ADP Privacy Code inzake Verwerken van Klantgegevens

ADP Privacy Code inzake Verwerken van Klantgegevens

Inleiding

ADP biedt haar klanten een brede reeks van HR en Payrolldiensten. ADP heeft zich verbonden tot het beschermen van Persoonsgegevens in de **ADP Code of Business Conduct and Ethics.**

Deze ADP Privacy Code inzake Verwerken van Klantgegevens bevat informatie over hoe deze is geïmplementeerd voor het verwerken door ADP van Persoonsgegevens van aan Werknemers van Klanten, in relatie tot het voorzien in Dienstverlening en Klantenservice. In dit raamwerk worden Klantgegevens verwerkt door ADP als Verwerker namens haar Klanten.

Voor de regels die gelden voor het Verwerken door ADP als Verwerkingsverantwoordelijke van Persoonsgegevens die toebehoren aan die Betrokkenen met wie ADP een zakelijke relatie heeft (bijv. Betrokkenen die de Klanten, Leveranciers en Zakelijke Partners van ADP vertegenwoordigen, andere professionals en consumenten) en andere Betrokkenen wiens Persoonsgegevens verwerkt worden door ADP in de context van haar bedrijfsactiviteiten als verwerkingsverantwoordelijke, zie de ***ADP Privacy Code*** voor Bedrijfsgegevens.

Artikel 1 - Reikwijdte, toepasselijkheid en implementatie

Reikwijdte - Toepasselijkheid op EER-gegevens

1.1 Deze Code bevat uitleg over het Verwerken van Persoonsgegevens van Werknemers van Klanten door ADP in haar capaciteit als Verwerker voor Klanten bij het leveren van Dienstverlening, waar dergelijke Persoonsgegevens (a) onderhevig zijn aan in de EER Toepasselijk Recht (of onderhevig waren aan in de EER Toepasselijk Recht voordat dergelijke Persoonsgegevens werden overdragen aan een Groepsmaatschappij buiten de EER in een land dat door bevoegde EER-instellingen niet geacht wordt een passend beschermingsniveau te bieden); en (b) verwerkt worden conform de Dienstverleningsovereenkomst die er specifiek in voorziet dat deze Code van toepassing is op dergelijke Persoonsgegevens.

Wanneer er een vraag rijst over de toepasselijkheid van deze Code, zal de desbetreffende Privacy Steward advies inwinnen van het Global Data Privacy and Governance-team voordat de Verwerking plaatsvindt.

Elektronisch Verwerken en Verwerken op papier

1.2 Deze Code is van toepassing op het elektronisch Verwerken van Klantgegevens door ADP en op het Verwerken in systematisch toegankelijke systemen voor archivering op papier.

Toepasselijkheid van lokale wetgeving

1.3 Niets in deze Code zal afbreuk doen aan enige rechten of rechtsmiddelen die Werknemers van Klanten kunnen inroepen onder Toepasselijk Recht. Daar waar Toepasselijk Recht meer bescherming biedt dan deze Code, gelden de relevante bepalingen van het Toepasselijk Recht. Daar waar deze Code meer

bescherming biedt dan het Toepasselijk Recht, of daar waar deze aanvullende waarborgen, rechten of rechtsmiddelen biedt aan Betrokkenen, geldt deze Code.

Beleid en richtlijnen **1.4** ADP kan deze Code aanvullen door middel van beleid, normen, richtlijnen en instructies die consistent zijn met deze Code.

Verantwoording **1.5** Deze Code is bindend voor ADP. De verantwoordelijke leidinggevenden zijn verantwoordelijk voor de naleving van deze Code door hun bedrijfsorganisaties. Personeel van ADP moet deze Code naleven.

Ingangsdatum **1.6** Deze Code is goedgekeurd door de General Counsel op voordracht van de Global Chief Privacy Officer en is vastgesteld door het ADP Executive Committee. Deze Code wordt van kracht op 11 april 2018 (**Ingangsdatum**). De Code (inclusief een lijst van de Groepsmaatschappijen die betrokken zijn bij het verwerken van Klantgegevens) wordt gepubliceerd op de website www.adp.com. Op verzoek wordt de Code ook aan Betrokkenen ter beschikking gesteld.

Deze Code wordt door de ADP-groep geïmplementeerd op basis van de tijdschema's als bepaald in artikel 16.

Voorafgaand beleid **1.7** Deze Code vult het privacybeleid van ADP aan en vervangt eerdere verklaringen voor zover deze in tegenspraak zijn met deze Code.

Rol van de Gedelegeerde Entiteit van ADP **1.8** Automatic Data Processing, Inc. heeft ADP Nederland BV, statutair gevestigd en kantoorhoudende te (2908 LG) CAPPELLE AAN DEN IJSSEL, aan de Lylantse Baan 1, Nederland, benoemd als Gedelegeerde Entiteit van ADP, belast met de handhaving van deze Code binnen de ADP-groep, en ADP Nederland BV heeft deze benoeming aanvaard.

Artikel 2 - Dienstverleningsovereenkomst

Dienstverlenings overeenkomst, Subverwerkers **2.1** ADP verwerkt Klantgegevens alleen op basis van een Dienstverleningsovereenkomst waarin de verplichte contractuele vereisten van de Verwerker staan conform Toepasselijk Recht van toepassing op de Verwerker en voor de specifieke Bedrijfsdoeleinden als vermeld in artikel 4.
De Contracterende Entiteit van ADP maakt gebruik van Subverwerkers, zowel ADP Subverwerkers als Derde-Subverwerkers, in de reguliere uitvoering van de Dienstverlening. De Dienstverleningsovereenkomsten van ADP geven toestemming voor het inzetten van dergelijke Subverwerkers, op voorwaarde

dat de Contracterende Entiteit van ADP verantwoordelijk blijft jegens de Klant voor de uitvoering door de Subverwerkers in overeenstemming met de voorwaarden in de Dienstverleningsovereenkomst. De voorwaarden in artikel 7 zijn van toepassing op het inzetten van Subverwerkers.

Beëindiging van de Dienstverlenings overeenkomst

2.2 Na beëindiging van de Dienstverlening voldoet ADP aan haar verplichtingen jegens de Klant als vermeld in de Dienstverleningsovereenkomst met betrekking tot het retourneren van de Klantgegevens, door aan de klant de Klantgegevens te overhandigen die nodig zijn voor de continuïteit van de bedrijfsactiviteiten van de klant (als de gegevens niet eerder overhandigd of toegankelijk gemaakt zijn voor de klant via relevante productfunctionaliteit, zoals de mogelijkheid de Klantgegevens te downloaden).

Als ADP aan haar verplichtingen uit de Dienstverleningsovereenkomst voldaan heeft, vernietigt ADP op veilige wijze de resterende kopieën van de Klantgegevens, en bevestigt (op verzoek van de Klant) aan de Klant dat dit gebeurd is. ADP kan een kopie van de Klantgegevens bewaren voor zover vereist onder Toepasselijk Recht, als geautoriseerd door de Klant, of als nodig voor het beslechten van geschillen. ADP verwerkt die Klantgegevens niet langer, behalve voor zover benodigd voor bovenvermelde doeleinden. De geheimhoudingsverplichtingen van ADP krachtens de desbetreffende Dienstverleningsovereenkomst blijven van kracht zolang ADP een kopie bewaart van dergelijke Klantgegevens.

Audit van beëindigingsmaat regelen

2.3 ADP zal, binnen 30 dagen na beëindiging van de Dienstverleningsovereenkomst (tenzij anderszins vereist wordt door een Privacytoezichthouder en op verzoek van de Klant of de bevoegde Privacytoezichthouder, toelaten dat haar verwerkingsfaciliteiten aan een audit worden onderworpen in overeenstemming met artikel 11.2 of 11.3 (al naar gelang het geval) om te controleren of ADP voldoet aan de aan beëindiging gerelateerde verplichtingen onder artikel 2.2.

Artikel 3 - Nalevingsverplichtingen

Instructies van de Klant

3.1 ADP verwerkt Klantgegevens namens de Klant, enkel in overeenstemming met de Dienstverleningsovereenkomst, conform alle gedocumenteerde instructies die zijn ontvangen van de Klant, of voor zover nodig, om te voldoen aan Toepasselijk Recht.

Naleving van Toepasselijk Recht

3.2 ADP verwerkt Klantgegevens in overeenstemming met Recht van toepassing op de Verwerker.

ADP reageert direct en passend op verzoeken om assistentie van de Klant, indien wettelijk verplicht en om de Klant in staat te stellen te voldoen aan zijn

verplichtingen onder aan Toepasselijk Recht voor Verwerkingsverantwoordelijken en in overeenstemming met de Dienstverleningsovereenkomst.

Niet-naleving, aanzienlijke nadelige gevolgen

3.3 Als een Groepsmaatschappij ontdekt dat Recht van toepassing op de Verwerker van een niet-EER-land, of een wijziging in de Recht van toepassing op de Verwerker van een niet-EER-land, of een instructie van de Klant, waarschijnlijk aanzienlijke nadelige gevolgen met zich meebrengt voor de mogelijkheden van ADP om te voldoen aan haar verplichtingen onder 31., 3.2 of 11.3, dan waarschuwt een dergelijke Groepsmaatschappij onmiddellijk de Contracterende Entiteit van ADP en de Klant hierover, in welk geval de Klant op basis van deze Code het recht heeft de relevante doorgifte naar ADP van Klantgegevens tijdelijk op te schorten, tot het moment waarop de Verwerking is aangepast en de niet-naleving is opgelost. In het geval dat een aanpassing niet mogelijk is, heeft de Klant het recht het betreffende deel van de Verwerking door ADP te beëindigen in overeenstemming met de voorwaarden in de Dienstverleningsovereenkomst. Deze rechten en verplichtingen gelden niet als de omstandigheden of wijziging in Recht van toepassing op de Verwerker voortvloeien uit Verplichte Vereisten.

Verzoek om verstrekken van Klantgegevens

3.4 Indien ADP van een wetshandhavingsinstantie, staatsveiligheidsorgaan of toezichthouder (gezamenlijk een 'Autoriteit') een verzoek ontvangt tot verstrekken van Klantgegevens, zal ADP vooraf, per geval, beoordelen of dit verzoek rechtsgeldig is en bindend voor ADP. Verzoeken die niet rechtsgeldig en bindend zijn voor ADP, zullen worden geweigerd in overeenstemming met Toepasselijk Recht.

Met inachtneming van het volgende lid, stelt ADP de Klant, de Leidende Privacytoezichthouder en de bevoegde Privacytoezichthouder conform artikel 11.3 onverwijld in kennis van dergelijke verzoeken van een Autoriteit die rechtsgeldig zijn en bindend voor ADP, en zal ADP de betreffende Autoriteit vragen dit verzoek voor een redelijke termijn aan te houden om de Leidende Privacytoezichthouder in staat te stellen om zich een mening te vormen over de geldigheid van het verzoek.

Als opschorting van de uitvoering en/of melding aan de Leidende Privacytoezichthouder van een wettelijk bindend verzoek verboden is, zoals in het geval van een strafrechtelijk verbod om de vertrouwelijkheid van een rechtshandhavingsonderzoek niet te schaden, zal ADP de Autoriteit verzoeken om opheffing van dit verbod en documenteren dat zij dit verzoek heeft gedaan. ADP verstrekt op jaarlijkse basis aan de Leidende Privacytoezichthouder de algemene informatie over het aantal en het soort kennisgevingsverzoeken dat zij in de voorafgaande 12 maanden van autoriteiten heeft ontvangen.

Dit artikel geldt niet voor verzoeken die worden ontvangen door ADP van

Autoriteiten in het normale verloop van haar activiteiten als verlener van HCM-diensten (zoals een gerechtelijk bevel tot loonbeslag), waaraan ADP kan blijven voldoen in overeenstemming met Toepasselijk Recht, de Dienstverleningsovereenkomst en de instructies van de Klant.

Klant vragen **3.5** ADP zal onmiddellijk en op gepaste wijze antwoorden op vragen van de Klant met betrekking tot het Verwerken van Klantgegevens conform de voorwaarden van de Dienstverleningsovereenkomst.

Artikel 4 - Doeleinden voor gegevensverwerking

Bedrijfsdoeleinde **4.1** ADP verwerkt Persoonsgegevens (met inbegrip van Bijzondere categorieën van Persoonsgegevens) die toebehoren aan Werknemers van Klanten voor zover nodig om Dienstverlening en Klantenservice te bieden en voor de volgende bijkomende doeleinden:

(a) Hosting, opslaan en andere vormen van Verwerking die nodig zijn voor de bedrijfscontinuïteit en herstel na rampen, inclusief het maken van back-ups en archiefkopieën van Persoonsgegevens;

(b) Beheer en beveiliging van systeem en netwerk, inclusief het monitoren van infrastructuur, beheer van identiteit en toegangsgegevens, verificatie en authenticatie en toegangscontrole;

(c) Monitoring en ander toezicht dat nodig is voor het waarborgen van veiligheid en integriteit van transacties (bijvoorbeeld financiële transacties en activiteiten met betrekking tot betaaldiensten), inclusief voor due diligence (zoals het verifiëren van de identiteit van de Betrokkene, en of de Betrokkene in aanmerking komt voor het ontvangen van producten of diensten (door bijvoorbeeld de status van het dienstverband of de account te verifiëren);

(d) Uitvoeren van overeenkomsten en bescherming van ADP, haar Medewerkers, Klanten, de Werknemers van Klanten en de samenleving tegen diefstal, aansprakelijkheid, fraude of misbruik, inclusief: (i) detecteren, onderzoeken, voorkomen en beperken van schade door daadwerkelijke en pogingen tot financiële fraude, identiteitsfraude en andere dreigingen jegens financiële en fysieke middelen, toegangsgegevens en informatiesystemen; (ii) deelname aan externe initiatieven op het gebied van cyberbeveiliging, anti-fraude- en anti-witwasinitiatieven; en (iii) als nodig om de vitale belangen van Betrokkenen te beschermen, zoals Betrokkenen waarschuwen voor een opgemerkte beveiligingsdreiging;

(e) Uitvoeren en beheren van interne bedrijfsprocessen van ADP die leiden tot de incidentele Verwerking van Klantgegevens voor:

(1) Interne audits en geconsolideerde rapportages;

(2) Naleving van wetgeving, inclusief het verplicht indienen, gebruiken en

verstrekken van informatie zoals op grond van Toepasselijk Recht wordt vereist;

(3) De-identificatie van gegevens en aggregatie van gede-identificeerde gegevens ten behoeve van gegevensminimalisering en analyses van diensten;

(4) Gebruik van gede-identificeerde en geaggregeerde gegevens, als door Klanten toegestaan, om het analyseren, continueren en verbeteren van de producten en diensten van ADP te faciliteren; en

(5) Faciliteren van goed ondernemingsbestuur, inclusief fusies, overnames, afstotingen en joint ventures.

Artikel 5 - Beveiligingsvereisten

Gegevensbeveiliging **5.1** ADP neemt commercieel redelijke en gepaste technische, fysieke en organisatorische maatregelen ter bescherming van om Klantgegevens tegen misbruik of onbedoeld(e), onrechtmatig(e) of ongeoorloofd(e) vernietiging, verlies, wijziging, vernietiging, verstrekking, verkrijging of toegang tijdens het Verwerken. Deze maatregelen voldoen aan de eisen van Toepasselijk EER-Recht, of eventueel strengere eisen, als opgelegd op grond van de Dienstverleningsovereenkomst. ADP neemt, in ieder geval, de maatregelen als omschreven in Bijlage 2 van deze Code, welke maatregelen door ADP kunnen worden aangepast, mits deze wijzigingen het beveiligingsniveau dat van toepassing is op Klantgegevens conform Bijlage 2 geboden wordt, niet wezenlijk verminderen.

Toegang tot en geheimhouding van gegevens **5.2** Personeel krijgt uitsluitend toegang tot Klantgegevens voor zover nodig voor de gegevensverwerkingsdoelen vermeld in artikel 4. ADP legt geheimhoudingsverplichtingen op aan Personeel dat toegang heeft tot Klantgegevens.

Melding Inbreuk op gegevensbescherming **5.3** ADP stelt de Klant zonder onnodige vertraging op de hoogte van een Inbreuk op Gegevensbescherming nadat hij een dergelijke inbreuk ontdekt heeft, tenzij een wetshandhaver of toezichthouder bepaalt dat melding een strafrechtelijk onderzoek zou kunnen belemmeren of de nationale veiligheid kan schaden, of kan leiden tot een schending van vertrouwen in de betreffende bedrijfstak. In dat geval wordt de melding opgeschort op last van de instructies deze wetshandhaver of toezichthouder. ADP reageert onverwijld op vragen van de Klant die betrekking hebben op de genoemde Inbreuk op de Gegevensbescherming.

Artikel 6 - Transparantie voor Werknemers van Klanten

Andere verzoeken van Werknemers van Klanten

6.1 ADP stelt de Klant direct op de hoogte van verzoeken of klachten met betrekking tot het Verwerken van Persoonsgegevens door ADP die rechtstreeks ontvangen worden van Werknemers van Klanten, zonder te reageren op dergelijke verzoeken of klachten, tenzij anderszins voorzien in de Dienstverleningsovereenkomst of geïnstrueerd door de Klant.

ADP zorgt dat, indien door de Klant geïnstrueerd om te reageren op verzoeken en klachten van Werknemers van de Klant onder de Dienstverleningsovereenkomst, Medewerkers van de Klant alle redelijk vereiste informatie ontvangen (zoals de contactpersoon en de procedure), zodat de Werknemer van de Klant efficiënt een verzoek of een klacht kan indienen.

De voorwaarden in dit artikel 6.1 gelden niet voor verzoeken die door ADP afgehandeld worden gedurende het normale verloop van het aanbieden van Dienstverlening en Klantenservice.

Artikel 7 – Subverwerkers

7.1

)vereenkomsten iet Derde-ubverwerkers

Derde-Subverwerkers mogen Klantgegevens uitsluitend Verwerken op grond van een Subverwerkersovereenkomst. In de Subverwerkersovereenkomst worden gegevensbeschermingsvoorwaarden opgelegd op aan de Derde-Subverwerker welke niet minder beschermend zijn dan de voorwaarden overeengekomen in de Dienstverleningsovereenkomst met de Contracterende Entiteit van ADP en deze Code.

7.2 ADP publiceert een overzicht van de categorieën Subverwerkers die betrokken zijn bij de uitvoering van de relevante Dienstverlening op de daarvoor bestemde internetpagina van ADP. Dit overzicht wordt in geval van wijzigingen direct bijgewerkt.

'ublicatie van 'verzicht van ubverwerkers

7.3 ADP bericht de Klant over nieuwe Subverwerkers die door ADP zijn ingeschakeld bij het verlenen van de Dienstverlening. Binnen 30 dagen na ontvangst van dit bericht kan de Klant bezwaar maken tegen een nieuwe Subverwerker door middel van een schriftelijk bericht aan ADP, met daarin objectieve, gerechtvaardigde gronden die betrekking hebben op het onvermogen van deze Subverwerker om de Klantgegevens te beschermen, in overeenstemming met de gerelateerde verplichtingen in de Subverwerkersovereenkomst, waarnaar verwezen wordt in artikel 7.1. Indien het de partijen niet lukt te komen tot een voor beiden aanvaardbare oplossing zal ADP, naar eigen keuze, de Subverwerker toegang

:ennisgeving van ieuwe ubverwerkers en et recht van ezwaar

tot de Klantgegevens ontzeggen, of de Klant de mogelijkheid geven de betreffende Dienstverlening te beëindigen in overeenstemming met de voorwaarden in de Dienstverleningsovereenkomst.

Uitzondering

7.4 De bepalingen van in dit artikel 7 zijn niet van toepassing voor zover de klant ADP instrueert om een Derde toe te staan Klantgegevens te Verwerken krachtens een overeenkomst die de Klant rechtstreeks met de Derde heeft (bijv. een derde uitkeringsaanbieder).

Artikel 8 - Toezicht en naleving

Global Chief Privacy Officer

8.1 De ADP-groep heeft een Global Chief Privacy Officer die verantwoordelijk is voor het:

(a) voorzitterschap van de Privacy Leadership Council,

(b) Toezicht houden op de naleving van deze Code,

(c) begeleiden, coördineren, informeren en raadplegen van de relevante leden van het Privacynetwerk inzake privacy- en gegevensbeschermingskwesties,

(d) verstrekken van jaarlijkse privacyrapporten over gegevensbeschermingsrisico's en nalevingskwesties aan het ADP Executive Committee,

(e) Coördineren van officiële onderzoeken of naar of vragen over het Verwerken van Klantgegevens door een overheidsinstantie, in samenwerking met de relevante leden van het Privacynetwerk en de juridische afdeling van ADP;

(f) Behandelen van conflicten tussen deze Code en het Toepasselijk Recht,

(g) Toezicht houden op het proces waarbij Privacy Impact Assessments (Privacy-effectbeoordelingen, PIA's) worden uitgevoerd en PIA's worden geëvalueerd waar nodig;

(h) Controleren van de documentatie, kennisgeving en communicatie van Inbreuken op de Gegevensbescherming,

(i) Adviseren over de processen, systemen en hulpmiddelen voor gegevensbeheer om het kader voor privacy- en gegevensbeschermingsbeheer te implementeren, zoals vastgesteld door de Privacy Leadership Council, waaronder:

(1) Bijhouden, bijwerken en publiceren van deze Code en aanverwant beleid en normen,

(2) Adviseren over de tools om inventarisaties te maken, te onderhouden en bij te werken met informatie over de structuur en het functioneren van alle systemen die Klantgegevens Verwerken;

(3) Het bieden van, assisteren bij of adviseren over de privacytraining voor het Personeel, zodat zij hun verantwoordelijkheden onder deze Code begrijpen en naleven;

(4) Coördineren met de afdeling interne audits van ADP en anderen om een passend assurance programma te ontwikkelen en te onderhouden om de naleving van deze Code te bewaken, te controleren en te rapporteren, en om ADP in staat te stellen deze naleving waar nodig te verifiëren en te certificeren,

(5) Procedures implementeren waar nodig om vragen en zorgen over privacy en gegevensbescherming te behandelen; en

(6) Adviseren over passende sancties voor overtredingen van deze Code (bijvoorbeeld disciplinaire maatregelen).

Privacynetwerk **8.2** ADP zal een Privacynetwerk opzetten, waarmee naleving van deze Code binnen de internationale ADP-organisatie geregeld kan worden.

Het Privacynetwerk zal een kader creëren en onderhouden ter ondersteuning van de Global Chief Privacy Officer en toezicht houden op de taken die worden uiteengezet in artikel 8.1 en andere taken om deze Code te handhaven en bij te werken, indien nodig. De leden van het Privacynetwerk vervullen, voor zover relevant voor hun rol in de regio of organisatie, de volgende aanvullende taken:

(a) Toezicht houden op de implementatie van de verwerkingsprocessen, -systemen en -hulpmiddelen die het mogelijk maken dat de Groepsmaatschappijen de Code kunnen naleven in hun respectieve regio's of organisaties,

(b) Ondersteuning en beoordeling van het algehele privacy- en gegevensbeschermingsbeheer en de naleving door de Groepsmaatschappijen binnen hun regio's,

(c) Regelmatig adviseren van hun Privacy Stewards en de Global Chief Privacy Officer over regionale of lokale privacyrisico's en nalevingskwesties;

(d) Controleren of geschikte inventarisaties worden gemaakt van de systemen die Klantgegevens verwerken;

(e) Beschikbaar zijn om te reageren op verzoeken om privacygoedkeuringen of -advies,

(f) Verstrekken van informatie die de Global Chief Privacy Officer nodig heeft om het jaarlijkse privacyrapport in te vullen,

(g) De Global Chief Privacy Officer assisteren bij van officiële onderzoeken of vragen van overheidsinstanties,

(h) Ontwikkelen en publiceren van privacybeleid en -normen die geschikt zijn voor hun regio's of organisaties,

(i) Groepsmaatschappijen adviseren over het bewaren en vernietigen van gegevens,

(j) De Global Chief Privacy Officer op de hoogte stellen van klachten en helpen bij het oplossen van deze klachten; en

(k) Assisteren van de Global Chief Privacy Officer, andere leden van het Privacynetwerk, Privacy Stewards en anderen bij het:

(1) Faciliteren van de bedrijven of organisaties van de groep om te voldoen aan de Code, met behulp van de instructies, hulpmiddelen en trainingen die zijn ontwikkeld,

(2) Delen van best practices voor privacy- en gegevensbeschermingsbeheer binnen de regio,

(3) Bevestigen dat er rekening wordt gehouden met privacy- en gegevensbeschermingsvereisten wanneer nieuwe producten en diensten worden geïmplementeerd in de bedrijven of organisaties van de groep; en

(4) Ondersteunen van de Privacy Stewards, Groepsmaatschappijen, business units, functionele gebieden en inkooppersoneel bij het gebruik van Subverwerkers.

Privacy Stewards **8.3** Privacy Stewards zijn executives van ADP die door een Verantwoordelijke Leidinggevende en/of ADP's executive management benoemd zijn voor het implementeren en uitvoeren van de Code binnen een business unit of functioneel gebied van ADP. Privacy Stewards zijn verantwoordelijk voor de effectieve implementatie van de Code binnen de relevante business unit of het functionele gebied. In het bijzonder moeten Privacy Stewards controleren of effectieve beheersmaatregelen voor privacy en gegevensbescherming zijn geïntegreerd in alle bedrijfspraktijken die van invloed zijn op Klantgegevens en of er voldoende middelen en budget beschikbaar zijn om aan de verplichtingen van deze Code te voldoen. Privacy Stewards kunnen taken delegeren en zullen waar nodig passende middelen toewijzen om hun verantwoordelijkheden te vervullen en nalevingsdoelstellingen te bereiken.

De verantwoordelijkheden van Privacy Stewards omvatten:

(a) Toezicht houden op het algehele privacy- en gegevensbeschermingsbeheer en de naleving binnen hun Groepsmaatschappij, business unit of functioneel gebied en controleren of

alle processen, systemen en hulpmiddelen die door het Global Data Privacy and Governance Team zijn ontwikkeld, effectief zijn geïmplementeerd;

(b) Vaststellen dat privacy- en gegevensbeschermingsbeheer en nalevingstaken op de juiste wijze worden gedelegeerd met de normale gang van zaken, evenals tijdens en na organisatorische herstructurering, outsourcing, fusies en overnames en desinvesteringen;

(c) Samenwerken met de Global Chief Privacy Officer en de betreffende leden van het Privacynetwerk om eventuele nieuwe wettelijke vereisten te begrijpen en behandelen en controleren of de privacy- en gegevensbeschermingsbeheerprocessen zijn bijgewerkt om te reageren op veranderende omstandigheden en wettelijke en regelgevende vereisten;

(d) In overleg treden met de Global Chief Privacy Officer en de betreffende leden van het Privacynetwerk in alle gevallen waarin er een daadwerkelijk of potentieel conflict is tussen het Toepasselijk Recht en deze Code;

(e) Controleren van Subverwerkers die door de Groepsmaatschappij, de business unit of het functioneel gebied worden gebruikt om te zorgen voor voortdurende naleving van deze Code en de Subverwerkersovereenkomsten door de Subverwerkers;

(f) Vaststellen dat het Personeel van de Groepsmaatschappij, de business unit of het functioneel gebied de vereiste privacytrainingen hebben voltooid en

(g) Regelen dat opgeslagen Klantgegevens worden verwijderd, vernietigd, ge-deidentificeerd of doorgegeven zoals vereist door Artikel 2.2.

Verantwoordelijke *executives* **8.4** De verantwoordelijke executives, als hoofden van business units of functionele gebieden, zijn ervoor verantwoordelijk dat effectief privacy- en gegevensbeschermingsbeheer wordt geïmplementeerd in hun organisaties. Elke Verantwoordelijke Leidinggevende moet (a) geschikte Privacy Stewards benoemen, (b) ervoor zorgen dat voldoende middelen en budget beschikbaar zijn voor naleving en (c) ondersteuning bieden aan de Privacy Steward voor zover nodig om nalevingsproblemen aan te pakken en risico's te beheersen.

Privacy Leadership Council **8.5** De Global Chief Privacy Officer geeft leiding aan een Privacy Leadership Council, die bestaat uit de Privacy Stewards, leden van het Privacynetwerk die geselecteerd zijn door de Global Chief Privacy Officer, en anderen die nodig kunnen zijn bij de ondersteuning van de missie van de Council. De Privacy Leadership Council creëert en onderhoudt een raamwerk ter ondersteuning van de taken die passend kunnen zijn voor de Groepsmaatschappijen, business units of functionele gebieden om aan deze Code te voldoen, om de hierin beschreven taken uit te voeren en om de Global Chief Privacy Officer te ondersteunen.

Standaard Privacynetwerk-leden en Privacy Stewards

8.6 Als er op enig moment geen Global Chief Privacy Officer is aangesteld of in staat is om de functies te vervullen die aan de rol zijn toegewezen, zal de General Counsel iemand aanstellen om op te treden als interim-Global Chief Privacy Officer. Indien er op enig moment geen lid van het Privacynetwerk is aangewezen voor een bepaalde regio of organisatie, zal de Global Chief Privacy Officer de taken van een dergelijk lid van het Privacynetwerk uitvoeren zoals uiteengezet in Artikel 8.2.

Indien er op enig moment geen Privacy Steward is aangewezen voor een Groepsmaatschappij, een business unit of een functioneel gebied, benoemt de Verantwoordelijke Leidinggevende een geschikte persoon om de taken uit te voeren zoals uiteengezet in artikel 8.3.

Statutaire functies

8.7 Wanneer leden van het Privacynetwerk, bijvoorbeeld gegevensbeschermingsfunctionarissen onder Toepasselijk Recht van de EER, hun posities krachtens de wet bekleden, zullen zij hun functieverantwoordelijkheden uitoefenen voor zover die niet in strijd zijn met hun statutaire functie.

Artikel 9 - Beleid en procedures

Beleid en procedures

9.1 ADP zal beleid, normen, richtlijnen en procedures ontwikkelen en implementeren om aan deze Code te voldoen.

Systeeminformatie

9.2 ADP zal direct beschikbare informatie bijhouden met betrekking tot de structuur en het functioneren van alle systemen en processen die Klantgegevens verwerken, zoals inventarisaties van systemen en processen die van invloed zijn op Klantgegevens, samen met informatie die is gegenereerd tijdens DPIA. Een kopie van deze informatie zal op verzoek worden verstrekt aan de Leidende Privacytoezichthouder of aan een Privacytoezichthouder die bevoegd is voor de klant overeenkomstig Artikel 11.3.

Artikel 10 – Training

Training

10.1 ADP geeft al het Personeel met toegang tot Klantgegevens of verantwoordelijkheden gekoppeld aan het Verwerken van Klantgegevens training inzake de verplichtingen en principes die vermeld zijn in deze Code, en andere privacy- en gegevensbeveiligingsverplichtingen.

Artikel 11 - Toezicht en controle op naleving

Interne audits

11.1 ADP controleert op regelmatige basis bedrijfsprocessen en -procedures die betrekking hebben op het Verwerken van Klantgegevens op naleving van deze Code. In het bijzonder:

(a) De audits kunnen worden uitgevoerd in het kader van de reguliere activiteiten van de afdeling ADP Internal Audit (zoals door het gebruik van onafhankelijke derden), andere interne teams die zich bezighouden met assurancetaken en op ad-hocbasis op verzoek van de Global Chief Privacy Officer;

(b) De Global Chief Privacy Officer kan ook verzoeken om een controle uitgevoerd door een externe auditor en zal de Verantwoordelijke Leidinggevende van de relevante business unit en / of het Executive Committee van ADP waar nodig op de hoogte brengen,

(c) De toepasselijke professionele normen voor onafhankelijkheid, integriteit en vertrouwelijkheid worden tijdens het auditproces in acht genomen,

(d) De Global Chief Privacy Officer en het relevante lid van het Privacynetwerk worden op de hoogte gebracht van de resultaten van de audits,

(e) Voor zover de controle aantoont dat deze Code niet wordt nageleefd, zullen deze bevindingen worden gerapporteerd aan de toepasselijke Privacy Stewards en verantwoordelijke executives. De Privacy Stewards werken samen met het Global Data Privacy and Governance-team om een passend herstelplan te ontwikkelen en uit te voeren,

(f) Een kopie van de auditresultaten met betrekking tot de naleving van deze Code zal op verzoek aan de Leidende Privacytoezichthouder of een Privacytoezichthouder die bevoegd is onder artikel 11.3 worden verstrekt.

Audit door Klant

11.2 ADP reageert op auditverzoeken van de Klant als vermeld in dit artikel 11.2. ADP beantwoordt vragen die gesteld worden door de Klant betreffende het Verwerken van Klantgegevens door ADP. In het geval dat de klant redelijkerwijs van mening is dat de antwoorden van ADP verdere analyse rechtvaardigen voert ADP, in overeenstemming met de klant, een van volgende handelingen uit:

(a) De faciliteiten die hij gebruikt voor het Verwerken van Klantgegevens beschikbaar stellen voor een audit door een gekwalificeerde onafhankelijke derde beoordelaar die acceptabel is voor ADP en gebonden is aan geheimhoudingsverplichtingen waarmee ADP akkoord kan gaan, en aangesteld is door de Klant. De Klant verstrekt een kopie van het auditrapport aan de Global Chief Privacy Officer dat behandeld wordt als vertrouwelijke informatie van ADP. Audits mogen niet meer dan eens per jaar, per Klant, uitgevoerd worden, gedurende de looptijd van de Dienstverleningsovereenkomst, gedurende normale kantooruren, en dienen te voldoen aan de volgende vereisten (i) een schriftelijk verzoek

ingediend bij ADP ten minste 45 dagen voor de voorgestelde auditdatum; (ii) een gedetailleerd schriftelijk auditplan dat gecontroleerd en goedgekeurd is door de beveiligingsorganisatie van ADP; en (iii) de beveiligingsmaatregelen die op locatie voor ADP gelden. Dergelijke audits vinden alleen plaats in de aanwezigheid van een vertegenwoordiger van het Global Security Office van ADP, ADP's Global Privacy and Governance-team, of een dergelijke persoon die door de passende vertegenwoordiger is aangewezen. De audits mogen de verwerkingsactiviteiten van ADP niet hinderen en de beveiliging en vertrouwelijkheid van Persoonsgegevens die toebehoren aan andere klanten van ADP niet in gevaar brengen; of

(b) ADP verstrekt een verklaring aan de Klant die is afgegeven door een gekwalificeerde onafhankelijke derde beoordelaar waarin verklaard wordt dat de bedrijfsprocessen en -procedures van ADP waar het Verwerken van Klantgegevens onderdeel van zijn, voldoen aan deze Code.

ADP kan Klanten een redelijk tarief in rekening brengen voor een dergelijke audit.

Dit Artikel 11.2 is een aanvulling op of verduidelijking van de auditrechten die Klanten onder Toepasselijk Recht en de Dienstverleningsovereenkomsten kunnen hebben. In geval van tegenstrijdigheid, prevaleren de bepalingen van Toepasselijk Recht en de Dienstverleningsovereenkomst.

Audits door Privacytoezicht-houders

11.3 Iedere Privacytoezichthouder van een EER-land met de bevoegdheid een audit uit te voeren bij een Klant van ADP heeft toestemming de relevante doorgifte te controleren op naleving van deze Code, onder dezelfde voorwaarden als die zouden gelden voor een audit door de Privacytoezichthouder van de Klant zelf onder Recht van toepassing op de Verwerkingsverantwoordelijke.

Om een dergelijke audit mogelijk te maken:

(a) Werken ADP en de Klant in goed vertrouwen samen om te proberen het verzoek op te lossen door informatie te verstrekken aan de Privacytoezichthouder, zoals auditrapporten van ADP, en maken gesprekken mogelijk tussen de Privacytoezichthouder en de experts van de Klant en ADP, die de beveiligings-, privacy- en operationele maatregelen kunnen herzien die getroffen zijn. De klant heeft toegang tot zijn Klantgegevens in overeenstemming met de Dienstverleningsovereenkomst, en kan dergelijke toegang delegeren aan vertegenwoordigers van de Privacytoezichthouder;

(b) Als de informatie die beschikbaar is via deze middelen onvoldoende is om de vermelde doelstellingen van de Privacytoezichthouder te verwezenlijken,

biedt ADP de Privacytoezichthouder de mogelijkheid te overleggen met de auditor van ADP;

(c) Als dit onvoldoende blijkt, biedt ADP de Privacytoezichthouder na voldoende voorafgaande melding een direct recht ADP's gegevensfaciliteiten te onderzoeken die gebruikt worden voor het verwerken van Klantgegevens, gedurende kantooruren, en met volledig respect van de vertrouwelijkheid van de verkregen informatie en de handelsgeheimen van ADP. de Privacytoezichthouder heeft alleen toegang tot de Klantgegevens die toebehoren aan de klant.

Dit Artikel 11.3 is een aanvulling op of verduidelijking van de auditrechten die Privacytoezichthouders onder Toepasselijk Recht en Dienstverleningsovereenkomsten kunnen hebben. In geval van tegenstrijdigheid prevaleren de bepalingen van het Toepasselijk Recht.

Jaarlijks verslag **11.4** De Global Chief Privacy Officer stelt een jaarlijks verslag op voor het Executive Committee over de naleving van deze Code, privacy, gegevensbeschermingsrisico's en andere relevante kwesties. Dit rapport weerspiegelt de informatie die wordt verstrekt door het Privacynetwerk en anderen met betrekking tot lokale ontwikkelingen en specifieke problemen binnen Groepsmaatschappijen.

Mitigatie **11.5** ADP neemt passende maatregelen om eventuele gevallen van niet-naleving van deze Code te mitigeren die tijdens nalevingscontroles zijn vastgesteld.

Artikel 12 - Juridische kwesties

Rechten van Werknemers van Klanten **12.1** Als ADP de Code overtreedt met betrekking tot Persoonsgegevens van een Werknemer van de Klant die gedekt is onder deze Code, , dan kan een dergelijke Werknemer van de Klant als derde begunstigde artikel 1.5, 1.6, 2.1, 2.2, 3, 5, 6, 7.1, 7.3, 7.4, 11.2, 11.3, 12.1, 12.2, 12.3, 12.5, 12.7, 12.8 en 14.3 van deze Code afdwingen bij de Contracterende Entiteit van ADP.

In de mate waarin de Werknemer van de Klant dergelijke rechten kan uitoefenen jegens de Contracterende Entiteit van ADP, mag de Contracterende Entiteit van ADP haar verplichtingen niet ontlopen door een overtreding van een Subverwerker aan te voeren, met uitzondering van de situatie waarin een verweer van de Subverwerker ook een verweer voor ADP is. ADP mag echter verweren of rechten gebruiken die ook voor de Klant beschikbaar zouden zijn. ADP mag ook verweren aanwenden die ADP zou hebben kunnen aanwenden tegen de Klant (zoals eigen schuld of nalatigheid), in verweer op de betrokken vordering van de Betrokkene.

Klachten-procedure

12.2 Werknemers van Klanten mogen bij het Global Data Privacy and Governance-team via de post of e-mail op het adres dat aan het eind van deze Code vermeld is, een schriftelijke klacht indienen met betrekking tot een vordering die ze hebben onder artikel 12.1. De Werknemer van de Klant mag ook een klacht of vordering indienen bij de autoriteiten of de rechter in overeenstemming met artikel 12.3 van deze Code.

Het Global Data Privacy and Governance Team is verantwoordelijk voor klachtenafhandeling. Elke klacht zal worden toegewezen aan een bevoegd personeelslid (hetzij binnen het Global Data Privacy and Governance-team of binnen de toepasselijke business unit of het functionele gebied). Dit personeelslid moet:

(a) Zo snel mogelijk de ontvangst van de klacht bevestigen,

(b) De klacht analyseren en zo nodig een onderzoek starten,

(c) Als de klacht gegrond is, de toepasselijke Privacy Steward en het relevante lid van het Privacynetwerk adviseren, zodat een herstelplan kan worden ontwikkeld en uitgevoerd, en

(d) De gegevens van alle ontvangen klachten, de antwoorden en door ADP genomen corrigerende maatregelen bijhouden en opslaan.

ADP zal redelijke inspanningen leveren om klachten zonder onnodige vertraging op te lossen, dusdanig dat de Werknemer van de Klant antwoord krijgt binnen vier weken na de datum waarop de klacht werd ingediend. Het antwoord is schriftelijk en wordt naar de Werknemer van de Klant verzonden op de manier waarop de Werknemer van de Klant oorspronkelijk contact heeft opgenomen met ADP (*bijvoorbeeld* per post of e-mail). Het antwoord geeft een overzicht van de stappen die ADP heeft genomen om de klacht te onderzoeken en geeft de beslissing van ADP weer met betrekking tot welke stappen er (eventueel) genomen zullen worden als gevolg van de klacht.

In het geval dat ADP haar onderzoek en reactie niet binnen vier weken redelijkerwijs kan voltooien, zal het de Werknemer van de Klant binnen vier weken informeren dat het onderzoek gaande is en dat een antwoord zal worden gegeven binnen de komende acht weken.

Als de reactie van ADP op de klacht onbevredigend is voor de Werknemer van de Klant (bijv. het verzoek is afgewezen) of als ADP zich niet houdt aan de voorwaarden in de klachtenprocedure als vermeld in dit artikel 12.2, dan kan de Werknemer van de Klant een klacht of vordering indienen bij de Leidende Privacytoezichthouder of de rechter in overeenstemming met artikel 12.3.

Geschillen met Werknemers van

12.3 Werknemers van Klanten worden aangemoedigd om eerst de klachtenprocedure zoals uiteengezet in Artikel 12.2 van deze Code te volgen

Klanten

voordat ze een klacht of vordering indienen bij de autoriteiten of de rechter.

Werknemers van Klanten kunnen, naar eigen keuze, vorderingen indienen op grond van artikel 12.1 door een klacht in te dienen bij
(i) de Privacytoezichthouder in het land van zijn/haar reguliere woonplaats, werkgever of plaats waar de inbreuk zich heeft voorgedaan, tegen de Contracterende Entiteit van ADP of de Gedelegeerde Entiteit van ADP; of
(ii) de Leidende Privacytoezichthouder of de rechter in Nederland, maar in dat geval alleen tegen de Gedelegeerde Entiteit van ADP.

Werknemers van Klanten kunnen, naar eigen keuze, vorderingen indienen onder artikel 12.1 door een klacht in te dienen bij:
(i) de rechter in het land van zijn/haar reguliere woonplaats of het land van oorsprong van de gegevensdoorgifte onder deze Code, tegen de Contracterende Entiteit van ADP of de Gedelegeerde Entiteit van ADP; of
(ii) de Leidende Privacytoezichthouder of de rechter in Nederland, maar in dat geval alleen tegen de Gedelegeerde Entiteit van ADP.

De Privacytoezichthouders en rechters passen hun eigen inhoudelijke en procedurele recht op de geschillen toe. De keuze gemaakt door de Werknemer van de Klant doet geen afbreuk aan de materiële of procedurele rechten die de partijen hebben onder het Toepasselijk Recht.

Rechten van Klanten

12.4 De Klant kan de uitvoering van deze Code afdwingen van (i) de Contracterende Entiteit van ADP of, (ii) de Gedelegeerde Entiteit van ADP bij de Leidende Privacytoezichthouder of de rechtbanken in Nederland, maar alleen als de Contracterende Entiteit van ADP niet gevestigd is in een EER-land. De Gedelegeerde Entiteit van ADP zorgt ervoor dat passende maatregelen worden genomen om overtredingen van deze Code door een Contracterende Entiteit van ADP of een ander Groepsmaatschappij aan te pakken.

De Contracterende Entiteit van ADP en de Gedelegeerde Entiteit van ADP mogen hun verantwoordelijkheid niet ontlopen door een overtreding van hun verplichtingen door een ander bedrijf in de groep of een Subverwerker aan te voeren, met uitzondering van de mate waarin een verweer van een dergelijk Groepsmaatschappij of Subverwerker ook een verweer inhoudt van ADP.

Beschikbare rechtsmiddelen, bewijslast voor Werknemers van Klanten

12.5 In het geval dat een Werknemer van een Klant een vordering heeft op grond van artikel 12.1, heeft de Werknemer van de Klant recht op compensatie van schade in de mate waarin wordt voorzien in toepasbare EER-wetgeving.

In het geval dat een Werknemer van de Klant een vordering tot schadevergoeding indient op grond van Artikel 12.1, moet de Werknemer van de Klant aantonen dat hij schade heeft geleden en feiten vaststellen waaruit blijkt dat het aannemelijk is dat de schade is ontstaan door een schending van deze

Code. Vervolgens heeft de Contracterende Entiteit van ADP (of de Gedelegeerde Entiteit van ADP, als van toepassing) de bewijslast dat de geleden schade door de Werknemer van de Klant die veroorzaakt is door een schending van deze Code niet toe te schrijven is aan het relevante Groepsmaatschappij of een Subverwerker, of hij kan andere toepasselijke verweren gebruiken.

Compensatie van de klant

12.6 In geval van schending van deze Code, en onderhevig aan de voorwaarden in de Dienstverleningsovereenkomst, hebben Klanten het recht op compensatie van directe schade, in overeenstemming met de voorwaarden in de Dienstverleningsovereenkomst.

Wederzijdse ondersteuning

12.7 De Groepsmaatschappijen zullen, als nodig, samenwerken en helpen in de mate die redelijkerwijs mogelijk is bij het (a) afhandelen van een verzoek, klacht of vordering ingediend door een Klant of een Werknemer van een Klant of (b) gehoor geven aan een rechtmatig onderzoek of verzoek door een competente overheidsinstantie.

De Groepsmaatschappij die een verzoek om informatie ontvangt conform artikel 6.1 of een klacht of vordering conform artikel 12.2 of 12.3, heeft de verantwoordelijkheid de communicatie met de klant of de Werknemer van de Klant af te handelen betreffende het verzoek of de vordering, met uitzondering van waar omstandigheden anders voorschrijven, of als op aanwijzingen van het Global Data Privacy en Governance-team.

Advies van Privacy toezichthouder en bindende besluiten

12.8 ADP zal te goeder trouw samenwerken met en alle redelijke inspanningen leveren om het advies van de Leidende Privacytoezichthouder en de bevoegde Privacytoezichthouder te volgen op grond van artikel 12.3 met betrekking tot de interpretatie en toepassing van deze Code. ADP houdt zich aan bindende beslissingen van de bevoegde Privacytoezichthouders.

Recht dat van toepassing is op deze Code

12.9 Deze Code wordt beheerst door en geïnterpreteerd in overeenstemming met Nederlands recht.

Artikel 13 - Maatregelen bij niet-naleving

Niet-naleving

13.1 Niet-naleving van deze Code door Personeel kan leiden tot passende disciplinaire of contractuele maatregelen in overeenstemming met het Toepasselijk Recht en het ADP-beleid, tot en met beëindiging van de arbeidsrelatie.

Artikel 14 - Conflicten tussen deze Code en het Recht van toepassing op de

Verwerkingsverantwoordelijke

Conflict tussen deze Code en wetgeving

14.1 Waar er een conflict is tussen Toepasselijk Recht en deze Code, zal de Verantwoordelijke Leidinggevende of de Privacy Steward in overleg treden met de Global Chief Privacy Officer, het relevante lid van het Privacynetwerk (indien van toepassing), en de juridische afdeling van de business unit om te bepalen hoe deze Code moet worden nageleefd en om het conflict op te lossen voor zover redelijkerwijs haalbaar gezien de wettelijke vereisten die van toepassing zijn op ADP.

Nieuwe tegenstrijdige wettelijke vereisten

14.2 De leden van de juridische afdeling, ADP Business Security Officers en Privacy Stewards informeren onmiddellijk het Global Data Privacy and Governance Team over nieuwe wettelijke eisen waarvan zij op de hoogte zijn en die mogelijk interfereren met de naleving door ADP van deze Code.

De betreffende Privacy Stewards zullen, in overleg met de juridische afdeling, de Verantwoordelijke Leidinggevende onmiddellijk op de hoogte brengen van elke nieuw wettelijk vereiste die het vermogen van ADP om aan deze Code te voldoen zou kunnen verstoren.

Rapportage aan Leidende Privacytoezichthouder

14.3 Als ADP ontdekt dat Recht van toepassing op de Verwerker of een wijziging in Recht van toepassing op de Verwerker waarschijnlijk een aanzienlijk negatieve invloed heeft op de mogelijkheid van ADP om te voldoen aan haar verplichtingen onder 3.1, 3.2 of 11.3, dan meldt ADP dit bij de Leidende Privacytoezichthouder.

Artikel 15 - Wijzigingen in deze Code

Goedkeuring voor wijzigingen

15.1 Alle materiele wijzigingen in deze Code vereisen de voorafgaande goedkeuring van de Global Chief Privacy Officer en de General Counsel, evenals de goedkeuring door het Executive Committee en zullen worden meegedeeld aan de Groepsmaatschappijen. Niet-materiële wijzigingen aan de Code kunnen gedaan worden na voorafgaande goedkeuring van de Global Chief Privacy Officer. De Gedelegeerde Entiteit van ADP stelt de Leidende Privacytoezichthouder jaarlijks op de hoogte van wijzigingen in deze Code.
Waar een wijziging in deze Code een aanzienlijke invloed heeft op de verwerkingsvoorwaarden van de Dienstverlening, informeert ADP de Leidende Privacytoezichthouder daarover onmiddellijk, inclusief een korte uitleg van dergelijke wijziging. Daarnaast meldt zij een dergelijke wijziging aan de Klant. De Klant mag binnen 30 dagen na ontvangst van dergelijke melding bezwaar maken tegen dergelijke wijziging door middel van een schriftelijke melding aan ADP. In het geval dat de partijen geen wederzijds acceptabele oplossing kunnen bereiken, voert ADP in plaats daarvan een alternatieve oplossing in voor doorgifte van gegevens. Als er geen alternatieve gegevensverwerkingsoplossing ingevoerd kan worden, heeft de klant onder deze Code het recht de relevante doorgifte aan ADP van Klantgegevens op te schorten. In het geval een opschorting van de gegevensdoorgifte niet mogelijk is, stelt ADP de klant in staat de relevante Dienstverlening te beëindigen in overeenstemming met de voorwaarden van de Dienstverleningsovereenkomst.

Ingangsdatum van wijzigingen

15.2 Elke wijziging wordt met onmiddellijke ingang van kracht nadat deze is goedgekeurd in overeenstemming met Artikel 15.1 en wordt gepubliceerd op de website www.adp.com en gecommuniceerd aan Klanten.

Vorige versies

15.3 Elke aanvraag, klacht of vordering van een Werknemer van de Klant met betrekking tot deze Code zal worden beoordeeld aan de hand van de versie van deze Code zoals die van kracht is op het moment dat het verzoek, de klacht of de vordering wordt ingediend.

Artikel 16 - Implementatie- en overgangsperioden

Implementatie

16.1 De implementatie van deze Code zal worden begeleid door de Privacy Stewards, met de hulp van het Global Data Privacy and Governance Team. Behalve zoals hieronder vermeld, wordt er een overgangsperiode van achttien maanden aangehouden vanaf de ingangsdatum (zoals beschreven in artikel 1.6) voor de naleving van deze Code.

Dienovereenkomstig, tenzij anders vermeld, worden binnen achttien maanden na de Ingangsdatum alle verwerkingen van Klantgegevens uitgevoerd in overeenstemming met deze Code en wordt de Code volledig van kracht.

Gedurende de overgangsperiode zal de Code van kracht worden voor een Groepsmaatschappij, zodra die betreffende Groepsmaatschappij de taken voltooit die nodig zijn voor volledige implementatie en die Groepsmaatschappij de Global Chief Privacy Officer de nodige kennisgeving heeft gedaan.

Nieuwe groepsmaatschappijen

16.2 Elke entiteit die na de ingangsdatum Groepsmaatschappij wordt, moet binnen twee jaar nadat het een Groepsmaatschappij is geworden aan deze Code voldoen.

Afgestoten ondernemingen

16.3 Een afgestoten onderneming kan na deze afstoting gedekt blijven door deze Code gedurende de periode die ADP nodig heeft om het Verwerken van Klantgegevens in verband met die afgestoten onderneming te ontvlechten.

Overgangsperiode voor bestaande overeenkomsten

16.4 Indien er bestaande overeenkomsten zijn met Subverwerkers of andere derden die worden beïnvloed door deze Code, prevaleren de bepalingen van die overeenkomsten totdat de overeenkomsten zijn vernieuwd in de normale gang van zaken, op voorwaarde echter dat al deze bestaande overeenkomsten binnen achttien maanden na de ingangsdatum in overeenstemming moeten zijn met deze Code.

Contactgegevens

ADP Global Data Privacy and Governance-team:
privacy@adp.com

Gedelegeerde Entiteit van ADP
ADP Nederland B.V.
Lylantse Baan 12908 LG CAPELLE AAN DEN IJSSEL
NEDERLAND

Interpretaties

INTERPRETATIE VAN DEZE Code:

(i) Tenzij de context anders vereist, zijn alle verwijzingen naar een bepaald artikel of een bijlage verwijzingen naar dat artikel of deze bijlage in of bij dit document, zoals ze van tijd tot tijd kunnen worden gewijzigd,

(ii) Kopteksten zijn alleen voor het gemak opgenomen en dienen niet te worden gebruikt voor interpretatie van enige bepaling van deze Code,

(iii) Als een woord of zin wordt gedefinieerd, hebben de andere grammaticale vormen een overeenkomstige betekenis,

(iv) De mannelijke vorm omvat ook de vrouwelijke vorm,

(v) De woorden "bevat", "waaronder, "zoals," en alle volgende woorden moeten worden opgevat zonder beperking van de algemeenheid van voorgaande woorden of concepten en vice versa;

(vi) Het woord "schriftelijk" omvat alle gedocumenteerde communicatie, schrijven, overeenkomsten, elektronische registraties, elektronische handtekeningen, faxberichten of andere geldige en geldig uitvoerbare bescheiden, ongeacht de vorm,

(vii) Een verwijzing naar een document (inclusief, zonder beperking, een verwijzing naar deze Code) is naar het document in gewijzigde, gevarieerde, aangevulde of vervangen vorm, behalve voor zover door deze Code of dit verwezen document niet toegestaan en

(viii) Een verwijzing naar wetgeving omvat alle wettelijke vereisten, sectorale aanbevelingen en best practices die zijn uitgegeven door relevante nationale en internationale Privacytoezichthouder en of andere instanties.

BIJLAGE 1 - BCR-definities

Adequaatheidsbesluit	ADEQUAATHEIDSBESLUIT betekent een beslissing door een College Bescherming Persoonsgegevens of een ander bevoegd orgaan, dat een land, een regio of een ontvanger van een gegevensoverdracht voorschrijft een passend niveau aan bescherming te bieden voor de Persoonsgegevens. Entiteiten die gedekt zijn door een Adequaatheidsbesluit zijn ontvangers die zich bevinden in landen die door Toepasselijk recht gezien worden als aanbieder van een passend niveau aan gegevensbescherming en ontvangers die gebonden zijn aan een ander instrument (zoals een reeks Binding Corporate Rules) die zijn goedgekeurd door het juiste College Bescherming Persoonsgegevens of een ander bevoegd orgaan. Met betrekking tot de Verenigde Staten zijn bedrijven die gecertificeerd zijn volgens een privacyraamwerk van de Verenigde Staten en de Europese Economische Ruimte en/of de Verenigde Staten en Zwitserland gedekt door een Adequaatheidsbesluit.
ADP (ADP-groep)	ADP (de ADP-GROEP) betekent, gezamenlijk, Automatic Data Processing, Inc. (de moedermaatschappij) en de ondernemingen van de groep, inclusief ADP, Inc.
ADP Subverwerker	In het kader van de Privacy Code inzake Verwerken van Klantgegevens, wordt onder een ADP SUBVERWERKER bedoeld een Groepsmaatschappij die door een andere Groepsmaatschappij als Subverwerker van Klantgegevens optreedt.
Afgeleid doeleinde	Afgeleid doeleinde betekent een doel anders dan het originele doel waarvoor Persoonsgegevens verder verwerkt worden.
Afgestoten Onderneming	AFGESTOTEN ONDERNEMING betekent een onderneming van de groep die niet langer in eigendom is van ADP als gevolg van de verkoop van aandelen en/of activa/passiva-transactie, of een andere afstoting, waardoor het bedrijf niet langer gekwalificeerd wordt als onderneming van de ADP.
Archief	Archief betekent een verzameling Persoonsgegevens die niet langer nodig is voor het doel waarvoor de Gegevens oorspronkelijk werden verzameld, of die niet langer wordt gebruikt voor algemene bedrijfsactiviteiten, maar uitsluitend nog voor historische, wetenschappelijke of statistische doelen, geschillenbeslechting, onderzoeken of algemene archiveringsdoeleinden wordt gebruikt. Toegang tot een Archief is beperkt tot systeembeheerders en anderen met een

	functie die uitdrukkelijk toegang tot het Archief vereist. De toegang tot een archief is beperkt tot systeembeheerders en anderen wiens functie specifiek toegang tot het archief vereist.
Automatic Data Processing, Inc.	AUTOMATIC DATA PROCESSING, INC. is de moedermaatschappij van de ADP-groep, naar het recht van Delaware (VS), met het hoofdkantoor op One ADP Boulevard, Roseland, New Jersey, 07068-1728, Verenigde Staten.
Bedrijfscontactgegevens	Bedrijfscontactgegevens betekent alle gegevens van een Professional, die gewoonlijk op een visitekaartje of in een e-mailhandtekening te vinden zijn.
Bedrijfsdoeleinde	BEDRIJFSDOELEINDE betekent een legitiem doel voor het Verwerken van Persoonsgegevens als bepaald in artikel 2, 3 of 4 van de Codes of voor het Verwerken van Bijzondere Categorieën van Gegevens als bepaald in artikel 4 van de Codes.
Betrokkene	BETROKKENE betekent een geïdentificeerd of te identificeren natuurlijk persoon wiens Persoonsgegevens worden verwerkt door ADP als Verwerkingsverantwoordelijke of als verwerkingsverantwoordelijke, met uitzondering van Co-Employed Betrokkenen. OPMERKING: de ADP Privacy Code voor Zakelijke Gegevens en de Privacy Code voor ADP Medewerkers zijn daarom niet van toepassing op het verwerken van Persoonsgegevens van Co-Employed Betrokkenen.
Bijzonder categorieën van Persoonsgegevens	Bijzondere Categorieën van Persoonsgegevens betekent Persoonsgegevens waaruit, met betrekking tot deze Betrokkene, informatie blijkt over zijn of haar ras of etnische afkomst, politieke opvattingen of lidmaatschap van een politieke partij of vergelijkbare organisatie, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een beroeps- of handelsorganisatie of vakbond, lichamelijke of geestelijke gezondheid inclusief het oordeel daarover, handicaps, genetische Code, verslavingen, seksueel gedrag, strafbare feiten, strafblad of procedures in verband met strafbaar of onrechtmatig gedrag.
Binding Corporate Rules	Binding Corporate Rules (BCR) betekent het privacybeleid van een groep gerelateerde bedrijven dat geacht wordt een voldoende beschermingsniveau te bieden voor de doorgifte van Persoonsgegevens binnen die groep bedrijven conform Toepasselijk Recht.
Code	Code betekent (als van toepassing) de ADP Privacy Code

	voor Bedrijfsgegevens, de Privacy Code voor ADP Medewerkers (voor intern gebruik door ADP) en de ADP Privacy Code inzake Verwerken van Klantgegevens; gezamenlijk te noemen de Codes.
Co-Employement-medewerker	CO-EMPLOYEMENT-MEDEWERKER betekent een medewerker van een Amerikaanse Klant die co-employed is bij een Amerikaanse indirecte gelieerde onderneming van Automatic Data Processing, Inc. als onderdeel van de professional employer organization dienstverlening die wordt aangeboden in de VS.
Consument	CONSUMENT betekent een Betrokkene die rechtstreeks contact heeft met ADP voor persoonlijke doeleinden. Het betreft bijvoorbeeld Betrokkenen die deelnemen aan talentontwikkelingsprogramma's of producten en diensten van ADP voor persoonlijk gebruik aanschaffen (*dat wil zeggen* buiten een arbeidsrelatie met ADP of een klant van ADP).
Contracterende Entiteit van ADP	Contracterende Entiteit van ADP betekent de Groepsmaatschappij die een overeenkomst is aangegaan die vereist is onder de Codes, zoals een dienstverleningsovereenkomst, Subverwerkersovereenkomst of overeenkomst inzake doorgifte van gegevens.
Data Protection Impact Assessment (DPIA)	Data Protection Impact Assessment (DPIA)betekent een procedure tot het uitvoeren en documenteren van een voorafgaande beoordeling van het effect dat een bepaalde Verwerken kan hebben op de bescherming van Persoonsgegevens, waar dergelijke bescherming waarschijnlijk zal leiden tot een hoger risico voor de rechten en vrijheden van Betrokkenen, in het bijzonder waar nieuwe technologieën gebruikt worden. Een DPIA moet het volgende bevatten:

	(i) een beschrijving van: (a) de omvang en context van het Verwerken; (b) de bedrijfsdoeleinden waarvoor de Persoonsgegevens verwerkt worden; (c) de specifieke doelen waarvoor Bijzondere Categorieën van gegevens verwerkt worden; (d) categorieën ontvangers van Persoonsgegevens, inclusief ontvangers die niet vallen onder een Adequaatheidsbesluit; (e) bewaartermijnen van Persoonsgegevens; (ii) een beoordeling van: (a) de noodzaak en evenredigheid van het Verwerken; (b) de risico's voor de privacyrechten van Betrokkenen; en de getroffen maatregelen om deze risico's te minimaliseren, inclusief beveiligingen, beveiligingsmaatregelen en andere mechanismen (zoals privacy-by-design) om de bescherming van Persoonsgegevens te garanderen.
Derde	Derde betekent een persoon, particuliere organisatie of overheidsinstantie, niet zijnde een Groepsmaatschappij.
Derde-Subverwerker	DERDE-SUBVERWERKER betekent een Derde die door ADP is ingeschakeld als Subverwerker.
Dienstverlening	Dienstverlening betekent de dienstverlening voor HR gerelateerde zaken geleverd door ADP aan klanten, zoals werving, salarisadministratie, secundaire arbeidsvoorwaarden, talentmanagement, HR-administratie, consultancy en analyses en pensioendiensten).
Dienstverleningsovereenkomst	Dienstverleningsovereenkomst betekent een overeenkomst of voorwaarden conform welke ADP diensten levert aan een Klant.
EER beperking op Gegevensdoorgifte	EER-Beperking op Gegevensdoorgifte betekent een beperking van de grensoverschrijdende doorgifte van Persoonsgegevens op grond van de Privacywetgeving van een EER-land.
EER of Europese Economische Ruimte	EER of EUROPESE ECONOMISCHE RUIMTE betekent alle Lidstaten van de Europese Unie, plus Noorwegen, IJsland en Liechtenstein en, in het kader van de Codes, Zwitserland en het Verenigd Koninkrijk na het verlaten van de Europese Unie.

	Bij besluit van de General Counsel – zoals wordt gepubliceerd op www.adp.com kan dit andere landen omvatten met Privacywetgeving die Beperkingen op Gegevensdoorgifte kennen die vergelijkbaar zijn met de Beperkingen op Gegevensdoorgifte van de EER.
EER Toepasselijk Recht	EER TOEPASSELIJK RECHT betekent de vereisten onder de toepasselijke wetten van de EER, die van toepassing zijn op Persoonsgegevens die origineel verzameld zijn in de context van de activiteiten van een Groepsmaatschappij dat gevestigd is in de EER (ook nadat ze doorgegeven zijn naar een ander Groepsmaatschappij die zich buiten de EER bevindt).
Executive Committee	ADP UITVOEREND COMITÉ betekent het comité van bestuurders bestaande uit (i) de Chief Executive Officer (CEO) van Automatic Data Processing, Inc. en (ii) de andere bestuurders die direct rapporteren aan de CEO en die, gezamenlijk, de verantwoordelijkheid hebben voor de groepsactiviteiten van ADP.
Externe Verwerker	Externe Verwerker betekent een externe partij die Persoonsgegevens verwerkt namens ADP die niet onder directe autoriteit van ADP valt.
Externe Verwerkingsverantwoor-delijke	Externe Verwerkingsverantwoordelijke betekent een externe partij die Persoonsgegevens verwerkt en doel en middelen van het Verwerken bepaalt.
Gedelegeerde entiteit van ADP	GEDELEGEERDE ENTITEIT VAN ADP betekent ADP Nederland, B.V., statutair gevestigd en kantoorhoudende te 2908 LG CAPELLE AAN DEN IJSSEL, aan de Lylantse Baan 1.
General Counsel	GENERAL COUNSEL betekent de General Counsel van Automatic Data Processing, Inc.
Global Chief Privacy Officer	GLOBAL CHIEF PRIVACY OFFICER betekent de medewerker van ADP die deze functie uitvoert bij Automatic Data Processing, Inc.
Global Data Privacy and Governance Team	GLOBAL DATA PRIVACY AND GOVERNANCE TEAM betekent het Office of Privacy and Data Governance van ADP. Het Office of Privacy and Data Governance wordt geleid door de Chief Privacy Officer en bestaat uit privacy officers, privacy managers en ander Personeel dat rapporteert aan de Global Chief Privacy Officer of de privacy officers en privacy managers.
Groepsmaatschappij	Groepsmaatschappij betekent een rechtspersoon die is aangesloten bij Automatic Data Processing, Inc. en/of ADP, Inc., waarbij Automatic Data Processing, Inc. of ADP, Inc.

	direct of indirect eigenaar is van meer dan 50% van het geplaatste aandelenkapitaal, minimaal 50% van de stemrechten heeft tijdens algemene aandeelhoudersvergaderingen, bevoegd is tot het benoemen van een meerderheid van de bestuurders, of de activiteiten van deze rechtspersoon anderszins aanstuurt.
Hoger belang	HOGER BELANG betekent de urgente belangen als bepaald in artikel 13.1 van de Privacy Code ADP Medewerkers en de Privacy Code voor Bedrijfsgegevens op basis waarvan de verplichtingen van ADP of de rechten van Betrokkenen als bepaald in artikel 13.2 en 13.3 van de codes, onder speciale omstandigheden, overschreven kunnen worden als dit urgente belang zwaarder weegt dan de belangen van de Betrokkene.
Inbreuk op gegevensbescherming	INBREUK OP GEGEVENSBESCHERMING betekent een incident dat gevolgen heeft voor de vertrouwelijkheid, integriteit of beschikbaarheid van Persoonsgegevens, zoals ongeoorloofd(e) gebruik of verstrekken van Persoonsgegevens, of ongeoorloofde toegang tot Persoonsgegevens, dat of die afbreuk doet aan de privacy of bescherming van de Persoonsgegevens
Ingangsdatum	INGANGSDATUM betekent de datum waarop de Codes van kracht worden, als bepaald in artikel 1 van de Codes.
Interne Verwerker	INTERNE VERWERKER betekent een Groepsmaatschappij die Persoonsgegevens namens een andere Groepsmaatschappij verwerkt als verwerkingsverantwoordelijke.
Kinderen	In het kader van gegevensverzameling en marketing door ADP, wordt onder KINDEREN verstaan Betrokkenen onder de leeftijd die in Toepasselijk Recht wordt aangeduid als bevoegd tot het geven van toestemming voor dergelijke gegevensverzameling en/of marketing
Klant	KLANT betekent een Derde die één of meer producten of diensten van ADP afneemt ten behoeve van het voeren van een onderneming.
Klantenservice	KLANTENSERVICE betekent de verwerkingsactiviteiten die worden ondernomen door ADP om de levering van producten en diensten te ondersteunen. Klantenservice kan het volgende omvatten: het trainen van professionals, het reageren op vragen over diensten, het openen en oplossen van support tickets, het bieden van product- en service-

	informatie (inclusief updates en compliance alerts), kwaliteitscontrole en -bewaking en gerelateerde activiteiten die het effectieve gebruik van de producten en diensten van ADP faciliteren.
Klantgegevens	KLANTGEGEVENS betekent Persoonsgegevens die betrekking hebben op Werknemers van de Klant (inclusief toekomstige werknemers, voormalige werknemers en van werknemers afhankelijke gezinsleden) en die door ADP worden Verwerkt in verband met de Dienstverlening
Leidende Privacytoezichthouder	LEIDENDE TOEZICHTHOUDER betekent de Nederlandse Autoriteit Persoonsgegevens.
Leverancier	LEVERANCIER betekent een externe partij die goederen of diensten levert aan ADP (bijv. als serviceleverancier, agent, Verwerkingsverantwoordelijke, consultant of verkoper).
Medewerker	MEDEWERKER betekent een Sollicitant, een huidige ADP-werknemer of een voormalig ADP-werknemer, met uitzondering van Co-Employed Betrokkenen. OPMERKING: de Privacy Code voor ADP Medewerkers is daarom niet van toepassing op het verwerken van Persoonsgegevens van Co-Employed Betrokkenen. OPMERKING: de Privacy Code voor ADP Medewerkers is daarom niet van toepassing op het verwerken van Persoonsgegevens van Co-Employed Betrokkenen.
Personeel	PERSONEEL medewerkers die in dienst zijn van ADP alsmede de Tijdelijk Medewerkers die werkzaam zijn voor ADP.
Persoonsgegevens of Gegevens	Persoonsgegevens OF GEGEVENS betekent informatie over een geïdentificeerde of identificeerbare Betrokkene. Persoonsgegevens kunnen ook worden aangeduid als ‘persoonlijke informatie in beleid of normen die de Codes nader uitwerken.
Privacy Leadership Counsel	PRIVACY LEADERSHIP COUNCEL betekent de raad die geleid wordt door de Global Chief Privacy Officer en bestaat uit de Privacy Stewards, leden van het Privacynetwerk die geselecteerd zijn door de Global Chief Privacy Officer, en anderen die nodig kunnen zijn bij de ondersteuning van de missie van de Counsel.
Privacy Steward	PRIVACY STEWARD betekent een executive van ADP die door een Verantwoordelijke Leidinggevende en/of ADP's executive management benoemd is voor het implementeren

	en uitvoeren van de Codes binnen een business unit van ADP.
Privacynetwerk	PRIVACYNETWERK betekent de leden van het Global Data Privacy and Governance-team en andere leden van de Juridische afdeling, inclusief compliance professionals en data protection officers die verantwoordelijk zijn voor privacy naleving binnen hun respectievelijke regio, land, business unit of functioneel gebied.
Privacytoezichthouder	PRIVACYTOEZICHTHOUDER betekent elke regelgevende of Privacytoezichthouder die toezicht houdt op gegevensbescherming of privacy in een land waarin een onderneming van ADP is gevestigd.
Professional	PROFESSIONAL betekent een persoon (anders dan een werknemer) die direct contact heeft met ADP in professionele of zakelijke capaciteit. Onder professionals valt bijvoorbeeld HR-Personeel van een klant dat contact heeft met ADP als gebruiker van de producten of diensten van ADP. Onder Professionals vallen ook klanten, leveranciers en vertegenwoordigers van een Zakelijke Partner, zakelijke contacten, contacten van handelsassociaties, regelgevers, mediacontacten en andere Betrokkenen die in commerciële capaciteit omgang hebben met ADP.
Recht van toepassing op de Verwerkingsverantwoordelijke	In het kader van de Privacy Code inzake Verwerken van Klantgegevens, wordt onder RECHT VAN TOEPASSING OP DE VERWERKINGSVERANTWOORDELIJKE verstaan alle wet- en regelgeving op het gebied van privacy- en gegevensbescherming die van toepassing is op een Klant van ADP als Verwerkingsverantwoordelijke van deze Klantgegevens.
Recht van toepassing op de Verwerker	In het kader van de Privacy Code inzake Verwerken van Klantgegevens, wordt onder RECHT VAN TOEPASSING OP DE VERWERKER verstaan alle wet- en regelgeving op het gebied van privacy- en gegevensbescherming die van toepassing is op ADP als Verwerker, namens een Klant die de Verwerkingsverantwoordelijke is.
Sollicitant	SOLLICITANT betekent een Betrokkene die Persoonsgegevens verstrekt aan ADP in de context van het solliciteren naar een baan als medewerker van ADP.
Subverwerkers	betekent gezamenlijk, de Subverwerkers van ADP en Derde-Subverwerkers.
Subverwerkersovereenkomst	SUBVERWERKERSOVEREENKOMST betekent een

	schriftelijke of elektronische overeenkomst tussen ADP en een Derde Subverwerker conform artikel 7.1 van de Privacy Code inzake Verwerken van Klantgegevens.
Tijdelijke Medewerker	TIJDELIJKE MEDEWERKER betekent een Betrokkene die diensten verleent aan ADP (en die onderhevig is aan directe supervisie door ADP) op tijdelijke of niet-permanente basis, zoals uitzendkrachten, ZZP'ers, gedetacheerden of consultants.
Toepasselijk Recht	TOEPASSELIJK RECHT betekent wet- en regelgeving op het gebied van privacy of gegevensbescherming die van toepassing is op specifieke Verwerkingen.
Van werknemers afhankelijke gezinsleden	Van werknemers afhankelijke gezinsleden betekent de echtgeno(o)t(e), het kind of de begunstigde van een edewerker, of de noodcontactpersoon van een Medewerker of Tijdelijke Medewerker
Verantwoordelijke Leidinggevende	Verantwoordelijke Leidinggevende betekent de Managing Director van een Groepsmaatschappij, of het hoofd van een business unit of functioneel gebied, die een primair budgettair eigendom heeft van het bedrijf in de groep, de business unit of het functionele gebied.
Verplichte Vereisten	VERPLICHTE VEREISTEN betekent de verplichtingen conform het Recht van toepassing op de Verwerker die het verwerken van Persoonsgegevens voorschrijft voor (i) nationale veiligheid of verdediging; (ii) openbare veiligheid; (iii) preventie, onderzoek, detectie of vervolging van strafrechtelijke overtredingen of van inbreuk op ethiek voor gereguleerde beroepen; of (iv) de bescherming van een Betrokkene, of de rechten en vrijheden van Betrokkenen.
Verwerken	VERWERKEN betekent een bewerking met betrekking tot Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, opslaan, ordenen, wijzigen, gebruiken, verstrekken (inclusief het verlenen van toegang op afstand), doorzenden of verwijderen van Persoonsgegevens
Verwerker	VERWERKER betekent de entiteit of natuurlijke Betrokkene die Persoonsgegevens verwerkt namens een verwerkingsverantwoordelijke.
Verwerkersovereenkomst	VERWERKERSOVEREENKOMST betekent een overeenkomst voor de verwerking van Persoonsgegevens die is aangegaan tussen ADP en een Derde-Verwerker).

Verwerkingsverantwoordelijke	VERWERKINGSVERANTWOORDELIJKE betekent de rechtspersoon of natuurlijk persoon die, alleen of samen met anderen, het doel en de middelen voor het Verwerken van Persoonsgegevens vaststelt.
Werknemer van de Klant	Werknemer van de Klant betekent een Betrokkene wiens Persoonsgegevens Verwerkt worden door ADP als Verwerker in opdracht van een Klant conform een dienstverleningsovereenkomst. Omwille van duidelijkheid, WERKNEMER VAN DE KLANT verwijst naar alle Betrokkenen wiens Persoonsgegevens worden verwerkt door ADP tijdens het uitvoeren van de dienstverlening (ongeacht de juridische aard van de relatie tussen de Betrokkene en de klant). Hieronder vallen geen professionals wiens Persoonsgegevens worden verwerkt door ADP met betrekking tot ADP's directe relatie met de klant. ADP kan bijvoorbeeld Persoonsgegevens van een HR-professional verwerken om een overeenkomst met de klant aan te gaan - deze gegevens zijn onderhevig aan de Privacy Code voor bedrijfsgegevens. Als ADP echter salarisadministratiediensten biedt aan de klant (bijv. uitgifte van loonstroken, bieden van hulp bij het gebruik van een ADP-systeem), dan worden de gegevens van de Betrokkene verwerkt als Klantgegevens.
Zakelijke partner	ZAKELIJKE PARTNER betekent een Derde, anders dan een Klant of een Leverancier die een zakelijke relatie of strategische alliantie heeft of had met ADP (bijv. gezamenlijke marketingpartner, joint venture of gezamenlijke ontwikkelingspartner).

BIJLAGE 2 - Beveiligingsmaatregelen

Gepresenteerd door:	**ADP - Global Security Organization**
Versi:	**2.0**
Publicatiedatum:	**september 2019**

Inhoudsopgave

Begrippen en definities

De volgende termen kunnen in het gehele document worden gebruikt:

Gebruikt begrip of acroniem	Definitie
GETS	**Global Enterprise Technology & Solutions**
GSO	**Global Security Organization)**
CAB	**Change Advisory Board**
DRP	**Disaster Recovery Plan**
CIRC	**Critical Incident Response Center**
SIEM	**Security Information and Event Management**
IDS	**Intrusion Detection System**
DNS	**Domain Name System**
NTP	**Network Time Protocol**
SOC	**Service Organization Controls**
TPSI	**Trusted Platform Security Infrastructure**

Overzicht

ADP onderhoudt een formeel programma voor informatiebeveiliging dat administratieve, technische en fysieke waarborgen bevat ter bescherming van de veiligheid, vertrouwelijkheid en integriteit van de klanteninformatie. Dit programma is redelijkerwijs ontworpen om (i) de veiligheid en vertrouwelijkheid van de klanteninformatie te waarborgen; (ii) te beschermen tegen verwachte dreigingen of risico's voor de veiligheid of integriteit van de informatie; en (iii) te beschermen tegen onbevoegde toegang tot of onbevoegd gebruik van de informatie.

Dit document bevat een overzicht van de maatregelen en praktijken van ADP ten aanzien van de informatiebeveiliging met ingang van de publicatiedatum. Deze maatregelen en praktijken zijn onder voorbehoud van wijzigingen door ADP. Deze vereisten en praktijken zijn zodanig opgezet dat ze in lijn zijn met de ISO/IEC 27001:2013-normen voor informatiebeveiliging. ADP verricht periodiek een beoordeling van haar veiligheidsrichtlijnen en -normen. Ons doel is ervoor te zorgen dat het beveiligingsprogramma op effectieve en efficiënte wijze functioneert om alle aan ons door onze klanten en hun werknemers toevertrouwde informatie te beschermen.

Beleid inzake informatiebeveiliging

Onafhankelijkheid van de informatiebeveiligingsfunctie

ADP heeft een Chief Security Officer aangesteld, die toezicht houdt op de Global Security Organization (GSO) van ADP en die direct verslag uitbrengt aan de General Counsel (Legal & Compliance), in plaats van aan de Chief Information Officer. Hierdoor heeft GSO de nodige onafhankelijkheid ten opzichte van IT. GSO is een divisieoverschrijdend, geconvergeerd beveiligingsteam met een multidisciplinaire benadering op het gebied van cyber- en informatiebeveiliging, alsook compliance, operationeel risicobeheer, klantbeveiligingsbeheer, bescherming van het personeel en veerkracht ten aanzien van bedrijfscontinuiteit. Het senior management van GSO staat onder leiding van onze Chief Security Officer en is verantwoordelijk voor het beheer van de beveiligingsmaatregelen, -procedures en -richtlijnen.

Formele definitie van het informatiebeveiligingsbeleid

ADP heeft formele beleidsregels inzake informatiebeveiliging ontwikkeld en gedocumenteerd. Hierin wordt de ADP's benadering voor het beheer van de informatiebeveiliging uiteengezet. Specifieke gebieden die onder dit beleid vallen, zijn onder meer, echter niet uitsluitend:

- **Beleid inzake beveiligingsbeheer –** omvat de verantwoordelijkheden van de Global Security Organization (GSO) en de Chief Security Officer (CSO), met inbegrip van de verantwoordelijkheden op het vlak van informatiebeveiliging en controleprocedures ten aanzien van het wervings- en selectieproces vanuit een oogpunt van beveiliging.
- **Mondiaal privacybeleid –** bepaalt hoe persoonlijke informatie wordt verzameld en hoe de toegang tot, nauwkeurigheid van en openbaarmaking van informatie is geregeld, en bepaalt de privacyverklaring voor klanten.
- **Werknemersbeleid inzake acceptabel gebruik van elektronische communicatie en gegevensbescherming –** beschrijft het acceptabel gebruik, de verschillende vormen van elektronische communicatie, versleuteling en sleutelbeheer.
- **Beleid inzake informatiebehandeling –** voorziet in de vereisten voor de classificatie van ADP-informatie en de vaststelling van de beveiligingscontroleprocedures.
- **Beleid inzake fysieke beveiliging –** definieert de beveiligingsvereisten van ADP-faciliteiten en vervolgens van onze werknemers en van de bezoekers die daar werkzaam zijn.
- **Beleid ten aanzien van de beveiliging van bedrijfsvoering –** voorziet in de minimale controles voor het onderhoud van de systeempatches, het effectief aanpakken van de dreiging van malware en het onderhoud van controles inzake back-ups en databasebeveiliging.
- **Beleid inzake het monitoren van de beveiliging –** voorziet in controles voor inbraakdetectiesystemen (IDS), logbestanden en preventie van gegevensverlies (DLP).
- **Beleid inzake onderzoek en incidentenbeheer –** definieert de standaarden voor de respons bij incidenten, elektronische opsporing, bescherming van personeel en toegang tot de elektronisch opgeslagen gegevens van werknemers.
- **Toegangs- en authenticatiebeleid –** omschrijft de vereisten voor authenticatie (bijv. gebruikers-ID en wachtwoord), toegang op afstand en draadloze toegang.
- **Beleid inzake netwerkbeveiliging –** betreft de beveiligingsarchitectuur van routers, firewalls, AD, DNS, e-mailservers, DMZ, clouddiensten, netwerkapparaten, web proxy, en geschakelde netwerktechnologie.
- **Mondiaal beleid inzake risico's voor externe partijen en fusie en acquisitie-operaties** definieert de minimale beveiligingscontroles voor het betrekken van derden om ADP te ondersteunen bij de verwezenlijking van haar bedrijfsdoelstellingen.
- **Beleid inzake applicatiebeheer –** stelt de passende beveiligingscontroles vast voor elke fase van de levenscyclus van de systeemontwikkeling.

- **Beleid inzake bedrijfscontinuiteit–** regelt de bescherming, de integriteit en het behoud van ADP door middel van de minimale eisen voor het documenteren, implementeren, onderhouden en voortdurend verbeteren van de programma's voor het bedrijfsherstellingsvermogen.
- **Beleid inzake geconvergeerd risicobeheer –** identificatie, controle, analyse en governance van nieuwe zakelijke initiatieven en de respons daarop.

Beleidsregels worden gepubliceerd op het ADP-intranet en zijn toegankelijk voor alle werknemers en contractanten binnen het ADP-netwerk.

Beoordeling van het informatiebeveiligingsbeleid

ADP beoordeelt de informatiebeveiligingsrichtlijnen ten minste één maal per jaar of wanneer er belangrijke wijzigingen worden aangebracht die van invloed zijn op het functioneren van de informatiesystemen van ADP.

Organisatie van de informatiebeveiliging

Rollen en verantwoordelijkheden bij informatiebeveiliging

GSO bestaat uit divisieoverschrijdende beveiligingsteams die zich op basis van een multidisciplinaire benadering inzetten voor de naleving van cyber- en informatiebeveiligingsnormen, operationeel risicobeheer, klantbeveiligingsbeheer, bescherming van het personeel en bedrijfsherstellingsvermogen. Voor alle leden van GSO zijn de rollen en verantwoordelijkheden formeel gedefinieerd. GSO is belast met het ontwerp van, de implementatie van en het toezicht op ons informatiebeveiligingsprogramma op basis van onze bedrijfsrichtlijnen. De activiteiten van GSO worden gecontroleerd door de Executive Security Committee, waarvan de leden bestaan uit de Chief Security Officer, Chief Executive Officer, Chief Financial Officer, Chief Strategy Officer, Chief Human Resources Officer en de General Counsel van ADP.

Beleid inzake mobiele automatisering en telewerken

Bij ADP wordt alle vertrouwelijke informatie op mobiele apparaten verplicht versleuteld. Zo kunnen gegevenslekken als gevolg van diefstal of verlies van een computer/apparaat worden voorkomen. Geavanceerde bescherming van eindpunten en 2 factor authenticatie via VPN zijn tevens vereist om op afstand toegang te verkrijgen tot de bedrijfsnetwerken. Alle apparaten op afstand moeten beschermd zijn met een wachtwoord. ADP-werknemers zijn verplicht om eventueel verlies of diefstal van op afstand bediende computerapparatuur direct te melden met behulp van een rapportageprocedure voor beveiligingsincidenten.

Alle werknemers en contractanten van ADP dienen, als voorwaarde om voor ADP te werken, het beleid inzake het acceptabel gebruik van elektronische communicatiemiddelen en inzake gegevensbescherming en overige relevante richtlijnen volledig na te leven.

Veilig personeelsbeleid

Antecedentenonderzoek

ADP verricht, met inachtneming van de geldende wettelijke vereisten in de afzonderlijke jurisdictie, een passend antecedentenonderzoek dat in verhouding staat tot de plichten en verantwoordelijkheden van haar werknemers, contractanten en externe partijen. Deze onderzoeken bevestigen de geschiktheid van de kandidaat voor het behandelen van de informatie van de klant, voordat deze wordt aangesteld of ingehuurd.

Bij antecedentenonderzoek gaat het onder meer om de volgende zaken:

- verificatie van identiteit en arbeidskwalificaties;
- arbeidshistorie;
- opleiding en beroepskwalificaties;
- een eventueel strafblad (voor zover wettelijk toegestaan en afhankelijk van de lokale landelijke voorschriften).

Geheimhoudingsverklaringen met werknemers en contractanten

De arbeidscontracten en de contracten met contractanten van ADP bevatten verplichtingen en verantwoordelijkheden met betrekking tot de klanteninformatie waartoe toegang zal worden verkregen. Alle werknemers en contractanten van ADP zijn gehouden aan geheimhoudingsverplichtingen.

Trainingsprogramma informatiebeveiliging

Alle werknemers dienen in het kader van hun inwerkschema een training informatiebeveiliging te volgen. Daarnaast biedt ADP jaarlijkse beveiligingstrainingen aan om werknemers te herinneren aan hun verantwoordelijkheden bij het verrichten van hun dagelijkse taken.

Verantwoordelijkheden van werknemers en disciplinaire processen

ADP heeft een beveiligingsbeleid gepubliceerd waaraan alle werknemers van ADP moeten voldoen. Inbreuk op het beveiligingsbeleid kan leiden tot intrekking van de toegangsbevoegdheden en/of disciplinaire maatregelen tot en met beëindiging van adviescontracten of dienstverbanden.

Beëindiging van de verantwoordelijkheden behorende bij het dienstverband

De verantwoordelijkheden bij beëindiging van het dienstverband zijn formeel gedocumenteerd en omvatten minimaal:

- het retourneren van alle informatie en bedrijfsmiddelen van ADP die in het bezit zijn van de desbetreffende werknemers en die op ongeacht welk medium zijn opgeslagen;
- beëindiging van de toegangsrechten tot de faciliteiten, informatie en systemen van ADP;
- wijziging van de wachtwoorden voor de resterende gedeelde accounts, voor zover van toepassing;
- overdracht van kennis, voor zover van toepassing.

Beheer van bedrijfsmiddelen

Aanvaardbaar gebruik van bedrijfsmiddelen

Aanvaardbaar gebruik van bedrijfsmiddelen wordt uitgelegd in diverse richtlijnen die gelden voor werknemers en contractanten van ADP. Deze zorgen ervoor dat de informatie van ADP en de klanteninformatie niet als gevolg van gebruik van die middelen openbaar worden gemaakt. Voorbeelden van in deze richtlijnen omschreven vlakken zijn: gebruik van elektronische communicatiemiddelen, gebruik van elektronische apparatuur en gebruik van informatiemiddelen.

Classificatie van informatie

De door of namens ADP verzamelde, aangemaakte of onderhouden informatie krijgt, voor zover van toepassing, een beveiligingsclassificatie toegekend:

- Openbaar – voorbeeld: marketingbrochures, gepubliceerde jaarverslagen
- Alleen voor intern gebruik binnen ADP – voorbeeld: interne communicatie-uitingen, werkprocedures
- Vertrouwelijk binnen ADP – voorbeeld: persoonlijke informatie en gevoelige persoonsgegevens
- Beperkt binnen ADP – voorbeeld: financiële prognoses, strategische planningsinformatie

De vereisten voor behandeling van informatie zijn direct gekoppeld aan de beveiligingsclassificatie van de informatie. Persoonlijke informatie en gevoelige persoonsgegevens worden altijd als 'Vertrouwelijk binnen ADP' aangemerkt. Alle klanteninformatie wordt geclassificeerd als vertrouwelijk.

Werknemers van ADP hebben de verantwoordelijkheid om de informatiemiddelen te beschermen en te behandelen overeenkomstig de beveiligingsclassificatie. Zo wordt voor elke classificatie voorzien in bescherming van informatie en toepasselijke behandelingsvereisten. De classificatie 'Vertrouwelijk binnen ADP' wordt toegepast op alle opgeslagen, verzonden of door derden behandelde informatie.

Verwijdering van apparatuur en media

Wanneer er apparatuur, documenten, bestanden en media van ADP worden verwijderd of hergebruikt, moeten passende maatregelen worden genomen om te voorkomen dat de oorspronkelijk daarop opgeslagen klanteninformatie alsnog kan worden opgehaald. Alle informatie op computers of elektronische opslagmedia moet ongeacht de classificatie veilig worden verwijderd, tenzij de media fysiek worden vernietigd voordat ze worden vrijgegeven buiten de faciliteit van ADP, of een ander gebruiksdoel krijgen. De procedures om te waarborgen dat de op apparatuur, in documenten, in bestanden of op media aanwezige ADP-informatie veilig wordt vernietigd of gewist, zijn formeel gedocumenteerd.

Fysieke media die worden getransporteerd

Er zijn organisatorische beschermingsmaatregelen geïmplementeerd om drukwerk met klanteninformatie te beschermen tegen diefstal, verlies en/of onbevoegde toegang/wijziging (i) tijdens transport, bijv. verzegelde enveloppen en containers, of overhandiging aan een bevoegde gebruiker; en (ii) tijdens onderzoek, herziening of overige verwerking, indien verwijderd van de veilige opslag.

Toegangscontrole

Bedrijfsvereisten en toegangscontrole

Het toegangsbeleid van ADP is gebaseerd op bedrijfsvereisten. De richtlijnen en controlenormen zijn geformuleerd in toegangscontroleregels die gelden voor alle onderdelen van de geleverde dienst en die uitgaan van het beginsel dat alleen strikt noodzakelijke rechten worden toegekend alsook het beginsel van noodzaak van kennisname.

Toegang tot infrastructuur – toegangscontrolebeheer

Toegangsverzoeken om informatie te verplaatsen, toe te voegen, aan te maken en te verwijderen worden geboekstaafd, goedgekeurd en periodiek gecontroleerd.

Ten minste één maal per jaar vindt een formele beoordeling plaats om te bevestigen dat elke individuele gebruiker nauwkeurig overeenkomt met de desbetreffende bedrijfsrol en geen doorlopende toegang heeft nadat diens rol is gewijzigd. Dit proces wordt gecontroleerd en gedocumenteerd in een SOC1[1] type II-rapport. Op basis van een identiteitsbeheersysteem is een speciaal ADP-team verantwoordelijk voor het toekennen, weigeren, annuleren, beëindigen en sluiten/deactiveren van de toegang tot ADP-faciliteiten en informatiesystemen. ADP werkt op basis van een systeem voor gecentraliseerd identiteits- en toegangsbeheer (IAM), dat centraal wordt beheerd door een speciaal GETS-team. Op grond van de toegangsrechten die zijn aangevraagd via het gecentraliseerde IAM-hulpmiddel, wordt een validatiewerkstroom in gang gezet waarbij mogelijk ook de leidinggevende van de gebruiker wordt betrokken. Toegang wordt verstrekt op tijdelijke basis en er zijn werkstromen opgezet die voorkomen dat dergelijke toegang permanent is. De toegang van een werknemer tot een faciliteit wordt direct na de laatste dag van diens dienstverband gesloten door de desbetreffende toegangskaart (werknemersbadge) te deactiveren. De gebruikers-ID's van de werknemer worden eveneens direct gedeactiveerd. Alle bedrijfsmiddelen van de werknemer moeten worden geretourneerd, waarna deze worden gecontroleerd door de bevoegde lijnmanager en vergeleken met een lijst met bedrijfsmiddelen in de database voor configuratiebeheer. Ook na functie- of organisatorische wijzigingen worden de gebruikersprofielen of gebruikerstoegangsrechten verplicht aangepast door het management van de desbetreffende bedrijfsafdeling en het IAM-team. Bovendien wordt er elk jaar een formele beoordeling van de toegangsrechten verricht om te verifiëren of de individuele gebruikersrechten overeenkomen met de desbetreffende bedrijfsrollen en of er geen irrelevante toegangsrechten na een functiewijziging resteren.

Wachtwoordbeleid

Het wachtwoordbeleid van ADP voor ADP-medewerkers wordt verplicht toegepast op servers, databases en netwerkapparaten en -applicaties, voor zover het apparaat of de applicatie dat toelaat. De complexiteit van het wachtwoord wordt bepaald op basis van een risicoanalyse van de beschermde gegevens en inhoud. De richtlijnen voldoen aan de heersende standaarden in de bedrijfstak voor sterkte en complexiteit, met inbegrip van, echter niet uitsluitend, het gebruik van stapsgewijze, tweedelige of biometrische authenticatie, waar van toepassing.

Authenticatievereisten voor klanttoepassingen verschillen per product. Voor specifieke ADP-applicaties die gebruikmaken van een geïntegreerd netwerk en een door GETS beheerde beveiligingslaag, zijn gebundelde diensten (SAML 2.0) beschikbaar.

[1] In het geval van bepaalde Amerikaanse diensten die door ADP worden geboden, wordt dit gecontroleerd aan de hand van een SOC 2 type II-rapport.

Sessietime-outs

ADP legt aan alle servers, werkstations, applicaties en VPN-verbindingen automatische time-outs op die zijn gebaseerd op een risicoanalyse in overeenstemming met de standaarden in de bedrijfstak. De sessie kan uitsluitend worden hervat nadat de gebruiker een geldig wachtwoord heeft opgegeven.

Cryptografie

Cryptografische beheersmaatregelen

ADP vereist dat gevoelige informatie die wordt uitgewisseld tussen ADP en derden, wordt versleuteld (of dat het transportkanaal wordt versleuteld) met behulp van door de bedrijfstak geaccepteerde versleutelingstechnieken en -beveiligingen. Zo niet, dan kan er een particuliere huurlijn worden gebruikt.

Sleutelbeheer

ADP maakt gebruik van een interne beveiligingsnorm voor versleuteling, met inbegrip van goed gedefinieerde procedures voor sleutelbeheer en sleutelbewaring, waaronder zowel symmetrisch als asymmetrisch sleutelbeheer.

De voor informatie van ADP gebruikte encryptiesleutels zijn altijd geclassificeerd als vertrouwelijke informatie. De toegang tot deze sleutels is strikt beperkt tot diegenen die daar noodzakelijk kennis van moeten nemen, en wanneer ook goedkeuring is verleend voor een uitzondering. Encryptiesleutels en de levenscyclus van sleutelbeheer volgen de standaardpraktijken van de bedrijfstak.

Fysieke beveiliging en beveiliging van de omgeving

De aanpak van ADP inzake fysieke beveiliging dient twee doelen – zorgen voor een veilige werkomgeving voor collega's van ADP en het beschermen van de persoonsgegevens die worden bewaard in de datacentra en overige strategische locaties van ADP.

Het beveiligingsbeleid van ADP vereist van het management van ADP dat het die gebieden identificeert die een bepaald niveau fysieke beveiliging nodig hebben. Toegang tot die gebieden wordt slechts verleend aan bevoegde collega's voor bevoegde doeleinden. Beveiligde gebieden van ADP beschikken over verschillende fysieke beveiligingsmiddelen, waaronder videobewakingssystemen, gebruik van beveiligingspassen (toegang met identiteitsverificatie) en beveiligingsmiddelen die bij ingangen en uitgangen zijn geplaatst. Aan bezoekers mag alleen toegang worden verleend, waar dat is toegestaan en zij staan te allen tijde onder toezicht.

Beveiliging van de bedrijfsvoering

Formalisering van de procedures van IT Operations

Binnen ADP is GETS de afdeling die verantwoordelijk is voor het beheer en het onderhoud van de IT-infrastructuur. GETS onderhoudt en documenteert formeel de beleidsregels en -procedures van de IT-functie. Deze procedures omvatten, echter niet uitsluitend:

- Wijzigingsbeheer
- Back-upbeheer
- Afhandeling van systeemfouten
- Herstarten en herstellen van het systeem
- Systeembewaking
- Takenplanning en -controle

Infrastructuurwijzigingsbeheer

Als onderdeel van GETS is ook een periodieke Change Advisory Board (CAB) ingesteld, met daarin vertegenwoordigers uit allerlei verschillende ADP-teams. De CAB houdt bijeenkomsten om effecten te bespreken van implementatievensters en de doorvoering van wijzigingen in de productie, alsook om eventuele wijzigingen in de productie-infrastructuur te coördineren.

Systeemcapaciteitsplanning en -acceptatie

De capaciteitseisen worden voortdurend gecontroleerd en periodiek beoordeeld. Op basis van deze beoordelingen worden systemen en netwerken overeenkomstig op- of afgeschaald. Wanneer er significante wijzigingen moeten worden doorgevoerd als gevolg van een wijziging in de capaciteit of een technologische ontwikkeling, dan kan het GETS-benchmarkingteam stresstests uitvoeren op de relevante applicatie en/of het relevante systeem. Bij de afronding van een stresstest stelt het team een gedetailleerd rapport op van de prestatieontwikkeling door de wijzigingen te meten in (i) onderdelen, (ii) systeemconfiguratie of -versie, of (iii) middlewareconfiguratie of -versie.

Bescherming tegen kwaadaardige code

Eindpuntbeschermingstechnologieën worden volgens de standaarden in de bedrijfstak ingezet teneinde bedrijfsmiddelen van ADP te beschermen in overeenstemming met de beste praktijken volgens die standaard.

Beleid inzake back-upbeheer

ADP heeft beleidsregels ingevoerd die van alle productiehosting-functies vereisen dat er back-ups van de productie-informatie worden gemaakt. De reikwijdte en frequentie van de back-ups worden bepaald conform de bedrijfsvereisten van de relevante ADP-diensten, de beveiligingseisen van de desbetreffende informatie en het kritieke karakter van de informatie met betrekking tot calamiteitenherstel. Het toezicht op de ingeplande back-ups wordt verricht door GETS met als doel problemen of uitzonderingen met betrekking tot de back-ups te identificeren.

Verslaglegging en monitoring van beveiliging

ADP heeft een centrale en 'alleen lezen' logging infrastructuur (SIEM) en een logcorrelatie- en meldingssysteem (TPSI). De logmeldingen worden gecontroleerd en tijdig afgehandeld door het CIRC.

Al deze systemen worden gesynchroniseerd met behulp van een unieke klokreferentie op basis van het Network Time Protocol (netwerktijdprotocol, NTP).

Ieder afzonderlijk logbestand omvat minimaal:

- een tijdsstempel;
- wie (identiteit van de operator of de beheerder);
- wat (informatie over de gebeurtenis).

De controlesporen en systeemlogs voor de applicaties van ADP zijn zodanig ontworpen en ingesteld dat de volgende informatie kan worden bijgehouden:

- bevoegde toegang;
- vertrouwelijke activiteiten;
- onbevoegde toegangspogingen;
- systeemmeldingen of -fouten;
- wijzigingen in de beveiligingsinstellingen van het systeem, voor zover het systeem dergelijke logbestanden toestaat.

Deze logbestanden zijn alleen beschikbaar voor bevoegd personeel van ADP en worden in de livemodus verstuurd om te voorkomen dat gegevens worden gewijzigd voordat deze worden opgeslagen in de veilige logtoepassingen.

Infrastructuursystemen en monitoring

ADP maakt gebruik van passende middelen om 24 uur per dag, 7 dagen per week toezicht te houden op de infrastructuur. Meldingen van uitval worden beheerd door verschillende teams overeenkomstig hun urgentieniveau en de vaardigheden die vereist zijn om het probleem op te lossen.

De faciliteiten van het hostingcentrum van ADP maken gebruik van controleapplicaties die continu worden ingezet op alle bijbehorende verwerkingssystemen en op de netwerkonderdelen, teneinde het personeel van ADP te voorzien van proactieve meldingen van problemen en van waarschuwingen voorafgaand aan mogelijke problemen.

Beheer van technische kwetsbaarheden

Alle computers die zijn geïnstalleerd op de hostinginfrastructuur moeten compatibel zijn met de installatie van een gespecialiseerd beveiligd besturingssysteem (of veilig build-proces). Gehoste activiteiten maken gebruik van een beveiligde, goedgekeurde en gestandaardiseerde build voor elk type server dat binnen onze infrastructuur wordt gebruikt. Het 'direct uit de verpakking' installeren van besturingssystemen is niet toegestaan, omdat deze installaties kunnen zorgen voor kwetsbaarheden, zoals algemene systeemwachtwoorden die een infrastructuurrisico met zich meebrengen. Op gehoste computers, waarop vaak onnodige diensten worden uitgevoerd die kunnen leiden tot kwetsbaarheden, kan door middel van deze configuraties de kwetsbaarheid worden gereduceerd.

ADP hanteert een gedocumenteerde methodiek voor het uitvoeren van releasebeoordelingen, periodieke kwetsbaarheidsbeoordelingen en nalevingsbeoordelingen van webapplicaties die in verbinding staan met het internet, en hun overeenkomstige infrastructuuronderdelen. Deze methodiek omvat ten minste 15 primaire testcategorieën. De beoordelingsmethodiek is gebaseerd op zowel interne als uit de bedrijfstak afkomstige best practices, waaronder, maar niet uitsluitend, Open Web Application Security Project (OWASP), SANS Institute en Web Application Security Consortium (WASC).

Communicatiebeveiliging

Netwerkbeveiligingsbeheer

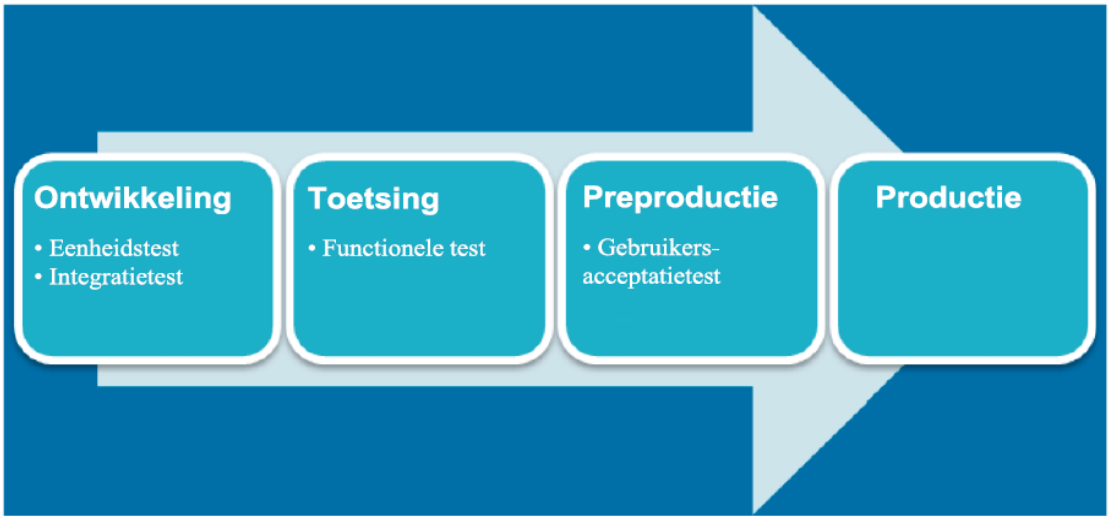
ADP maakt gebruik van een inbraakdetectiesysteem op basis van het netwerk, dat 24 uur per dag en 7 dagen per week het verkeer op netwerkinfrastructuurniveau controleert en verdachte activiteiten of mogelijke aanvallen identificeert.

Uitwisseling van informatie

ADP past passende controles toe, zodat de klanteninformatie die ADP verstuurt naar derden, alleen wordt verstuurd tussen goedgekeurde informatiesystemen en -middelen, en alleen wordt uitgewisseld via de veilige en goedgekeurde overdrachtsmechanismen van ADP.

Beveiliging binnen ontwikkelings- en ondersteuningsprocessen

Tijdens de ontwikkelingscyclus wordt bruikbare documentatie gegenereerd en worden de testschema's voor de testfase opgesteld. Voor elke omgeving worden de verschillende fasen gedefinieerd, waarbij voor elke fase goedkeuring vereist is:



- Van de test- naar de preproductie-omgeving is goedkeuring vereist van het kwaliteitsteam van ADP.
- Van de preproductie naar de productie is goedkeuring vereist van IT Operations.

Er zijn ontwikkelingsteams vereist om veilige coderingsmethoden in te zetten. Applicatiewijzigingen worden getest in een ontwikkelings- en een regressieomgeving, voordat ze de productiesystemen bereiken. Er worden tests uitgevoerd en gedocumenteerd. Na goedkeuring worden de wijzigingen geïmplementeerd in de productie. Na significante wijzigingen worden penetratietests verricht.

Als onderdeel van GETS is ook een periodieke Change Advisory Board (CAB) ingesteld, met daarin vertegenwoordigers uit allerlei verschillende ADP-teams. De CAB houdt op regelmatige basis bijeenkomsten, die zijn bedoeld om effecten te bespreken, implementatievensters overeen te komen en de doorvoering van softwarepakketten in de productie goed te keuren en ook om informatie te verstrekken over overige wijzigingen in de productie-infrastructuur.

Het IT Operations-team van ADP zorgt voor de definitieve goedkeuring voordat de softwarepakketten worden opgenomen in de productieomgeving.

Beveiliging binnen de ontwikkelingsomgeving

Productie- en ontwikkelingsomgevingen zijn van elkaar gescheiden en zijn onafhankelijk van elkaar. Passende toegangscontrolemiddelen worden ingezet om de juiste scheiding van taken te handhaven. Softwarepakketten zijn tijdens elke fase van het ontwikkelingsproces alleen toegankelijk voor de teams die betrokken zijn bij die fase.

Testgegevens

Op grond van het beleid van ADP inzake toepassingsbeheer is het gebruik van werkelijke of niet-geanonimiseerde gegevens niet toegestaan in ontwikkeling en testen, tenzij dit expliciet door de klant is aangevraagd en goedgekeurd.

Leveranciersrelaties

Vaststelling van risico's met betrekking tot externe partijen

Er worden periodiek risicobeoordelingen verricht van derden die toegang moeten hebben tot informatie van ADP en/of de klant, met als doel om vast te stellen of zij zich houden aan de beveiligingseisen van ADP voor derden en om eventuele hiaten in de toegepaste controles te identificeren. Indien een dergelijk hiaat in de beveiliging wordt ontdekt, worden nieuwe controles overeengekomen met deze derde.

Informatiebeveiligingscontracten met externe partijen

ADP ondertekent met alle derden contracten die passende verbintenissen ten aanzien van beveiliging bevatten, zodat wordt voldaan aan de beveiligingseisen van ADP.

Beheer van informatiebeveiligingsincidenten en verbeteringen

ADP heeft een gedocumenteerde methode die voorschrijft hoe tijdig, consistent en doelmatig moet worden gereageerd op beveiligingsincidenten.

In het geval zich een incident voordoet, activeert een vooraf gedefinieerd team van ADP-werknemers een formeel incidentresponsplan met betrekking tot onder meer het volgende:

- escalaties op basis van de classificatie of ernst van het incident;
- een lijst met contactpersonen voor de verslaglegging/escalatie van het incident;
- richtlijnen voor de eerste response en de vervolgacties met betrokken klanten;
- naleving van de geldende wetgeving inzake kennisgeving van de beveiligingslekken;
- onderzoekslogbestand;
- systeemherstel;
- oplossing, verslaglegging en beoordeling van het probleem;
- onderliggende oorzaak en herstel;
- geleerde lessen.

In de beleidsregels van ADP zijn omschrijvingen opgenomen van een beveiligingsincident en incidentenbeheer, alsmede van alle verantwoordelijkheden van werknemers ten aanzien van de verslaglegging van beveiligingsincidenten. ADP organiseert ook regelmatige trainingen voor werknemers en contractanten van ADP om het bewustzijn inzake de verslagleggingseisen te vergroten. De training wordt gemonitord om er zeker van te zijn dat deze werd voltooid.

Het bedrijfscontinuïteitsprogramma van ADP

ADP zet zich in voor het behoud van het soepele verloop van onze diensten en activiteiten, zodat we onze klanten de best mogelijke service kunnen leveren. Onze prioriteit is het identificeren – en beperken – van de technologie-, milieu-, proces- en gezondheidsrisico's die kunnen verhinderen dat wij onze zakelijke diensten leveren. ADP heeft een geïntegreerd raamwerk gemaakt dat onze beperkings-, bereidheids-, respons- en herstelprocessen toelicht en dat het volgende omvat:

- risicoanalyse;
- risicodreigingsanalyse;
- bedrijfseffectanalyse;
- planontwikkeling;
- planning bedrijfscontinuïteit;
- noodherstelplanning;
- gezondheids- en veiligheidsplanning;
- reactie aan het publiek;
- crisisbeheer;
- noodmaatregelen;
- testen en validering;
- beoordelen;
- herziening;
- oefenen.

Naleving

Naleving van beveiligingsbeleid en -normen

ADP hanteert een proces om periodiek interne nalevingsbeoordelingen uit te voeren. Bovendien laat ADP periodiek een SOC1[2] type II-audit verrichten. Deze audits worden uitgevoerd door een bekend extern accountantsbureau en het auditrapport wordt desgewenst jaarlijks aan klanten beschikbaar gesteld, voor zover van toepassing.

Technische naleving

Om te zorgen voor de technische naleving van de 'best practices' verricht ADP met regelmaat een geplande scan van de netwerkkwetsbaarheid. Op basis van de scanresultaten worden vervolgens in overleg met hostingteams en hun management prioritaire corrigerende actieplannen opgesteld.

De kwetsbaarheidsscans worden periodiek verricht voor zowel interne als externe omgevingen. Bovendien worden de broncodescans en penetratietests verricht per afzonderlijk product. Met behulp van gespecialiseerde hulpmiddelen voor het scannen van applicaties worden vervolgens de kwetsbaarheden op applicatieniveau, indien aanwezig, geïdentificeerd. Deze worden gedeeld met de productontwikkelingsmanagementteams en ter correctie opgenomen in de kwaliteitsborgingsprocessen. De resultaten worden geanalyseerd waarna er corrigerende actieplannen worden opgesteld en bijbehorende prioriteiten bepaald.

Bewaren van gegevens

Het ADP-beleid inzake het bewaren van gegevens met betrekking tot klanteninformatie is zodanig ontworpen dat dit voldoet aan de geldende wetgeving. Bij beëindiging van een klantenovereenkomst leeft ADP de contractuele verplichtingen na met betrekking tot de informatie van de klant. Bij beëindiging van een klantencontract retourneert ADP alle klanteninformatie die vereist is voor de continuïteit van de bedrijfsactiviteiten van de klant, of biedt de klant gelegenheid deze te downloaden (voor zover deze informatie niet reeds eerder is verstrekt). ADP vernietigt vervolgens op veilige wijze alle resterende klantinformatie, behalve voor zover vereist op grond van de vigerende wetgeving, goedgekeurd door de klant of benodigd ten behoeve van het beslechten van geschillen.

[2] In het geval van bepaalde Amerikaanse diensten die door ADP worden geboden, wordt er ook een SOC 2 type II-rapport opgesteld

BIJLAGE 3 - Groepsmaatschappijen die gebonden zijn aan de Code

ADP (Philippines), Inc	6/F Glorietta 2 Corporate Center, Palm Drive, Ayala Center, Makati City, Filippijnen, 1224
ADP (Suisse) SA	Lerzenstr. 10, 8953 Dietikon, Zwitserland
ADP Canada Co.	3250 Bloor Street West, 16th Floor, Etobicoke, Ontario M8X 2X9, Canada
ADP Employer Services Belgium BVBA	Koningsstraat 97/4, 1000 Brussels, België
ADP Employer Services Ceska Republika a.s.	Rohanske nabrezi 670/17, 18600 Praha 8, Tsjechische Republiek
ADP Employer Services GmbH	Frankfurter Str. 227, 63263 Neu-Isenburg, Duitsland
ADP Employer Services Iberia, S.L.U.	Cami Antic de Valencia, 54 B, 08005 Barcelona, Spanje
ADP Employer Services Italia SPA	Viale G. Richard 5/A – 20143 Milan, Italië
ADP ES Tunisie SARL	MIRMAR Business City Lot B16 Centre Urbain Nord – 1003 Tunis, Tunesië
ADP Europe, S.A.S.	31, avenue Jules Quentin, 92000 Nanterre, Frankrijk
ADP France SAS	31, avenue Jules Quentin, 92000 Nanterre, Frankrijk
ADP GlobalView B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Nederland
ADP GSI France SAS	31-41, avenue Jules Quentin, 92000 Nanterre, Frankrijk
ADP HR and Payroll Services Ireland Limited	Unit 1, 42 Rosemount Park Dr, Rosemount Business Park, Dublin, D11 KC98, Ireland
ADP India Private Ltd.	Tamarai Tech Park, S.P. Plot No.16 to 20 & 20A, Thiru-Vi-Ka Industrial Estate, Inner Ring Road, Guindy, Chennai – 600 032 India
ADP International Services B.V.	Lylantse Bann 1, 2908 LG Capelle aan den, Ljseel, Nederland
ADP Nederland B.V.	K.P. van der Mandelelaan 9-35, 3062 MB Rotterdam, Postbus 4065, 3006 AB Rotterdam, Nederland
ADP Outsourcing Italia SRL	Viale G. Richard 5/A – 20143 Milan, Italië
ADP Payroll Services, Inc.	One ADP Boulevard, Roseland, NJ, Verenigde Staten 07068

ADP Polska Sp. zo.o.	Prosta 70, 00-838 Warsaw, Polen
ADP Private Limited	6-3-1091/C/1, Fortune 9, Raj Bhavan Road, Somajiguda, Hyderabad, Telangana, India – 500082
ADP RPO UK Limited	22 Chancery Lane, London, Engeland, WC2A 1LS
ADP RPO, LLC	3401 Technology Drive, Findlay, OH, Verenigde Staten 45840
ADP Screening and Selection Services, Inc.	One ADP Boulevard, Roseland, NJ, Verenigde Staten 07068
ADP Slovakia s.r.o.	Cernysevskeho 26, 851 01 Bratislava, Slovakia
ADP Software Solutions Italia SRL	Via Oropa 28 – 10153 Turin, Italië
ADP, Inc.	One ADP Boulevard, Roseland, NJ, Verenigde Staten 07068
Automatic Data Processing (ADP) Romania SRL	4B Gara Herastrau St., 1st – 6th floor, District 2, Bucharest, Roemenië 020334
Automatic Data Processing Limited (Australia)	6 Nexus Court, Mulgrave, VIC 3170, Australië
Automatic Data Processing Limited (UK)	Syward Place, Pyrcroft Road, Chertsey, Surrey, KT16 9JT, England
Business Management Software Limited	2 Peterborough Business Park, Lynch Wood, Peterborough, Cambridgeshire, PE2 6FZ, England
Celergo Hungary kft	1093 Budapest, Kozraktar utca 30. 6. emelet., Cg. 01-090980824, Hungary
Celergo LLC	One ADP Boulevard, Roseland, NJ, USA 07068
Celergo PTE. LTD.	62, Ubi Road 1, #11-07, Oxley Bizhub 2, Singapore 408734
Ridgenumber - Processamento de Dados LDA	Rua Brito e Cunha, 254 - 2º, 4450-082 Matosinhos, Portugal
The Marcus Buckingham Company	8350 Wilshire Boulevard, #200, Beverly Hills, CA, Verenigde Staten 90211
VirtualEdge Corporation	One ADP Boulevard, Roseland, NJ, Verenigde Staten 07068