Honeywell

Beleid voor het gehele bedrijf

Bescherming persoonsgegevens

Kennisgeving aan lezers

In dit document wordt met "Honeywell" en het "Bedrijf" bedoeld: Honeywell International Inc. en haar dochterondernemingen die volledig eigendom zijn. Dit Beleid is niet bedoeld om contractuele verplichtingen te scheppen tussen een Werknemer en het Bedrijf. In de Verenigde Staten en bepaalde andere landen is het dienstverband bij het bedrijf "vrijblijvend", wat betekent dat het Bedrijf of de Werknemer het dienstverband te allen tijde en om elke reden zonder opzeggingstermijn kan beëindigen. Het Bedrijf behoudt zich het recht voor om dit Beleid te allen tijde te wijzigen, aan te vullen of te herroepen. Dit Beleid vervangt voorgaand beleid van Honeywell International Inc. of haar voorgangers en haar dochterondernemingen die volledig eigendom zijn, (hetzij schriftelijk of mondeling) met betrekking tot de onderwerpen die hierin zijn opgenomen. Beleid is eigendom van het Bedrijf en Werknemers dienen zorg te dragen voor het veilig bewaren van alle exemplaren van het Beleid en de Procedures en dienen deze documenten en de informatie daarin te behandelen als eigendom van het Bedrijf. Verspreid dit Beleid of de documenten waarnaar wordt verwezen in Sectie 9, getiteld "Formulieren en bewijsstukken", niet opnieuw via e-mail en post deze niet opnieuw op websites op het bedrijfsintranet of op internet. Verwijs werknemers naar de officiële website op http://policy.honeywell.com/. Indien u ontdekt dat er (1) in lokaal beleid onderwerpen zijn opgenomen die al worden behandeld in ons Beleid voor het gehele bedrijf of dat er (2) Bedrijfsbeleid is gepost op andere websites dan de officiële website, dan geeft u het adres van die website via e-mail door aan de beleidsbeheerder op: policy.steward@honeywell.com.

Verspreid dit Beleid niet opnieuw door dit opnieuw te posten op de intranetsite van het Bedrijf of op openbare internetsites. Verwijs werknemers naar de officiële website op http://policy.honeywell.com/.

Mondiaal hoofdkantoor
101 Columbia Road | Morris Township | New Jersey 07962 | Verenigde Staten

Honeywell

INHOUDSOPGAVE

Honeywell

Bescherming persoonsgegevens

Eigenaar beleid: Senior adjunct-directeur en Hoofd juridische zaken
Contactpersoon: Chris Foster
http://policy.honeywell.com/2006

Goedkeuringen

Datum van goedkeuring	Type goedkeuring	Functie	Naam
4 AUGUSTUS 2008	Goedkeuring van eigenaar beleid	Senior adjunct-directeur en Hoofd juridische zaken	Peter M. Kreindler
02 JANUARI 2008	Juridische goedkeuring	Privacyfunctionaris	Lisa Parlato LeDonne
10 JUNI 2008	Administratieve goedkeuring	Beleidbeheerder	Ashitha Varghese

Relevant beleid

Naam beleid	Categorie	URL (Universal Resource Locator)
Recordbeheer	Voor het gehele bedrijf	http://policy.honeywell.com/2004
Beveiligingsbeheer	Voor het gehele bedrijf	http://policy.honeywell.com/2071
Acceptabel gebruik van informatiebronnen	Voor het gehele bedrijf	http://policy.honeywell.com/2072
Acceptabel gebruik van mobiele apparaten voor berichten	Voor het gehele bedrijf	http://policy.honeywell.com/2073
Bedrijfscontinuïteitsbeheer	Voor het gehele bedrijf	http://policy.honeywell.com/2074
Milieubescherming van essentiële middelen	Voor het gehele bedrijf	http://policy.honeywell.com/2075
Toegangsclassificatie	Voor het gehele bedrijf	http://policy.honeywell.com/2076
Beoordeling van veiligheidsrisico's en vermindering van bedreiging	Voor het gehele bedrijf	http://policy.honeywell.com/2077
Geldende voorwaarden en bepalingen voor informatie en leveranciers van systeembeveiliging	Voor het gehele bedrijf	http://policy.honeywell.com/2078

1.0 Doel

Dit Beleid bepaalt uniforme, mondiale richtlijnen over hoe het Bedrijf in het algemeen persoonlijke gegevens wil verwerken en beschermen. Dit Beleid moet niet worden beschouwd als garantie voor actie door het Bedrijf of als basis voor contractueel bindende beloftes. Voor zover de lokale wet strengere eisen stelt dan de richtlijnen hieronder, zal het Bedrijf de lokale wet naleven.

2.0 Overzicht van wijzigingen

Ingangsdatum	Versie	Beschrijving van wijziging	Betreffende sectie(s)
18 JULI 2008	1.0	Nieuw beleid	Alle

3.0 Betrokken personen

3.1 Alle Werknemers van Honeywell International Inc., de bedrijfseenheden, directe en indirecte dochterondernemingen en gemeenschappelijke ondernemingen waarin Honeywell een meerderheidsbelang heeft.

4.0 Beleid

4.1 Wetten van toepassing

4.1.1 Het Bedrijf verwerkt persoonlijke gegevens in navolging van de toepasselijke wetten en dit Beleid. De vereisten in dit Beleid zijn van toepassing behalve wanneer de wetten van een bepaald rechtsgebied strengere beperkingen van het gebruik van persoonlijke gegevens voorschrijven.

4.2 Het verzamelen van persoonlijke gegevens

4.2.1 Het Bedrijf verzamelt persoonlijke gegevens voor geldige zakelijke doeleinden en verwerkt persoonlijke gegevens niet op een manier die tegenstrijdig is met deze doeleinden.

4.2.2 De routineuze doeleinden waarvoor het Bedrijf de persoonlijke gegevens van werknemers verzamelt en verwerkt, worden hieronder vermeld.

- Beheer van personeelszaken.
- Beheer van compensatie- en bonusprogramma's.
- Training.
- Opvolgingsplanning
- Het mogelijk maken van zakelijke transacties.
- Het beschermen van het Bedrijf, werknemers of het publiek tegen bedreigingen van veiligheid, het milieu of de gezondheid.
- Het beschermen van het Bedrijf, werknemers of het publiek tegen schade, diefstal, wettelijke aansprakelijkheid, fraude, misbruik of andere misdragingen.
- Werving.
- Prestatiebeheer.
- Voldoen aan wettelijke vereisten.
- Reisplanning en kostenbeheer.
- Fondsenbeheer.
- Taken van werknemers beheren.
- Zie overige redenen die wettelijk zijn toegestaan.

4.2.3 De routineuze doeleinden waarvoor het Bedrijf de persoonlijke gegevens van klanten en leveranciers verzamelt en verwerkt, worden hieronder vermeld

- Transacties verwerken.
- Informatie opgeven over de diensten en producten van het Bedrijf.
- Garantieclaims behandelen.
- Vragen van klanten over diensten beantwoorden.

5.0 Procedure

5.1 Wetten van toepassing toepassen

5.1.1 Voor informatie over wetten met betrekking tot de bescherming van persoonsgegevens en voor advies over wanneer toepasselijke wetten een norm creëren die strenger is dan de vereisten van dit Beleid, raadpleegt u de Adjunct-directeur juridische afdeling – Bescherming persoonsgegevens. Raadpleeg voor meer details Sectie 8.

5.2 Persoonlijke gegevens verzamelen

5.2.1 Verzamel persoonlijke gegevens uitsluitend voor zakelijke doeleinden en gebruik de gegevens uitsluitend voor deze doeleinden. Als u niet zeker weet of een bepaald voorstel geldt als zakelijk doeleinde, raadpleegt u de Adjunct-directeur juridische afdeling – Bescherming persoonsgegevens.

5.2.2 N.v.t.

5.2.3 N.v.t.

- Producten en diensten verbeteren.
- Te betalen rekeningen beheren.
- Diensten leveren.
- Producten registreren.
- Handleidingen vervangen.
- Het gebruik van de websites van het Bedrijf mogelijk maken.
- De websites van het Bedrijf aanpassen.
- Contactgegevens bijhouden.
- Vorderingen beheren.
- Zie overige redenen die wettelijk zijn toegestaan.

4.3 Het minimale verwerken van persoonlijke gegevens

4.3.1 Het Bedrijf beperkt de verzamelde en verwerkte persoonlijke gegevens tot de hoeveelheid die nodig is voor een geldig zakelijk doeleinde. Het Bedrijf deelt die gegevens met personeel voor zakelijke doeleinden, voor zover strikt noodzakelijk.

4.4 Nauwkeurig, toegankelijk en aanpasbaar

4.4.1 Het Bedrijf zorgt ervoor dat persoonlijke gegevens nauwkeurig en actueel zijn en werkt samen met de mensen van wie de gegevens worden verwerkt om deze waar nodig te wijzigen of verwijderen.

4.4.2 Indien vereist door toepasselijke wetten verleent het Bedrijf aan een persoon toegang tot zijn/haar persoonlijke gegevens. 4.4.2 Het Bedrijf is niet verplicht die toegang te verlenen wanneer de last of de kosten daarvoor zwaarder wegen dan de privacyrechten van de persoon of anderen. Als het Bedrijf een persoon toegang weigert of een verzoek voor aanpassing weigert, laat het Bedrijf de persoon de redenen voor die weigering weten. Als de persoon het niet eens is met het besluit, kan de persoon dit aangeven bij het juiste personeel zoals beschreven in Sectie 5.15.

4.5 Behoud en vernietiging

4.5.1 Het Bedrijf bewaart persoonlijke gegevens niet langer dan nodig is om de doelstellingen te realiseren waarvoor deze gegevens zijn verzameld en om te voldoen aan de vereisten van de toepasselijke wet. Nadat de persoonlijke gegevens aan het doel voor verzameling hebben beantwoord, worden de

5.3 Zorgen voor de minimale verwerking van persoonlijke gegevens

5.3.1 Voordat u een onderdeel van persoonlijke gegevens verzamelt, analyseert u of uw zakelijke doeleinde ook zonder dat onderdeel kan worden bereikt. In veel gevallen zijn anonieme gegevens (gegevens waardoor de identiteit van een individu niet kan worden achterhaald)) voldoende. In andere gevallen zijn verzamelde statistische gegevens (zoals het aantal nieuwe aangenomen werknemers in een SBG ten opzichte van het aantal inclusief de namen) voldoende.

5.4 Zorgen voor nauwkeurige, toegankelijke en aanpasbare gegevens

5.4.1 Een persoon wiens persoonlijke gegevens worden verzameld door het Bedrijf, moet het Bedrijf op de hoogte stellen als de gegevens moeten worden gewijzigd. Een werknemer moet contact opnemen met zijn/haar manager Personeelszaken of, indien mogelijk, de wijzigingen zelf aanbrengen. Een klant of leverancier moet contact opnemen met zijn/haar primaire contactpersoon bij het Bedrijf.

5.4.2 Raadpleeg sectie 5.15 voor meer details over welk personeel moet worden benaderd als de persoon niet tevreden is met de reactie van het Bedrijf op een verzoek tot wijziging.

5.5 Behoud en vernietiging beheren

5.5.1 Raadpleeg Beleid Recordbeheer voor details over het behouden en vernietigen van documenten.

persoonlijke gegevens verwijderd of vernietigd, tenzij anders wordt vereist door een contractuele overeenkomst, de wet of een regelgeving. Bestanden die persoonlijke gegevens bevatten, worden behouden of vernietigd in overeenstemming met het Beleid Recordbeheer van het Bedrijf.

4.6	Technische, fysieke en organisatorische voorzorgsmaatregelen.	5.6 Technische, fysieke en organisatorische voorzorgsmaatregelen nemen
4.6.1	Het Bedrijf beschermt persoonlijke gegevens door redelijkerwijs technische, fysieke en organisatorische voorzorgsmaatregelen te nemen om onbevoegde verwerking van deze persoonlijke gegevens te voorkomen.	5.6.1 Raadpleeg het relevante Beleid.
4.6.2	De beschermingsmaatregelen van het Bedrijf zijn toereikend voor branchenormen, de kosten van de bescherming, de gevoeligheid van de persoonlijke gegevens die worden beschermd en de risico's van de onthulling van de gegevens.	5.6.2 Raadpleeg het relevante Beleid.
4.6.3	Het Bedrijf zet administratieve en organisatorische maatregelen in om persoonlijke gegevens te beschermen. De professionele werknemers voor bescherming van persoonsgegevens van het Bedrijf zorgen voor naleving van dit beleid. Deze werknemers waarborgen toegang tot de kantoren en systemen van het bedrijf waarin persoonlijke gegevens zijn opgeslagen. Voorbeelden van de organisatorische maatregelen die het Bedrijf neemt voor het beschermen van persoonlijke gegevens, zijn procedures voor het behandelen van klachten over het gebruik van persoonlijke gegevens, het trainen van relevante werknemers in het verwerken van persoonlijke gegevens volgens dit Beleid en toepasselijke wetten, en het bijwerken van de records.	5.6.3 Raadpleeg het relevante Beleid.
4.6.4	Het Bedrijf neemt ook fysieke en elektronische maatregelen ter bescherming tegen ongewenste inbraak op systemen die persoonlijke gegevens kunnen bevatten en ter voorkoming van onrechtmatige pogingen om persoonlijke gegevens in de bestanden van het Bedrijf in te zien. Alle nieuwe systemen of toepassingen die persoonlijke gegevens verwerken, moeten eerst worden goedgekeurd door de professionele werknemers voor de bescherming van persoonsgegevens van het Bedrijf.	5.6.4 Raadpleeg het relevante Beleid. IT-systemen die persoonlijke gegevens verwerken, en materiële wijzigingen in bestaande IT-systemen moeten worden goedgekeurd voorafgaande aan implementatie. Raadpleeg Bewijsstuk 9.5.
4.6.5	Systemen die persoonlijke gegevens verwerken, moeten zo zijn beschermd dat toegang tot de gegevens uitsluitend mogelijk is voor bevoegd personeel voor zakelijke doeleinden en voor zover strikt noodzakelijk, dat er een kennisgeving van het gebruik van de gegevens wordt geleverd, dat de gegevens worden beveiligd en dat het verwijderen van de gegevens indien toepasselijk wordt vereist.	5.6.5 Raadpleeg het relevante Beleid.

4.7 Mededeling	5.7 Kennisgevingen sturen
4.7.1 Het Bedrijf stelt personen wiens persoonlijke gegevens worden verzameld, op de hoogte van de manier waarop het Bedrijf de persoonlijke gegevens verwerkt en beschermt.	5.7.1 N.v.t.
4.7.2 Voor routineuze verwerking van persoonlijke gegevens geeft het Bedrijf een algemene mededeling uit – via een privacymededeling aan werknemers wanneer dit wordt vereist door de wet of volgens dit Beleid, zoals gedefinieerd in Secties 4.2.2 en 4.2.3. Wanneer dit wordt vereist door toepasselijke wetten, wordt voor niet-routineuze verwerking van persoonlijke gegevens een specifieke mededeling voorbereid en uitgegeven.	5.7.2 Raadpleeg voor richtlijnen bij het produceren van een bijzondere kennisgeving de Adjunct-directeur juridische afdeling – Bescherming persoonsgegevens. Specifieke kennisgevingen die zijn geproduceerd volgens Sectie 4.7.2, moeten het volgende uitleggen: • de soorten persoonlijke gegevens die worden verzameld, • de doeleinden waarvoor de gegevens worden verwerkt, • de personen of groepen personen die de persoonlijke gegevens kunnen verwerken, • de maatregelen die het Bedrijf toepast om de persoonlijke gegevens te beschermen, • contactgegevens van het Bedrijf voor vragen of klachten over het verwerken van de persoonlijke gegevens, • alle maatregelen die worden genomen om het verwerken van persoonlijke gegevens te beperken, en • de maatregelen die het Bedrijf toepast om de persoonlijke gegevens te beschermen.
4.7.3 De specifieke mededeling wordt geleverd voordat de persoonlijke gegevens worden verzameld of zo snel als redelijkerwijs mogelijk na afloop.	5.7.3 N.v.t.
4.8 Toestemming	5.8 Bepalen of toestemming wordt vereist
4.8.1 Het Bedrijf verzamelt persoonlijke gegevens van verschillende bronnen, waaronder werknemers, klanten en leveranciers. Wanneer er een wettelijke of contractuele verplichting bestaat dat het Bedrijf toestemming verkrijgt voor het verzamelen en gebruiken van persoonlijke gegevens, leeft het Bedrijf die verplichting na.	5.8.1 Raadpleeg voor richtlijnen bij het bepalen of een bepaalde wet het verkrijgen van toestemming vereist, raadpleegt u de Adjunct-directeur juridische afdeling – Bescherming persoonsgegevens.
4.8.2 Als een werknemer tegenzin uit om het Bedrijf te voorzien van persoonlijke gegevens die nodig zijn voor een zakelijk doeleinde, geeft het Bedrijf hier antwoord aan volgens toepasselijke wetten. Maar de onwil van een werknemer om het Bedrijf te voorzien van persoonlijke gegevens kan het voor het Bedrijf lastiger maken om de werknemer bepaalde diensten te verlenen. Ook kan de werknemer worden benadeeld. Het Bedrijf zal echter geen represailles nemen tegen een werknemer die een klacht uit.	5.8.2 N.v.t.

4.8.3 In een aantal uitzonderlijke gevallen, zoals een onderzoek naar een mogelijke overtreding, noodsituaties en bij bevoegdheid of eis door wet of een juridisch proces, mag het Bedrijf persoonlijke gegevens verzamelen, gebruiken of openbaar maken, zonder toestemming, kennisgeving of het aanbieden van de mogelijkheid tot protest tegen het verwerken van de gegevens.	5.8.3 Herken uitzonderlijke gevallen, zoals beschreven in Sectie 4.8.3, en behandel deze uitzonderlijke gevallen uitsluitend op een manier die in overeenstemming is met wettelijke vereisten en na het verkrijgen van toestemming van een jurist van de juridische afdeling.
4.9 Bescherming van gevoelige persoonlijke gegevens	5.9 Gevoelige persoonlijke gegevens beschermen
4.9.1 Vanwege de aard van gevoelige persoonlijke gegevens biedt het Bedrijf hiervoor een hoger beschermingsniveau in vergelijking met niet-gevoelige persoonlijke gegevens.	5.9.1 Neem extra maatregelen, zoals in detail uitgelegd in Secties 5.9.2 en 5.9.3.
4.9.2 Elektronische documenten die gevoelige persoonlijke gegevens bevatten, worden beschermd met een wachtwoord. Afgedrukte exemplaren van documenten of tastbare materialen met gevoelige persoonlijke gegevens worden in een afgesloten archiefkast of kast opgeborgen of op andere wijze beveiligd.	5.9.2 Bescherm elektronische documenten met gevoelige persoonlijke gegevens met een wachtwoord; berg afgedrukte exemplaren van documenten of andere tastbare materialen met gevoelige persoonlijke gegevens op in een afgesloten archiefkast, kast of kamer.
4.9.3 Tenzij bevoegd door toepasselijke wetten zal het Bedrijf geen gevoelige persoonlijke gegevens verwerken, tenzij de bron van de gevoelige persoonlijke gegevens uitdrukkelijk toestemming heeft verleend voor de verwerking, of de verwerking: • van levensbelang is voor een persoon; • noodzakelijk is voor het vaststellen van wettelijke claims of verdedigingen; • noodzakelijk is voor het verlenen van medische zorg of het stellen van een medische diagnose; • noodzakelijk is om de verplichtingen van het Bedrijf op het gebied van dienstbetrekkingswetten na te komen; of • is gerelateerd aan gegevens die door de persoon openbaar zijn gemaakt.	5.9.3 Neem contact op met de adjunct-directeur juridische afdeling – Bescherming persoonsgegevens voor informatie over wanneer het verwerken van gevoelige persoonlijke gegevens is toegestaan volgens toepasselijke wetten.
4.10 Elektronische controle	5.10 Elektronische controle uitvoeren
4.10.1 Alle elektronische controle van persoonlijke gegevens wordt uitgevoerd in overeenstemming met lokale wetten en bepalingen, zoals overeenkomsten van een ondernemingsraad of CAO, en met de goedkeuring van een jurist in de juridische afdeling.	5.10.1 Voer elektronische controle van persoonlijke gegevens uit in overeenstemming met lokale wetten en bepalingen, zoals overeenkomsten van een ondernemingsraad of CAO. Voer geen elektronische controle uit zonder een jurist in de juridische afdeling te raadplegen.
4.11 Gevoelige identificatiegegevens	5.11 Omgaan met gevoelige identificatiegegevens
4.11.1 Gevoelige identificatiegegevens worden niet verzameld, opgeslagen, verwerkt of overgedragen, behalve indien dit absoluut vereist is voor een essentieel zakelijk doeleinde dat betrekking heeft op het beheer van werknemersuitkeringen, voor belastingdoeleinden, indien vereist door toepasselijke wetten of voor andere essentiële doeleinden die vooraf zijn goedgekeurd door de Privacyfunctionaris. Gevoelige identificatiegegevens worden niet langer	5.11.1 Raadpleeg de Adjunct-directeur juridische afdeling – Bescherming persoonsgegevens voor richtlijnen over toepasselijke wetten.

dan nodig bewaard en worden verwijderd of bewerkt wanneer ze niet meer nodig zijn.	
4.11.2 Gevoelige identificatiegegevens worden alleen als gemeenschappelijke id's of als een databasesleutel in een elektronisch informatiesysteem gebruikt, indien dit is goedgekeurd door de Privacyfunctionaris.	5.11.2 Bestaande systemen die niet in overeenstemming zijn met deze bepaling, gebruiken een plan van corrigerende acties en verstrekken het plan aan de Adjunct-directeur juridische afdeling – Bescherming persoonsgegevens.
4.11.3 Gevoelige identificatiegegevens worden alleen op verwisselbare opslagmiddelen, zoals laptops, cd's, dvd's, USB-opslagapparaten en Blackberry's opgeslagen indien de gegevens zijn gecodeerd.	5.11.3 N.v.t.
4.11.4 Gevoelige identificatiegegevens worden alleen elektronisch per e-mail overgebracht of door enig ander middel verzonden indien de gegevens zijn gecodeerd. Gevoelige identificatiegegevens worden in afgedrukte vorm uitsluitend overgedragen of overgebracht indien de Privacyfunctionaris dit goedkeurt. In dergelijke gevallen worden alle praktische voorzorgsmaatregelen genomen om de gegevens te beschermen of te bewerken.	5.11.4 Raadpleeg de Adjunct-directeur juridische afdeling – Bescherming persoonsgegevens voor richtlijnen.
4.11.5 Gevoelige identificatiegegevens worden zonder de goedkeuring van de Privacyfunctionaris niet, zelfs niet tijdelijk, overgebracht naar een thuiscomputer van een gebruiker, een website op internet of enige andere niet-geautoriseerde elektronische apparatuur.	5.11.5 Raadpleeg de Adjunct-directeur juridische afdeling – Bescherming persoonsgegevens voor goedkeuring.
4.12 Overdracht van Persoonlijke Gegevens uit de EU.	5.12 Overdracht van Persoonlijke Gegevens uit de EU
4.12.1 Persoonlijke gegevens van werknemers die zijn overgebracht uit een van de entiteiten van het Bedrijf in de EU naar een van de entiteiten van het Bedrijf in de VS, worden verwerkt in overeenstemming met de "Privacyrichtlijnen Safe Harbor Agreement" van het Bedrijf. Raadpleeg Bewijsstuk 9.2 voor "Privacyrichtlijnen Safe Harbor Agreement".	5.12.1 Raadpleeg de Privacyrichtlijnen Safe Harbor Agreement in Bewijsstuk 9.2.
4.12.2 Wanneer vereist door toepasselijke wetten moet overdracht van persoonlijke gegevens uit een van de entiteiten van het Bedrijf in de EU naar een van de entiteiten van het Bedrijf in de VS worden goedgekeurd door de standaard contractbepalingen. Deze voorwaarden vereisen dat de entiteit die de persoonlijke gegevens ontvangt, de gegevens beschermt in overeenstemming met EU-vereisten voor bescherming van persoonsgegevens.	5.12.2 Omdat het Bedrijf de Amerikaanse Safe Harbor Agreement naleeft, zijn standaard contractclausules niet noodzakelijk voor het overdragen van persoonlijke werkgegevens van de entiteiten van het Bedrijf in de EU naar entiteiten van het Bedrijf in de VS. Standaard contractclausules zijn in andere gevallen vereist, tenzij een uitzondering van toepassing is. Raadpleeg de Adjunct-directeur juridische afdeling – Bescherming voor het formulier voor standaard contractclausules en om te bevestigen wanneer dergelijke clausules noodzakelijk zijn.
4.12.3 Aanvragen voor overdracht van persoonlijke gegevens van het EU-exemplaar van PeopleSoft naar een locatie buiten de EU moeten worden goedgekeurd door de Adjunct-directeur juridische afdeling – Bescherming persoonsgegevens.	5.12.3 Neem voor informatie over het verkrijgen van goedkeuring voor een dergelijke overdracht contact op met de Adjunct-directeur juridische afdeling – Bescherming persoonsgegevens.
4.13 Overdracht van persoonlijke gegevens naar een derde partij	5.13 Overdracht van persoonlijke gegevens naar een derde partij

4.13.1 Het Bedrijf mag persoonlijke gegevens pas naar een derde partij versturen wanneer de derde partij heeft toegezegd de gegevens ten minste in overeenstemming met dit Beleid te bewaken en de instructies van het Bedrijf te volgen bij het verwerken van de persoonlijke gegevens. Het Bedrijf kiest derde partijen die het betrouwbaar acht.	5.13.1 Zorg ervoor dat de derde partij schriftelijk heeft ingestemd met het beschermen van de gegevens in overeenstemming met de vereisten genoemd in Sectie 4.12. Neem contact op met de adjunct-directeur juridische afdeling – Bescherming persoonsgegevens.
4.13.2 Het Bedrijf kan persoonlijke gegevens delen met haar gelieerde ondernemingen. De gelieerde ondernemingen van het Bedrijf volgen dit Beleid en moeten, wanneer van toepassing, contracten of overeenkomsten naleven die van toepassing zijn op de persoonlijke gegevens die naar hen worden overgedragen.	5.13.2 Raadpleeg voor meer details over de Privacyrichtlijnen Safe Harbor Agreement Bewijsstuk 9.2.
4.13.3 Het Bedrijf kan ook persoonlijke gegevens openbaar maken wanneer zij daar wettelijk bevoegd toe zijn. Wij kunnen bijvoorbeeld persoonlijke gegevens delen bij juridische situaties, om onze wettelijke rechten te beschermen of in een noodgeval, wanneer de gezondheid of veiligheid van een persoon in gevaar is.	5.13.3 Raadpleeg de Adjunct-directeur juridische afdeling – Bescherming persoonsgegevens voor richtlijnen over toepasselijke wetten.
4.14 Naleving van het Beleid	5.14 Het Beleid naleven
4.14.1 Alle werknemers worden geacht zich aan dit Beleid te houden.	5.14.1 Dit Beleid wordt aan alle werknemers gecommuniceerd.
4.14.2 Werknemers die zich niet aan dit Beleid houden, worden mogelijk onderworpen aan disciplinaire maatregelen, in het uiterste geval leidend tot ontslag.	5.14.2 Neem contact op met de adjunct-directeur juridische afdeling – Bescherming persoonsgegevens of met uw manager als u vragen hebt over de naleving van het Beleid.
4.14.3 Het Bedrijf verspreidt dit Beleid door het te publiceren in het "Systeem algemeen beleid en procedures" en door het op andere gepaste manieren te publiceren. Zie Bewijsstuk 9.5.	5.14.3 Dit Beleid moet eenvoudig toegankelijk zijn. Zie Bewijsstuk 9.4.
4.14.4 Het Bedrijf controleert naleving van dit Beleid via periodieke controles.	5.14.4 De Afdeling Bedrijfscontrole voert audits uit om naleving van dit Beleid te controleren.
4.14.5 Het Bedrijf geeft ook training aan relevant personeel dat persoonlijke gegevens verwerkt. De training wordt afgestemd op de hoeveelheid en aard van de persoonlijke gegevens die het personeel verwerkt.	5.14.5 De functie Bescherming persoonsgegevens van de juridische afdeling geeft training aan werknemers die persoonlijke gegevens verwerken.
4.15 Klachten en beroep	5.15 Een klacht indienen of beroep aantekenen
4.15.1 Het Bedrijf onderneemt redelijkerwijs stappen om het een werknemer mogelijk te maken klachten in te dienen over de manier waarom de persoonlijke gegevens van die persoon worden verwerkt.	5.15.1 Voor werknemers. Als een werknemer een klacht heeft over de wijze waarop het bedrijf persoonlijke gegevens verwerkt, moet deze contact opnemen met zijn/haar lokale afdeling personeelszaken, afdeling werknemersservices of de Adjunct-directeur juridische afdeling – Bescherming persoonsgegevens. Als de klant niet tevreden is, kan deze de klachten doorsturen naar de Afdeling integriteit en naleving van het Bedrijf door de ACCESS-hulplijn voor integriteit en naleving te e-mailen op access.integrity.helpline@honeywell.com of door de Hulplijn te bellen op 800-237-5982 (bellen van buiten de VS vereist mogelijk een landcode die u kunt vinden op www.att.com/traveler).

	Werknemers in Europa kunnen de Hulplijn bellen via telefoonnummers die te vinden zijn op de pagina Integriteit en naleving. Raadpleeg Sectie 9.3 voor de Website integriteit en naleving. Als de pogingen om het probleem op te lossen onbevredigend zijn, kan de werknemer uiteindelijk, indien hij/zij zich in de EU bevindt, contact opnemen met het panel van de EU-gegevensbeschermingsautoriteit die is opgericht als onafhankelijk klachtenorgaan in het kader van de Safe Harbor Agreement. Als de werknemer zich in Zwitserland bevindt, kan hij/zij contact opnemen met de Zwitserse federale gegevensbeschermingsautoriteit. Neem contact op met Adjunct-directeur internationale juridische afdeling – Bescherming persoonsgegevens om het juiste formulier te verkrijgen. Het Bedrijf werkt mee aan het oplossen van zulke problemen en voldoet aan het advies dat wordt gegeven door het panel van de EU-gegevensbeschermingsautoriteit of de Zwitserse federale gegevensbeschermingsautoriteit.
4.15.2 Een klant of leverancier kan ook klachten indienen bij het Bedrijf over de manier waarop het de persoonlijke gegevens van de klant of de leverancier verwerkt.	5.15.2 Voor klanten en leveranciers. Als een klant of leverancier vragen heeft over het behandelen van persoonlijke gegevens door het Bedrijf, kan die persoon een e-mail sturen naar privacy@honeywell.com. Het Bedrijf reageert snel op de vraag en onderneemt snel stappen om de zaak naar bevrediging op te lossen.
4.16 Elektronische marketing	5.16 Elektronische marketing beheren
4.16.1 Het Bedrijf gebruikt geen persoonlijke gegevens die zijn verzameld bij een persoon om producten of diensten aan die persoon te marketen, tenzij het Bedrijf de persoon de mogelijkheid geeft om te bepalen wanneer het Bedrijf marketinginformatie elektronisch naar hem/haar verstuurt.	5.16.1 Neem contact op met de adjunct-directeur juridische afdeling – Gegevensbescherming voor informatie over de wetten die van toepassing zijn op elektronische marketingcommunicatie in een bepaald rechtsgebied.
4.16.2 In bepaalde rechtsgebieden zal het Bedrijf personen de mogelijkheid bieden om geen andere aanbiedingen te ontvangen. In andere rechtsgebieden zal het Bedrijf vooraf goedkeuring verkrijgen om elektronisch aanbiedingen te versturen.	5.16.2 Neem contact op met de adjunct-directeur juridische afdeling – Gegevensbescherming voor informatie over de wetten die van toepassing zijn op elektronische marketingcommunicatie in een bepaald rechtsgebied.

6.0 Rollen en verantwoordelijkheden

6.1 De Adjunct-directeur en Hoofd juridische zaken garanderen naleving van dit Beleid.

6.2 De **Privacyfunctionaris**:

- blijft op de hoogte van wereldwijde ontwikkelingen op het gebied van privacywetten.
- geeft leiding aan de functie bescherming persoonsgegevens binnen het Bedrijf.
- werkt dit Beleid van tijd tot tijd bij in navolging van wijzigende wereldwijde privacywetgeving.
- reageert op vragen van werknemers, klanten of leveranciers die zijn doorverwezen naar de Privacyfunctionaris.
- stelt problemen en gebieden voor onderzoek vast (in een audit) om een effectieve strategie te maken voor het uitvoeren van een audit met betrekking tot het behandelen van persoonlijke gegevens binnen het Bedrijf.
- adviseert het bedrijf over de risico's en zakelijke impact van wereldwijde privacywetten.

6.3 De **Adjunct-directeur juridische afdeling – Bescherming persoonsgegevens**:

- stelt richtlijnen op voor toepasselijke wetten.
- stelt richtlijnen op voor het opstellen van een bijzondere kennisgeving aan relevante personen, die wordt gegeven voorafgaande aan de verzameling van persoonlijke gegevens.
- geeft onder begeleiding van de Privacyfunctionaris de leiding aan uitvoering van de bedrijfsstrategie voor het beschermen van persoonsgegevens.
- blijft op de hoogte van wereldwijde ontwikkelingen op het gebied van wetten met betrekking tot gegevensbescherming.
- adviseert de Privacyfunctionaris over wijzigingen die moeten worden aangebracht in dit beleid.
- beantwoordt vragen met betrekking tot gegevensbescherming.

6.4 De **Bedrijfsaccountant**:

- geeft onafhankelijke en objectieve beoordelingen van financiële zaken, gegevensverwerking en andere relevante onderwerpen binnen het Bedrijf, ter controle van naleving van dit Beleid.
- stelt problemen en gebieden voor onderzoek vast (in een audit) om een effectieve strategie te maken voor het uitvoeren van een audit met betrekking tot het behandelen van persoonlijke gegevens binnen het Bedrijf.

7.0 Definities

7.1	**Persoonlijke gegevens**	Alle gegevens waardoor de identiteit van een individu kan worden achterhaald. Bron: Functie Bescherming persoonsgegevens
7.2	**Verwerking**	Alle handmatige of automatische handelingen die worden uitgevoerd met persoonlijke gegevens. Voorbeelden van deze handelingen zijn het maken, verzamelen, opslaan, organiseren, opnemen, wijzigen, ophalen, raadplegen, gebruiken, onthullen, verspreiden, verzenden, aaneensluiten, combineren, blokkeren, verwijderen of vernietigen van persoonlijke gegevens. Bron: Functie Bescherming persoonsgegevens
7.3	**Gevoelige identificatiegegevens**	Een nationaal identificatienummer (bijvoorbeeld het burgerservicenummer in Nederland), rijbewijsnummer, bankrekeningnummer en creditcard- of bankpasnummer. Bron: Functie Bescherming persoonsgegevens
7.4	**Gevoelige persoonlijke gegevens**	Persoonlijke gegevens die bijzondere informatie over de achtergrond van een persoon onthullen die extra beschermd moet worden. Deze informatie bestaat uit persoonlijke gegevens die ras of etniciteit, politieke, religieuze of filosofische overtuigingen, lidmaatschap van een vakbond of werknemersorganisatie, fysieke of mentale toestand, seksleven of strafblad onthullen. Bron: Functie Bescherming persoonsgegevens

8.0 Normen, wetten en voorschriften

8.1 **Norm:** EU-richtlijn richtlijn gegevensbescherming 1995/46/EC.

8.2 **Norm:** EU-richtlijn privacy elektronische communicatie 2002/58/EC.

8.3 **Wet:** Children's Online Privacy Protection Act (COPPA) (Wet voor de bescherming van privacy van kinderen op internet), 15 US Code, sectie 6501, e.v.
Het voornaamste doel van de Children's Online Privacy Protection Act (COPPA) is dat ouders controle krijgen over welke gegevens van hun kinderen online worden verzameld en hoe die gegevens kunnen worden gebruikt.
http://www.ftc.gov/privacy/privacyinitiatives/childrens.html

8.4 **Wet:** Federal Trade Commission Act (wet federale handelscommissie) van 1914.
Onder 15 U.S.C. § 45(a)(2) (sectie 5 van de Federal Trade Commission Act) is de Federal Trade Commission ("FTC") bevoegd personen, partnerschappen of ondernemingen ervan te weerhouden oneerlijke concurrentiemethodes toe te passen of misleidend te handelen bij handel of om handel te beïnvloeden. Hoewel deze wet de FTC-autoriteit niet het recht geeft privacy te beschermen, wordt de wet de laatste jaren wel zo uitgelegd dat deze bepaalde privacyschendingen op basis van misleiding verbiedt. Als een bedrijf dus bijvoorbeeld een schriftelijke belofte doet op haar website of in andere bedrijfsteksten zich te houden aan bepaalde regels en die belofte vervolgens overtreedt of zich er niet aan houdt, kan het bedrijf worden vervolgd door de FTC voor het voeren van oneerlijke en misleidende praktijk in tegenspraak met sectie 5 van de FTC Act.
http://www.law.cornell.edu/uscode/html/uscode15/usc_sec_15_00000045----000-.html

8.5 **Wet:** verschillende staatswetten (in de VS) met betrekking tot kennisgeving van privacyschending.

8.6 **Wet:** verschillende landelijke en regionale privacywetten in de Europese Unie (EU), Argentinië, Australië, Canada, Hongkong, Japan, Nieuw-Zeeland en Zwitserland.

8.7 **Wet:** Financial Modernization Act van 1999.
De Financial Modernization Act van 1999, ook bekend als de "Gramm-Leach-Bliley Act" of GLB Act, bevat voorwaarden voor het beschermen van persoonlijke financiële gegevens van klanten die worden bijgehouden door financiële instituten. Er zijn drie principiële partijen betrokken bij privacyvereisten: Financial Privacy Rule, Safeguards Rule en Pretexting provisions.
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

8.8 **Wet:** Fair Credit Reporting Act (FCRA).
De Fair Credit Reporting Act (FCRA), afgedwongen door de Federal Trade Commission, bevordert nauwkeurigheid bij klantenrapporten en is bedoeld om de bescherming van de gegevens daarin te garanderen. De FCRA is onlangs aangevuld met de Fair and Accurate Credit Transactions Act van 2003 (FACTA) (PL 108-159, 12/04/03). De FACTA vereist dat de Federal Trade Commission en andere instanties vele van de nieuwe voorwaarden van de FCRA implementeren volgens regels en reglementen die in 2004 zijn uitgegeven.
http://www.ftc.gov/privacy/privacyinitiatives/credit.htm

9.0 Formulieren en bewijsstukken

9.1 **Bewijsstuk:** Beleid acceptabel gebruik van Honeywell.
http://inside.honeywell.com/hgs/policies.html?c=5

9.2 **Bewijsstuk:** Privacyrichtlijnen Safe Harbor Agreement.
http://inside.honeywell.com/law/data-privacy/pol-guidelines-details/safe-harbor-privacy.html?c=3&pag

9.3 **Bewijsstuk:** Website integriteit en naleving.
http://teamsites.honeywell.com/sites/compliance/default.aspx

9.4 **Bewijsstuk:** Systeem algemeen beleid en procedures.
Beleidshandleiding
https://policy.honeywell.com

9.5 **Bewijsstuk:** Controleproces bescherming persoonsgegevens.
Indeling zoeken op Digital Forms.
https://digitalforms.honeywell.com