verband met uw gebruik van apparatuur, systemen of eigendom. Zelfs als u wachtwoorden aanmaakt of toegang hebt tot wachtwoorden om u te beschermen tegen ongeoorloofde toegang tot correspondentie en activiteiten, maakt het gebruik van dat wachtwoord de daarmee verband houdende communicatie of activiteiten niet privé. Bovendien kunnen, voor zover toegestaan door de lokale wetgeving, telefoongesprekken die op een zakelijke telefoon worden gevoerd of ontvangen, worden gecontroleerd of opgenomen voor juridische, regelgevende en nalevingsdoeleinden en/of interne onderzoeken. Monitoring kan op afstand of lokaal worden uitgevoerd, en gerelateerde Persoonsgegevens kunnen worden verzameld en verwerkt door het Bedrijf, Wells Fargo & Company, Gelieerde Entiteiten, en/of Verwerkers met behulp van software, hardware of andere middelen. Persoonsgegevens die via monitoring zijn verkregen, kunnen worden doorgegeven aan regelgevende instanties en andere autoriteiten, alsmede aan de Raad van Bestuur van Wells Fargo & Company, en andere ontvangers voor zover noodzakelijk voor de hierboven beschreven doeleinden, met inbegrip van ontvangers in uw eigen land of andere rechtsgebieden. Persoonsgegevens die via toezicht zijn verkregen en die relevant zijn voor de hierboven beschreven Doeleinden van de Verbintenis, worden gedurende redelijke perioden bewaard om deze doeleinden te verwezenlijken, en behalve de rechten die niet-werknemers kunnen hebben op grond van de toepasselijke wetgeving.

Bij de monitoringop het gebruik van onze apparatuur of systemen past het Bedrijf passende maatregelen toe ter bescherming tegen misbruik van dergelijke Persoonsgegevens die in verband met deze controle worden verwerkt, zoals opleiding en toezicht op het personeel en periodieke herziening van procedures en programma's.

9. Hoe werken we deze Kennisgeving bij?

Wij kunnen delen van deze Kennisgeving wijzigen of bijwerken om wijzigingen in onze praktijken en/ ofwijzigingen in toepasselijke wet- en regelgeving weer te geven. Gelieve deze Kennisgeving van tijd tot tijd te controleren, zodat u op de hoogte bent van eventuele wijzigingen of updates ervan, die kunnen worden aangegeven door een wijziging van de ingangsdatum die aan het begin van de Kennisgeving is vermeld. Indien en wanneer vereist door de toepasselijke wetgeving, zullen we u op de hoogte brengen van elke wijziging of bijwerking met betrekking tot deze Kennisgeving door een individueel bericht of door de wijzigingen in de gegevensverwerking openbaar te maken op een beschikbaar medium.

10. Hoe neemt u contact op met een Regionale Functionaris Gegevensbescherming voor vragen?

Het Bedrijf heeft Regionale Functionarissen Gegevensbescherming die zich toeleggen op het beantwoorden van verzoeken in verband met uw Persoonsgegevens. Neem contact op met onze Regionale Functionaris Gegevensbescherming voor EMEA via de onderstaande contactgegevens:

EMEA Regional Privacy Officer
 Adres: 33 King William Street
 Londen, Verenigd Koninkrijk
 EC4R 9AT
 Telefoon: +44 (0) 203-942-8000
 Email: privacy.emea@wellsfargo.com

11. Welke Wells Fargo entiteiten zijn actief in Europa?

Een lijst van entiteiten die Wells Fargo in Europa exploiteert is hieronder te vinden:

Naam van Wells Fargo Entiteiten	Rechtsgebieden
<u>Wells Fargo Bank, National Association, London Branch</u>	Verenigd Koninkrijk
<u>Wells Fargo Securities International Limited</u>	Verenigd Koninkrijk
<u>Wells Capital Finance (UK) Limited</u>	Verenigd Koninkrijk
<u>Wells Fargo Bank International Unlimited Company</u>	Ierland
<u>Wells Fargo Bank International Unlimited Company, Frankfurt</u>	Duitsland
<u>Wells Fargo International Finance (France) S.A.S.</u>	Frankrijk
<u>Wells Fargo Securities Europe S.A.</u>	Frankrijk
<u>Wells Fargo Capital Finance, Amsterdam Branch</u>	Nederland
<u>Wells Fargo Capital Finance, Stockholm Branch</u>	Zweden
<u>Wells Fargo Bank, National Association, DIFC Branch</u>	Dubai, Verenigde Arabische Emiraten