Stappenplan 1: is de Wbp van toepassing?

Bijlage 1a: rechtmatige verwerking?

Bijlage 1b: melden?

Bijlage 2: RIGHT Call Hotline procedures CCE

Bijlage 3: Bewerkersovereenkomst CCE-NL en CCE Inc.

Bijlage 4: voorbereiding meldingsformulier Wbp : "Klantenbestand"

Bijlage 5: brief van het ministerie 20 oktober 2014

Bijlage 6: Vergunning voor data uitwisselen met de VS

Bijlage 7: Policy voor Acceptabel IT-gebruik

Bijlage 8: Voorbereiding meldingsformulier Wbp: "WebEx meetings (incidenteel) opnemen"

Bijlage 9: Code of Business Conduct, p. 14.

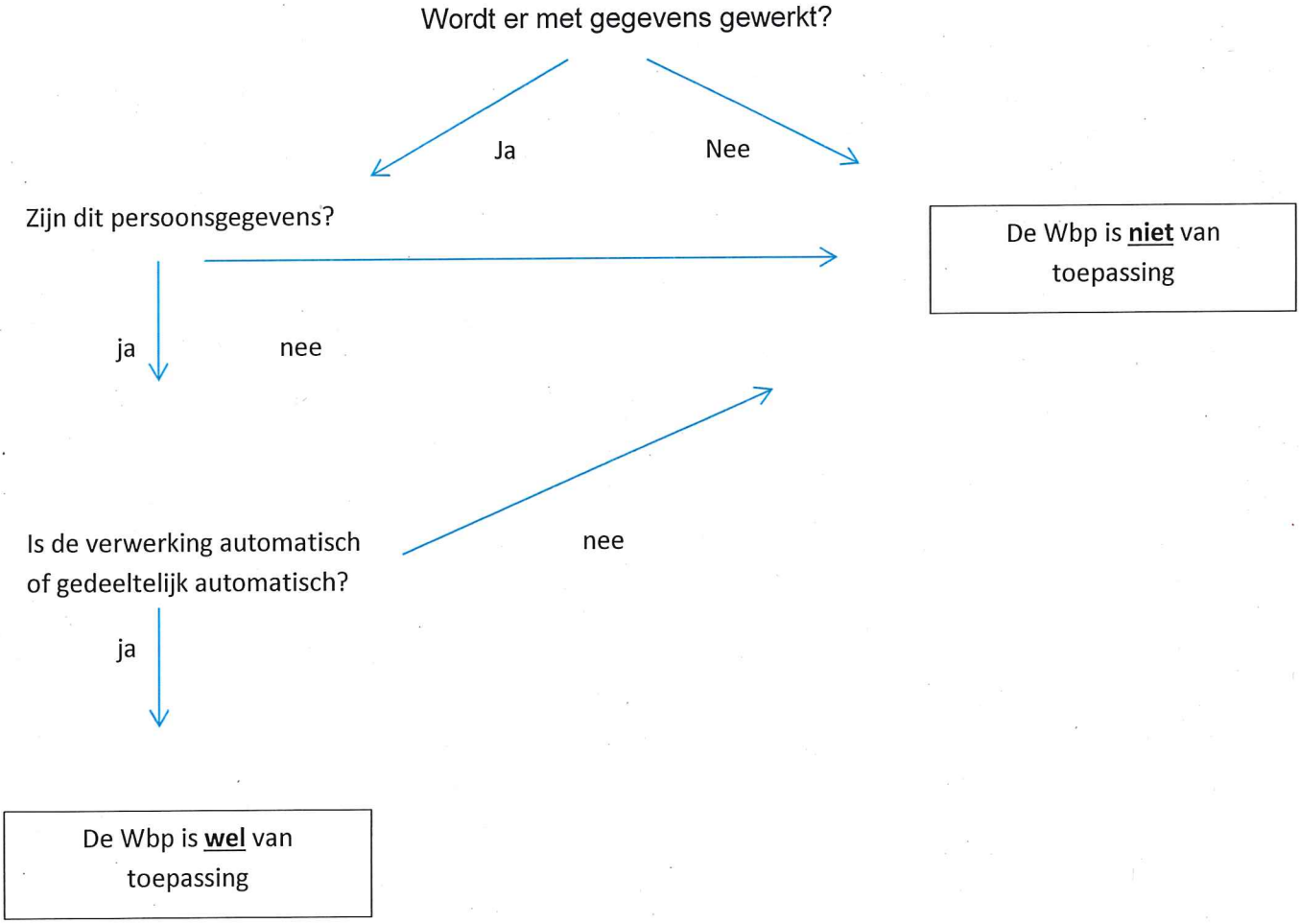
Bijlage 10: Gesprek met IT-specialist Rob Franken en Perry Wetsteijn

Bijlage 11: Privacy Policy

Bijlage 12: Richtlijn Gegevens Privacy

Stappenplan 1: is de Wbp van toepassing?

Stappenplan 1



Bijlage 1a: rechtmatige verwerking?

Bijlage 1a Rechtmatige verwerking?

1. Doeleinden: Is er sprake van een duidelijk bepaald en uitdrukkelijk omschreven **doel** voor het verzamelen van de persoonsgegevens?
   Ja, vraag 2.
   Nee, gegevensverwerking onrechtmatig
2. Grondslag: Kan de verwerking op tenminste één van de grondslagen van de Wbp worden gebaseerd?
   Ja, vraag 3.
   Nee, onrechtmatig.
3. Proportionaliteit: Zijn er maatregelen genomen opdat de persoonsgegevens juist, nauwkeurig, relevant en niet bovenmatig worden verwerkt, gelet op het doel?
   Ja, vraag 4.
   Nee, onrechtmatig.
4. Bijzonder: Worden er bijzondere persoonsgegevens verwerkt?
   Ja, vraag 5.
   Nee, vraag 6.
5. Uitzondering: Valt die verwerking onder één van de algemene of specifieke uitzonderingen op het verbod van de verwerking van bijzondere persoonsgegevens?
   Ja, vraag 6.
   Nee, onrechtmatig.
6. Marketing: Is de gegevensverwerking gericht op directe marketing doeleinden?
   Ja, vraag 7.
   Nee, vraag 8.
7. Aanvullende regels: Wordt er voldaan aan alle specifieke regels die daarvoor gelden?
   Ja, vraag 8.
   Nee, onrechtmatig.
8. Doorgifte: Worden de gegevens doorgegeven aan een land buiten de Europese Unie?
   Ja, vraag 9.
   Nee, vraag 12.
9. Verbod op doorgifte: Is doorgifte naar dat land verboden door de Europese Commissie?
   Ja, vraag 10.
   Nee, vraag 11.
10. Uitzondering verbod: Valt de verwerking onder tenminste één van de uitzonderingen op het verbod van doorgifte naar een land buiten de Europese Unie zonder een passend beschermingsniveau?
    Ja, vraag 12.
    Nee, onrechtmatig.
11. Beschermingsniveau: Waarborgt dat land een passend beschermingsniveau?
    Ja, vraag 12.
    Nee, vraag 10.
12. Restverplichtingen: Heb ik voldaan aan alle andere verplichtingen die op mij rusten? Zie opsomming A hieronder.
    Ja? Gegevensverwerking rechtmatig. Nee? Onrechtmatig.

Opsomming A hoort bij vraag 12.

a) Gegevensverwerking beveiligen
b) Niet langer bewaren dan noodzakelijk
c) Informatie verstrekken aan betrokkene
d) Op verzoek inzage geven
e) Op verzoek gegevens corrigeren
f) De verwerking stop zetten als de betrokkene zich verzet.

Bijlage 1b: melden?

Bijlage 1b melden?

1. Verwerk ik geheel of gedeeltelijk op geautomatiseerde wijze, persoonsgegevens?
   Ja, ga naar stap 3.
   Nee, ga naar stap 2.
2. Is mijn handmatige gegevensverwerking onderworpen aan voorafgaand onderzoek?
   Ja, melden bij Cbp
   Nee, je hoeft niet te melden.
3. Is mijn verwerking van melding vrijgesteld?
   Ja, dan hoef je niet te melden. Einde stappenplan
   Nee, ga naar stap 3.
4. Heb ik of heeft mijn brancheorganisatie een functionaris voor de gegevensbescherming benoemd?
   Nee, melden bij het Cbp
   Ja, melden bij de functionaris.

Bijlage 2: RIGHT Call Hotline procedures CCE

Bijlage 2: RIGHT Call Hotline Coca-Cola Enterprises

1 Inleiding

Dit document dient te worden gelezen naast de "Global Right Call richtlijnen" en voorziet in specifieke informatie voor diegenen die voor CCE-NL werken.

Deze richtlijn beschrijft de situaties waarin het u is toegestaan om de RIGHT Call hotline te gebruiken en de mogelijke gevolgen hiervan. Meer in het bijzonder behandelt de richtlijn de volgende onderwerpen:

- Wanneer kunt u gebruik maken van de RIGHT Call hotline?
- Hoe dient u gebruik te maken van de RIGHT Call hotline?
- Wat gebeurt er indien een melding wordt gemaakt via de RIGHT Call hotline?
- Hoe worden mijn rechten overeenkomstig de wetgeving omtrent gegevensbescherming gerespecteerd door de RIGHT Call hotline?

2 Wanneer kunt u gebruik maken van de RIGHT Call hotline?

De RIGHT Call hotline is opgezet voor de medewerkers van Coca-Cola Enterprises NL om melding te maken van serieus wangedrag waarbij CCE's gedragsregels ('Code of Business Conduct') wordt overtreden.

2.1 Werknemers van Coca-Cola Enterprises

Deze Richtlijn is van toepassing op alle Coca-Cola Enterprises dochterondernemingen in Nederland.

De RIGHT Call hotline mag worden gebruikt door **iedere CCE medewerker**, ongeacht zijn positie binnen CCE, zijn contractuele verhouding ten aanzien van CCE (arbeidsovereenkomst of enig ander type van overeenkomst) of zijn huidige plaats van tewerkstelling en/of nationaliteit.

Als u zich bewust bent van een situatie die een overtreding van CCE's Code of Business Conduct, bedrijfsrichtlijnen of enige van toepassing zijnde wetgeving of voorschrift met zich meebrengt, bent u verplicht dit te rapporteren bij CCE. Bij nalatigheid is dit een overtreding van onze Code of Business Conduct. Het gebruik van de RIGHT Call hotline is **optioneel**; u bent niet verplicht om meldingen te doen via de RIGHT Call hotline. CCE zal geen vergelding tolereren tegen u voor het te goeder trouw melden van vermoedelijke of bestaande overtredingen van onze gedragsregels.

2.2 Code of Business Conduct

CCE verbindt zich ertoe om gepaste middelen te voorzien om punten van zorg omtrent mistoestanden binnen CCE te kunnen melden. CCE heeft specifieke onderwerpen geïdentificeerd waarvoor, naar het oordeel van CCE , een bijkomend meldingssysteem – de RIGHT Call hotline - beschikbaar moet zijn voor u.

De RIGHT Call hotline kan **enkel en alleen** worden gebruikt **met betrekking tot de volgende onderwerpen**:

- Financiële of boekhoudkundige onregelmatigheden;
- Corruptiezaken;
- Antitrust of oneerlijke mededinging;
- Belangenconflicten;
- Klantenrelaties;
- Discriminatie;
- Werknemersrelaties;
- Vervalsing van zakelijke documenten;
- Fraude;
- Gefraudeerde verzekeringsclaims;
- Ongepaste leningen aan kaderleden;
- Handel met voorkennis;
- Smeergeld;
- Beleidsproblemen;
- Zorgen omtrent productkwaliteit;
- Vrijgeven van vertrouwelijke informatie;
- Vergelding;
- Veligheids- en hygiëneproblemen;
- Seksuele intimidatie;
- Misbruik van verboden middelen;
- Diefstal van geld;
- Diefstal van goederen of diensten;
- Diefstal van tijd;
- Ongeoorloofde kortingen;
- Problemen omtrent loon of werkuren;
- Geweld of bedreiging op de werkvloer.

Het merendeel van bovengenoemde kwesties ziet op het risico dat CCE kan lopen met betrekking tot het vermogen en de boekhouding, zoals handelingen van verduistering, belastingontduiking, wanordelijkheden met betrekking tot de boekhouding en audit van de boekhouding, witwaspraktijken, handel met voorkennis, kapitaalsverduistering of financiële fraude.

De RIGHT Call hotline is bedoeld om **bestaande controle- en auditprocedures aan te vullen** die deze specifieke en beperkte kwesties behandelen,zoals nader uiteengezet in de "Global Right Call richtlijnen". Echter, CCE begrijpt dat u zich niet altijd comfortabel voelt om via deze bestaande procedures meldingen te doen, bijvoorbeeld gezien de omvang van de beweerde mistoestand of de identiteit van de betrokken personen. In dergelijke gevallen nodigt CCE u uit om uw zorgen te delen via de RIGHT Call hotline in plaats van meldingen te doen via deze andere bestaande procedures.

Daarnaast dienen alle meldingen met betrekking tot **andere kwesties**, zoals algemene onderwerpen met betrekking tot de uitoefening van uw werk, gericht te worden aan uw gebruikelijke contactpersoon voor deze kwesties (leidinggevende, het HeRe team of HR vertegenwoordiger, etc.).

Indien u dringende zorgen heeft over gezondheid en veiligheid binnen of in relatie tot CCE of over andere risico's welke een onmiddellijk gevaar vormen voor onze onderneming of werknemers, dient u het IMT alarm nummer te bellen – 0808 100 2653.

In het geval dat u het niet zeker weet of een bepaald geval binnen het bereik van deze Policy valt dan kunt u advies vragen aan het Ethics & Compliance team. Hun contact gegevens treft u aan op iConnect.

3 Hoe dient u gebruik te maken van de RIGHT Call hotline?

3.1 De RIGHT Call hotline te goeder trouw gebruiken

U kunt gebruik maken van de RIGHT Call hotline in alle gevallen waar u redelijkerwijs van mening bent dat er een inbreuk op onze Code of Business Conduct is gemaakt of vermoedelijk gemaakt gaat worden, of dat een van bovenvermelde kwesties zich heeft voorgedaan of zich vermoedelijk zal voordoen.

Meldingen dienen steeds **te goeder trouw** te gebeuren. In deze context verzoekt CCE u om te garanderen dat elk gemeld feit gedateerd, precies, gedetailleerd en strikt gerelateerd is tot hierboven weergegeven onderwerpen. U moet enkel feiten melden waarvan u persoonlijk getuige was of kennis van heeft. Bijgevolg dient u zich ervan te weerhouden om geruchten te melden waarvoor u over geen materieel bewijsmateriaal beschikt. Bij een melding dient u gematigd en objectief taalgebruik te hanteren.

CCE zal u **niet straffen of een vergelding tegen u toelaten** voor het te goeder trouw doen van een melding, ook indien het later vaststaat dat de feiten die zijn gemeld niet correct of niet onwettig zijn.

Misbruik van de RIGHT Call hotline kan u blootstellen aan disciplinaire maatregelen en/of een gerechtelijke procedure. In deze context herinneren we er u aan dat lasterlijke meldingen of openlijke veroordelingen illegaal zijn.

3.2 Toegang tot de RIGHT Call hotline

CCE biedt u de mogelijkheid om meldingen via de RIGHT Call hotline **telefonisch** te maken:

Om telefonisch een melding te maken, bel: 00800 1888 9888.

3.3 Identificatie bij het maken van een melding

Ten einde elk misbruik van de RIGHT Call hotline te vermijden, zal u, bij het doen van een melding, **verzocht worden uzelf te identificeren** door uw naam, positie en contactgegevens mee te delen. Dit laat CCE toe om u te contacteren voor verdere opvolging mocht dit nodig zijn.

CCE zal garanderen dat uiterste vertrouwelijkheid wordt gerespecteerd zowel ten aanzien van de persoon die de melding doet als ten aanzien van de dader van de beweerde mistoestand, indien deze persoon werd geïdentificeerd in de melding.

Dus, indien u een melding doet via de RIGHT Call hotline, **zal uw identiteit nooit worden meegedeeld** aan de persoon op wie uw melding betrekking heeft, noch tegen zijn/haar leidinggevende, zelfs indien deze persoon zijn/haar recht op toegang tot zijn/haar persoonsgegevens uitoefent. Bij wijze van uitzondering kan uw identiteit worden bekendgemaakt in de context van een gerechtelijke procedure.

4 Wat gebeurt er indien een melding werd gemaakt via de RIGHT Call hotline?

4.1 Eerste ontvangst van meldingen

Voor de dagdagelijke verwerking van telefonische en online meldingen, **werkt CCE samen met een onafhankelijke derde**, The Network Inc., gevestigd te 333 Research Court, Norcross, Georgia 30092, Verenigde Staten van Amerika.

De taak van The Network is beperkt tot het beheren van de RIGHT Call hotline voor rekening vanCCE, door oproep- en beantwoordingsdiensten te voorzien, te luisteren naar uw zorgen, u vragen te stellen en de informatie te bekijken om na te gaan of alles nauwkeurig werd voorzien van documentatie. The Network is onderhevig aan een strikte vertrouwelijkheidsplicht en een contractuele verplichting om alle noodzakelijke voorzorgsmaatregelen te nemen om de veiligheid van de persoonsgegevens met betrekking tot de verzameling, mededeling en bewaring te handhaven.

4.2 Onderzoek van meldingen

Alle meldingen zullen door The Network worden doorgestuurd aan **CCE voor eerste beoordeling om de omvang van het onderzoek te bepalen**.In sommige gevallen kunnen in het kader van een onderzoek – afhankelijk van het niveau van de mistoestanden en de ernst van de meldingen - **de volgende personen** binnen de Coca-Cola Enterprises groep aan het onderzoeksteam worden toegevoegd:

- Corporate niveau - Coca-Cola Enterprises, Inc.
  - VP & Deputy General Counsel;
  - Chief Compliance and Risk Officer (Directeur du département de conformité et de gestion des risques) en Associate Director Ethics and Compliance;
  - VP Internal Audit.
- Europees niveau - Coca-Cola Enterprises, Inc. :
  - Director, Employee Relations;
  - VP Security and Associate Director Security;
  - VP Internal Control and Associate Director Internal Control;
  - VP Legal (Deputy General Counsel) and Associate Director Legal.
- Nederlands niveau :
  - VP Legal and Associate Director Legal

Dit betekent niet dat een melding systematisch zal worden doorgestuurd naar de bovenvermelde ontvangers maar enkel dat deze personen op de hoogte kunnen worden gebracht van de melding indien, en enkel indien, dit binnen de reikwijdte van hun taken valt.

4.3 Rechten van verdediging

CCE **respecteert de rechten van verdediging van haar werknemers**, en personen op wie een melding betrekking heeft zullen altijd worden verondersteld onschuldig te zijn. Betrokken zijn in een melding die is gedaan via de RIGHT Call hotline betekent niet dat CCE klachten heeft ten aanzien van u. Het betekent enkel dat een feit, handeling of gedrag kan leiden tot problemen van naleving voor CCE geldende wetten en regelgeving waardoor CCE genoodzaakt is om verduidelijking te krijgen.

Alle werknemers zullen rechtvaardig en in overeenstemming met de wet worden behandeld tijdens een intern onderzoek. Onderzoeken zullen gestructureerd verlopen ten einde de vertrouwelijkheid te garanderen en om navraag enkel toe te laten met betrekking tot kwesties die rechtstreeks verband houden met de melding.

Om te verzekeren dat de procedure niet deloyaal is ten aanzien van de medewerkers van CCE, **zal u automatisch en onmiddellijk worden geïnformeerd omtrent het bestaan van de melding**, indien een melding direct of indirect naar u verwijst. Deze informatie zal gebeuren in de vorm van een schriftelijke kennisgeving waarin het volgende wordt weergegeven:

- De onderneming belast met de RIGHT Call hotline;
- De ontvanger(s) van de melding zoals opgesomd in onderdeel 4.2;
- De beweringen die tegen u werden geuit;

- Het feit dat u beschikt over een recht tot toegang en verbetering van uw persoonsgegevens, en de manier waarop u deze rechten kan uitoefenen;
- Het feit dat u het recht heeft om de beweringen te beantwoorden, en de manier waarop u dit recht kan uitoefenen.

Enige commentaar of bedenkingen die u zou indienen ten gevolge ontvangst van dergelijke kennisgeving, zullen worden bewaard samen met de oorspronkelijke melding, zodanig dat uw positie duidelijk blijkt in de verklaringen omtrent de beweerde feiten.

Bij wijze van uitzondering, indien een melding direct of indirect naar u verwijst, **zult u hiervan niet worden geïnformeerd** in geval de melding geen verband houdt met een kwestie die gedekt wordt door de RIGHT Call hotline (zoals beschreven in onderdeel 2.2) en ten gevolge hiervan onmiddellijk wordt vernietigd. Bovendien, indien CCE redelijkerwijs beschouwt dat er een risico bestaat dat de kennisgeving aan u de mogelijkheid van CCE om efficiënt de bewering te onderzoeken of het nodige bewijs te verzamelen zou verhinderen, zal CCE uw kennisgeving uitstellen tot dat dergelijk risico niet langer bestaat.

4.4 Bewaring en archivering van meldingen

Elke melding die geen betrekking heeft op één van de kwesties die gedekt worden door de RIGHT Call hotline (zoals beschreven in onderdeel 2.2) zal onmiddellijk worden verwijderd. Meldingen waarvan wordt beschouwd dat ze onvoldoende gefundeerd zijn zullen eveneens onmiddellijk worden verwijderd, en alle werknemers betrokken in dergelijke melding zullen hiervan op de hoogte worden gebracht.

Persoonsgegevens met betrekking tot een melding die verder werd onderzocht, zullen worden verwijderd binnen 2 maanden na afsluiting van het onderzoek, op voorwaarde dat dergelijk onderzoek niet wordt gevolgd door een disciplinaire maatregel of gerechtelijke procedure.

In geval een melding en verder onderzoek de start van een gerechtelijke procedure of een disciplinaire maatregelen impliceren ten aanzien van de beschuldigde persoon, of ten aanzien van een werknemer die de melding heeft gemaakt en hierbij misbruik heeft gemaakt van de de RIGHT Call hotline, zullen de persoonsgegevens worden bewaard tot afsluiting van deze procedure en de termijn toegestaan om beroep aan te tekenen.

5 Op welke manier worden mijn rechten overeenkomstig de privacywetgeving beschermd door de RIGHT Call hotline?

CCE is van mening dat de werkwijzes en procedures van de RIGHT Call hotline zoals hierboven beschreven blijk geven van het engagement van CCE met betrekking tot uw privacy en naleving van de wetgeving omtrent bescherming van persoonsgegevens. Voor uw gemak, worden in dit onderdeel 5 de manieren weergegeven waarop de RIGHT Call hotline uw persoonsgegevens verwerkt indien u een melding doet en/or indien iemand een melding doet waarin u wordt beschuldigd, alsook de manier waarop u uw rechten overeenkomst de wetgeving omtrent bescherming van persoonsgegevens kan uitoefenen.

Types van persoonsgegevens – In de context van de RIGHT Call hotline, zal de verzameling van persoonsgegevens beperkt zijn tot de volgende types van persoonsgegevens:

- Identiteit, positie en contactgegevens van de werknemer die melding doet;
- Identiteit, positie en contactgegevens van de persoon die het voorwerp uitmaakt van de melding;
- De gemelde feiten;
- Gegevens van de persoon belast met de gegevensverwerking;
- Het bewijs verzameld gedurende de onderzoeksprocedure;
- Resultaten en uitkomst van de onderzoeken;

- Gevolgen van de melding.

Doeleinden van de verwerking – Persoonsgegevens verzameld in de context van de RIGHT Call hotline zullen worden gebruikt door CCE voor doeleinden van:

- Het opvolgen van meldingen;
- Het onderzoeken van meldingen;
- Het instellen en voeren van gerechtelijke procedures of disciplinaire maatregelen, indien van toepassing.

Ontvangers van persoonsgegevens – Uw persoonsgegevens verzameld in de context van een melding gemaakt via de RIGHT Call hotline, kunnen worden verwerkt door of meegedeeld aan de volgende partijen:

- The Network, de onafhankelijke derde die de RIGHT Call hotline beheert op een dagdagelijkse basis;
- Personen die verantwoordelijk zijn voor het onderzoeken van meldingen en die zijn tewerkgesteld door dezelfde CCE entiteit zoals u;
- Personen die verantwoordelijk zijn voor het onderzoeken van meldingen en die tewerkgesteld zijn door een andere CCE entiteit, indien de aard of omvang van de gemelde feiten hun betrokkenheid vereisen.

Doorgifte van persoonsgegevens – Het beheer van de RIGHT Call hotline en het onderzoek van de meldingen zoals omschreven in deze Policy, brengt de doorgifte van persoonsgegevens naar de Verenigde Staten, en in het bijzonder aan The Network In. en Coca-Cola Enterprises Inc., met zich mee.

Beide ondernemingen beschikken over een Safe Harbor certificaat. De Safe Harbor certificering is een systeem van privacybeginselen onderhandeld tussen de Verenigde Staten van Amerika en de Europese Commissie die Amerikaanse ondernemingen toelaat om persoonsgegevens uit Europa te ontvangen in overeenstemming met het beschermingsniveau vereist door de Europese wetgeving.

Verkrijgen van informatie omtrent de verwerking van uw persoonsgegevens – Deze Policy beschrijft op een gedetailleerde manier de manier waarop uw persoonsgegevens worden verwerkt in de context vande RIGHT Call hotline.

Bovendien werden alle werknemers van CCE geïnformeerd omtrent de inhoud van deze Policy via (i) de vereiste consultatieprocedure van de Ondernemingsraad, en (ii) de publicatie van de Policy op het intranet vanCCE .

Indien een melding werd gemaakt die betrekking heeft op u, zal u hiervan worden op de hoogte gebracht op de manier zoals omschreven in onderdeel 4.3.

Recht van toegang, verbetering en verwijdering – Indien u uw recht van toegang, verbetering en/of verwijdering wenst uit te oefenen, mag u contact opnemen met uw locale VP HR.

Bijlage 3: Bewerkersovereenkomst CCE-NL en CCE Inc.

DATA TRANSFER AGREEMENT

Name of data exporting organisation:
Coca-Cola Enterprises Nederland B.V.

Registered Office Address:
Watermanweg 30
3067 GG Rotterdam

Tel.: 00 31 (0) 10 2455400; ***Fax:*** 00 31 (0)10 2455428

Other information needed to identify the organisation:
Registered Company Number: 24172526

("the Data Exporter")

and

Name of data importing organisation:
Coca-Cola Enterprises Inc.

Address:
2500 Windy Ridge Parkway
Atlanta,
GA 30339
USA

Tel.: 01-770-989-3000; ***Fax***: 01-770-989-3619;

("the Data Importer")

HAVE AGREED, with effect from July 1st, 2004, on the following contractual clauses in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the Data Exporter to the Data Importer of the personal data specified in the Appendix I:

Clause 1 **Definitions**

For the purposes of the Agreement:

(a) "***personal data***", "***special categories of data***", "***process/processing***", "***Controller***", "***processor***", "***Data Subject***" and "***Supervisory Authority***" shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("the Directive");

(b) "the ***Data Exporter***", who has been identified above, shall mean the Controller who transfers the Personal Data;

(c) "the ***Data Importer***", who has been identified above, shall mean the Controller who agrees to receive from the Data Exporter personal data for further processing in accordance with the terms of this agreement and who is not subject to a third country's system ensuring adequate protection.

Clause 2 **Details of the Transfer**

The details of the transfer, and in particular the categories of personal data and the purposes for which they are transferred, are specified in Appendix I which forms an integral part of this agreement.

Clause 3 **Third Party Beneficiary Clause**

The Data Subjects can enforce this clause and Clauses 4 (b) and (c), Clauses 5 (a), (b), (c) and (e), Clause 6 (1) and (2) and Clauses 7, 9 and 11 as third party beneficiaries. The parties do not object to the data subjects being represented by an association or other bodies if they so wish and if permitted by national law.

Clause 4 **Obligations of the Data Exporter**

The Data Exporter agrees and warrants:

(a) that the processing of the personal data by it, including the transfer itself, has been and, up to the moment of the transfer, will continue to be carried out in accordance with all the requirements and relevant provisions (and where applicable has been notified to the relevant Authorities) of the Member State in which the Data Exporter is established and does not violate the current laws or regulations in that Member State;

(b) that, if the transfer involves special categories of data, the Data Subjects have been informed or they will be so informed at the latest at the time of the transfer that their data could be transmitted to a third country not providing adequate protection; and

(c) to make available to the Data Subjects upon request a copy of this agreement as agreed and to respond in a reasonable time and to the extent reasonably possible to enquiries from the Supervisory Authority on the processing of the relevant personal data by the Data Importer and to any enquiries from the Data Subject concerning the processing of his or her personal data by the Data Importer.

Clause 5 **Obligations of the Data Importer**

The Data Importer agrees and warrants:

(a) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling its obligations under the contract. If a change of this legislation is made, which is likely to have a substantial adverse effect on the guarantees provided by the Agreement, it will notify the change to the Data Exporter and to the Supervisory Authority where the Data Exporter is established. The Data Importer agrees that in such circumstances the Data Exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) to process the personal data in accordance with the set of principles attached to this agreement at Appendix II ("Mandatory Data Protection Principles");

or, if explicitly agreed by the parties, by ticking below, without prejudice to compliance with provisions relating to the purpose limitation, the restrictions on onward transfers and the rights of access, rectification, deletion and objection mentioned in the "Mandatory Data Protection Principles", to process in all other respects the data in accordance:-

☐ with the relevant legislation of national law protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data applicable to a Data Controller in the country in which the Data Exporter is established; or

☐ the relevant provisions found in any Commission decision under Article 25(6) of Directive 95/46/EC finding that a third country provides adequate protection in certain sectors of activity only, provided that the Data Importer is based in that third country and not covered by those provisions, in so far those provisions are of a nature which makes them applicable in the sector of the transfer.

The relevant texts/documents are attached to this agreement.

(c) to deal promptly and properly with all reasonable inquiries from the Data Exporter or a Data Subject relating to its processing of the Personal Data subject to the transfer and to co-operate with the competent Supervisory Authority in the course of all its inquiries and abide by the advice of the Supervisory Authority with regard to the processing of the data transferred; and

(d) at the request of the Data Exporter to submit its data processing facilities for audit. The audit shall be carried out by the Data Exporter or an inspection body composed of independent members and in possession of the required professional qualifications, selected by the Data Exporter and, where applicable, in agreement with the Supervisory Authority;

(e) to make available to a Data Subject upon request a copy of this agreement as agreed and indicate the office which handles complaints.

Clause 6 **Liability**

(a) The parties agree that Data Subjects who have suffered damage as a result of any violation of the provisions referred to in Clause 3 are entitled to receive compensation from the parties for the damage suffered. The parties agree that they may be exempted from this liability only if they prove that none of them is responsible for the act incompatible with the obligations contained in this agreement.

(b) The Data Exporter and the Data Importer agree that they will be jointly and severally liable for damage to a Data Subject resulting from any violation of the provisions referred to in Clause 6(a). In the event of a violation of these obligations and/or conditions, the Data Subject may take action before a court against either the Data Exporter or the Data Importer or both.

(c) The parties agree that if one party is held liable for a violation by the other party of any of the provisions referred to in Clause 3, the other party will indemnify the first party from any cost, charge, damages, expenses or loss incurred by the first party to the extent to which the other party is liable.

Clause 7. **Mediation and Jurisdiction**

(a) The parties agree that in the event of a dispute between a Data Subject and either party to this agreement, which is not amicably resolved and where the Data Subject invokes the third party beneficiary provision in Clause 3, they accept the decision of the Data Subject:

(i) to enter into third party mediation, including by the Supervisory Authority, where that facility is provided; and

(ii) to refer the dispute to the Courts in the Member State in which the Data Exporter is established.

(b) The parties agree that by common agreement between a Data Subject and the relevant party to the this agreement, the resolution of a specific dispute can be referred to an arbitration body provided that that party is established in a country which has ratified the New York Convention on Enforcement of Arbitration Awards.

3. The parties agree that the available above options will not prejudice the Data Subject's substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 **Co-operation with Supervisory Authorities**

The parties agree to deposit a copy of this agreement with the Supervisory Authority if it so requests or where deposit is required under national law.

Clause 9 **Termination of the Agreement**

The parties agree that the termination of this agreement at any time, in any circumstances and for whatever reasons does not exempt them from the obligations and/or conditions under this agreement as regards the processing of the data transferred.

Clause 10 **Governing Law**

This agreement shall be governed by the laws of the Netherlands

Clause 11 **Variation of the contract**

The parties undertake not to vary or modify the terms of this agreement unless agreed in writing.

On behalf of the Data Exporter:

Name: M. Voets
Position: Director Human Resources
Signature: Date:

On behalf of the Data Importer:
Name:
Position:
Signature: Date:

APPENDIX I
This appendix is part of this agreement and it has to be completed and signed by the parties

Data Exporter
The Data Exporter is the manufacturer and distributor of certain non-alcoholic beverages within the Netherlands and may send Personal Data to its ultimate parent company, the Data Importer, for the purposes of managing and administering the affairs of the Coca-Cola Enterprises group of companies' business, such purposes more particularly described below.

Data Importer
The Data Importer is the ultimate Parent Company of the Data Exporter and receives Personal Data as a result of its capacity as the ultimate Parent Company.

Data Subjects
The Personal Data transferred concern the following categories of Data Subjects:

- Staff including volunteers, agents, temporary and casual workers
- Former Staff of the Data Exporter
- Relatives, guardians and associates of the data subject
- Advisers, consultants and other professional experts
- Customers and clients
- Suppliers, including supplier's agents and workers
- Complainants, correspondents and enquirers

Purposes of the transfer
The transfer is necessary for the following purposes:

(a) **Staff administration**
Appointments or removals, pay, discipline, superannuation work management or other personnel matters in relation to the staff of the Data Exporter, including the administration and management of a HR IS system and payroll system for the Coca-Cola Enterprises Group of Companies.

(b) **Assessment and collection of taxes and other revenue**
Assessment and collection of taxes, duties, levies and other revenue.

(c) **Benefits, grants and loans administration**

The administration of welfare and other benefits in particular (without limitation) the administration of the Data Exporter's Share Plan scheme.

(d) **Information and databank administration**
Maintenance of information or databanks as a reference tool, as a general resource or for training purposes in particular the maintenance of the Data Exporter's internal address book, the Data Exporter's email system, the Data Exporter's voicemail system.

(e) **Legal services**
The provision of in-house legal services.

(f) **Pensions administration**
The administration of funded pensions or superannuation schemes.

(g) **Complaints/Queries**
The resolution of third party and customer complaints.

Categories of data
The personal data transferred concern the following categories of data:

Personal details:- data which identify the data subject and their personal characteristics including names, addresses, contact details, age, sex, date of birth, physical descriptions, identifiers issued by public bodies, eg NI number.

Family, lifestyle and social circumstances:- matters relating to the family of the data subject and the data subject's lifestyle and social circumstances, for example details about current marriage and partnerships and marital history, details of family and other household members, housing, travel details, leisure activities, membership of charitable or voluntary organisations.

Education and training details - matters relating to the education and any professional training of data subjects such as academic records, qualifications, skills, training records, professional expertise, student and pupil records.

Employment details:- matters relating to the employment of the data subject. Employment and career history, recruitment and termination details, attendance record, health and safety records, performance appraisals, training records, security records.

Financial details:- matters relating to the financial affairs of the data subject including income, salary, assets and investments, payments, creditworthiness of customers, loans, benefits, grants, insurance details, pension information.

Sensitive Data

The personal data transferred concern the following categories of sensitive data:

Information about the Physical or mental health or condition of employees

Recipients
The personal data transferred maybe disclosed only to the following recipients or categories of recipients:

(a) Those employees, agent or professional adviser of the Data Importer who have a need to know such information;

(b) Data Processors;

(c) Insurance and pension companies, fund managers, brokerage houses, actuaries, US governmental agencies and departments for the purposes of visa applications, work permits, I-9 forms, other disclosure documents for governmental agencies or regulatory bodies.

Storage limit
The personal data transferred may be stored only for the times indicated in the CCE document retention policy attached at Appendix III.

On behalf of the Data Exporter:

Name:
Position
Address:

Signature: Date:

On behalf of the Data Importer:
Name:
Position
Address:

Signature: Date:

APPENDIX II

Mandatory Data Protection Principles referred to in the first paragraph of Clause 5 (b)

These data protection principles should be read and interpreted in the light of the provisions (principles and relevant exceptions) of Directive 95/46/EC.

They shall apply subject to the mandatory requirements of the national legislation applicable to the Data Importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13 of the Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others.

These data protection principles represent a minimum requirement for data protection which the Data Importer agrees and warrants to respect as provided for in Clause 5 of the standard contractual clauses.

1) **Purpose limitation** - Data must be processed and subsequently used or further communicated only for the specific purposes in the Appendix I attached to these standard contractual clauses. Data must not be kept longer than necessary for the purposes for which they are transferred.

2) **Data quality and proportionality** - Data must be accurate and, where necessary, kept up to date. The data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3) **Transparency** – Data Subjects must be provided with information as to the purposes of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fair processing, unless such information has already been given by the Data Exporter.

4) **Security and confidentiality** - technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as unauthorised access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the controller.

5) **Rights of access, rectification, erasure and blocking of data: as provided for in Article 12 of Directive 95/46/EC,** the Data Subject must have a right of access to all data relating to him/her that are processed and, as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the provisions of these principles, in particular because of the incomplete or inaccurate nature of the data. He/she should also be able to object to the

processing of the data relating to him/her on compelling legitimate grounds relating to his/her particular situation.

6) **Restrictions on onward transfers.** Further transfers of personal data from the Data Importer to another controller established in a country outside the Community not providing adequate protection or not covered by a decision adopted by the Commission pursuant to Article 25(6) of the Directive 95/46/EC (onward transfer) may only take place if one of the following conditions is fulfilled:

a) Data Subjects have given their unambiguous consent to the onward transfer if special categories of data are involved, or have been given the opportunity to object in other cases. The minimum information to be provided to Data Subjects must contain in a language understandable to them:
   - the purposes of the onward transfer,
   - the identification of the Data Exporter established in the Community,
   - the categories of further recipients of the data and the countries of destination and,
   - an explanation that, after the onward transfer, the data may be processed by a controller established in a country where there is not an adequate level of protection of the privacy of individuals, or

b) the Data Exporter and the Data Importer agree to the adherence of another controller to the standard contractual clauses who therefore becomes a new party to these clauses and enters the same obligations as the Data Importer.

7) **special categories of data** - where 'sensitive' data and data relating to offences, criminal convictions or security measures are processed, additional safeguards should be in place within the meaning of Directive 95/46/EC, in particular, appropriate security measures such as strong encryption for transmission or such as keeping a record of access to sensitive data.

8) **direct marketing** - where data are processed for the purposes of direct marketing, effective procedures should exist allowing the Data Subject to 'opt-out' at any time from having his/her data used for such purposes.

9) **automated individual decisions** - Data Subjects are entitled not to be subject to a decision which is based solely on automated processing of data, unless other measures are taken to safeguard the individual's legitimate interests as provided for in Article 15(2) of Directive 95/46/EC. Where the purpose of the transfer is the taking of an automated decision as referred to in Article 15 of the Directive 95/46/EC, which produces legal effects concerning the individual or significantly affects him and which is based solely on automated processing of data intended to

evaluate certain personal aspects relating to him such as his performance at work, creditworthiness, reliability, conduct etc the individual should have the right to know the reasoning for this decision.

APPENDIX III –Data Importer's Document Retention Policy

Permanent Retention

- Form 5500 Annual returns (employee pension reporting for tax purposes)
- PBGC Form 1 and Form 1-ES (annual premium payment on employee pensions)
- Annuity or deferred payments

Term of Years

A. **1 Year**
- Union reports

B. **3 Years**
- Assignments, attachments, garnishments
- Authorizations for voluntary payroll deductions
- Employment verifications
- Incentive plan evaluations
- I-9 form (verification of employee's citizenship or eligibility to work in the United States) : later of 3 years after hire or 1 year after employment ceases

C. **5 Years**
- Time cards or equivalent
- Occupational Safety and Health Administration reports and records (except employee exposure records [30 years] and medical records [duration of employment plus 30 years])
- Direct deposit information

D. **7 Years**
- Fair Labor Standards Act overtime exemption reports
- Gross-up tax calculations
- Relocation Approval Forms

E. **10 Years**
- Benefit files
- QTD payroll master files (quarterly records of company-wide payroll)
- Restricted Stock Awards data
- Stock option and stock appreciation rights documents

Retention until Tax Department Authorizes Discard

- Commission worksheets
- Employment agreements – longer of tax department authorization or 3 years after expiration
- Personal use of club memberships or company-owned vehicles

- Account distribution files (records of payroll charges to the general ledger account categorized by account divisions)
- Labor distribution files (records of payroll charges to the general ledger account categorized by labor divisions)
- W-2 listing data (comprehensive record of employees' wage and tax statements)
- Federal unemployment returns
- State and local returns
- State withholding forms
- W-2 forms (wage and tax statement provided to employees annually)
- W-4 forms (employees' tax reporting document filed with the federal government)
- 940 Annual returns (employer's annual federal unemployment tax return)
- 941 Quarterly returns (employer's reporting of payroll to federal government)
- Account/labor distribution analysis
- Check registers
- Deferred compensation data
- Moving and location support
- Noncash renumeration records

The following documents shall be kept until the expiration of the applicable statute of limitations:-

- Non-compete agreements
- Pension plan records/reports (as required by Benefits Administration)
- Personal Choice plan records/reports (as required by Benefits Administration) (records relating to employees' benefits)
- 401(k) records/reports (tax-free employee retirement fund)
- Employment Applications
    - Hired and Declined:
- Personnel record folders:
- Service bureau records:
- Termination checklists
- Authorizations for changed pay rates or salary amount
- Payroll Registers:
- Severance agreements
- Payroll employee master files
- Bonus calculations
- Payroll journals/registers

Bijlage 4: voorbereiding meldingsformulier Wbp : ''Klantenbestand''

Deze ruimte niet beschrijven

0 E Meldingsnr. | | | | | | | | |

0 M

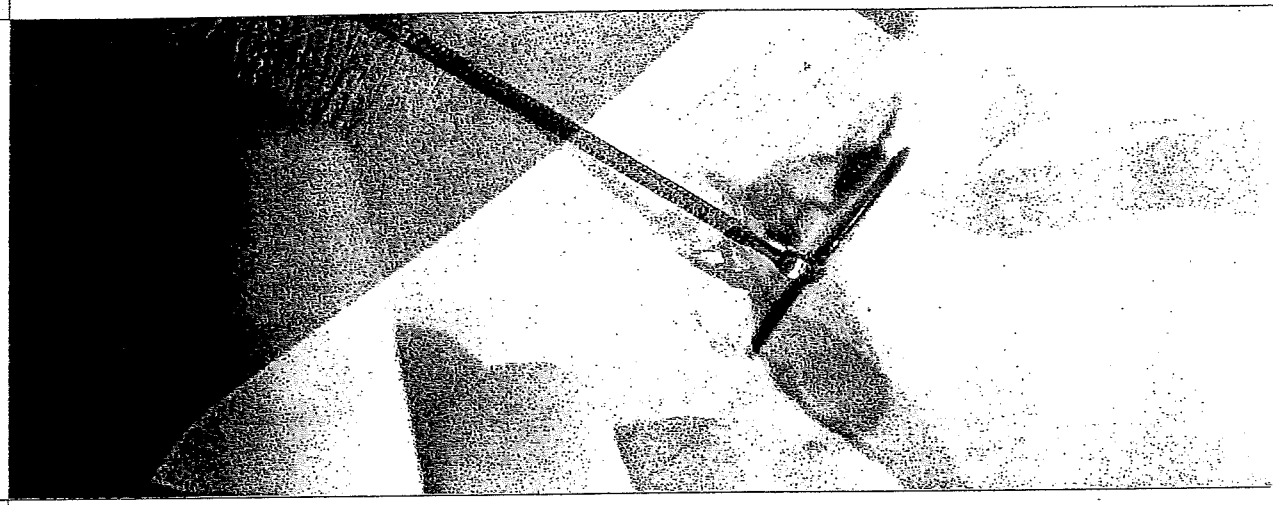
Datum

Deze melding betreft een:

● Eerste WBP-melding | *ga naar vraag 1* |

0 Mutatie | *vul hier uw toegekende meldingsnummer in* |

| | | | | | | | |



Meldingsformulier verwerking persoonsgegevens

Met dit formulier kan een verwerking van persoonsgegevens gemeld worden bij het College bescherming persoonsgegevens (CBP). Het betreft de melding bij het CBP die op grond van de Wet bescherming persoonsgegevens (WBP) geldt voor niet van melding vrijgestelde verwerkingen van persoonsgegevens. Tevens kunt u door middel van dit formulier wijzigingen op een eerder gedane WBP-melding doorgeven.

De melding dient te geschieden door of namens de verantwoordelijke. Zijn er meer verantwoordelijken, dan moet de melding geschieden door of namens elk van de betrokken verantwoordelijken. Vergeet u niet in bovenstaand invulvak aan te geven of het een eerste melding onder de WBP of een mutatie inclusief meldingsnummer betreft.

Vraag 1

Verantwoordelijke

*De antwoordvelden die zijn voorzien van een * moeten altijd worden ingevuld.*

De verantwoordelijke is degene die het doel en de middelen voor de verwerking vaststelt. Dit kan een rechtspersoon of bestuursorgaan of een natuurlijk persoon zijn. Indien er meerdere verantwoordelijken voor een melding zijn, dienen deze apart opgegeven te worden.

| TOELICHTING VRAAG 1 | *Wie is de verantwoordelijke?* | *Voorbeelden* | *Meerdere verantwoordelijken* | *SBI-nummer* | *Vestiging verantwoordelijke in Nederland* |

1.1 **Hoeveel verantwoordelijken zijn er voor deze verwerking?** *Om meer dan één verantwoordelijke te kunnen melden, dient u deze bladzijde oningevuld evenzoveel maal te kopiëren als er verantwoordelijken zijn.*

● 1 | *ga naar vraag 1.3* |

○ meer dan 1, namelijk | | *kopieer de bladzijde* |

1.2 **Voor welk deel van de verwerking is de onderstaande (mede) verantwoordelijke verantwoordelijk?**

1.3 **De verantwoordelijke is:** *Slechts één van beide categorieën invullen.*

● **Een rechtspersoon of bestuursorgaan**

Naam*	Coca-Cola Enterprises Nederland B.V.
Adres*	Watermanweg 30
Postcode en plaats*	3067GG Rotterdam
Land*	Nederland
Postbus	3775
Postcode en plaats	3009AT Rotterdam
Land	Nederland
Telefoonnummer*	0102455156
Faxnummer	0102455537
E-mailadres	
SBI-nummer	

○ **Een natuurlijk persoon**

Achternaam*	
Voorvoegsel(s)	
Voorletter(s)*	
De heer of mevrouw*	○ M ○ V
Adres*	
Postcode en plaats*	
Land*	
Postbus	
Postcode en plaats	
Land	
Telefoonnummer*	
Faxnummer	
E-mailadres	
SBI-nummer	

Vraag 2

Contactpersoon

*De antwoordvelden die zijn voorzien van een * moeten altijd worden ingevuld.*

Bij deze vraag moet u aangeven wie de contactpersoon is voor deze melding. Alle correspondentie over de melding zal naar de contactpersoon worden gestuurd. Het CBP neemt ook contact op met deze persoon indien er vragen zijn over de melding.

| TOELICHTING VRAAG 2 | *Contactpersoon* |

2.1

Wie is de contactpersoon voor deze melding?

Achternaam*	Sturms
Voorvoegsel(s)	
Voorletter(s)*	K H
De heer of mevrouw*	O M ● V
Organisatie*	Coca-Cola Enterprises Nederland B.V.
Afdeling	Legal
Functie*	Legal Counsel
Adres*	Waterman weg 30
Postcode*	3067 GG
Plaats*	Rotterdam
Postbus	8775
Postcode	3009 AT
Plaats	Rotterdam
Telefoonnummer*	0 10 245 55 65 6
Faxnummer	0 10 245 55 53 7
E-mailadres	

Vraag 3

Bewerker

Een bewerker is een persoon of organisatie aan wie de verantwoordelijke de verwerking van persoonsgegevens heeft uitbesteed. Het invullen van deze vraag is niet verplicht, maar is wel van belang om inzicht te krijgen in de wijze waarop de verwerking verloopt. Indien er meerdere bewerkers voor een melding zijn, dienen deze apart opgegeven te worden.

*De antwoordvelden die zijn voorzien van een * moeten altijd worden ingevuld, als u de bewerker meldt.*

| TOELICHTING VRAAG 3 | *Bewerker* | *Meerdere bewerkers* |

3.1

Door hoeveel bewerkers worden de persoonsgegevens die in deze melding worden beschreven, verwerkt?
Om meer dan één bewerker te kunnen melden, dient u deze bladzijde oningevuld evenzoveel maal te kopiëren als er bewerkers zijn.

- ○ geen | *ga naar vraag 4* |
- ● 1 | *ga naar vraag 3.2* |
- ○ meer dan 1, namelijk | *kopieer de bladzijde* |

3.2

De bewerker is: *Slechts één van beide categorieën invullen.*

● **Een rechtspersoon of bestuursorgaan**

Naam*	Touch Incentive Marketing B.V.
Adres*	Triathlonstraat 17
Postcode*	3079HX Rotterdam
Plaats*	Rotterdam
Land*	Nederland
Postbus	
Postcode	
Plaats	
Land	
Telefoonnummer*	0102926666
Faxnummer	
E-mailadres	

○ **Een natuurlijk persoon**

Achternaam*	
Voorvoegsel(s)	
Voorletters*	
De heer of mevrouw*	○ M ○ V
Adres*	
Postcode*	
Plaats *	
Land*	
Postbus	
Postcode	
Plaats	
Land	
Telefoonnummer*	
Faxnummer	

Vraag 4

Wat meldt u aan?

Hier dient de verwerking van persoonsgegevens omschreven te worden. Dat kan door de naam van de verwerking of het systeem te vermelden zoals deze binnen de organisatie(s) van de verantwoordelijke(n) bekend is, bijvoorbeeld 'personeelsadministratie' of 'klachtenregistratie'.

| TOELICHTING VRAAG 4 | *Wat moet u melden?* | *Incidentele verwerking* |

4.1

Hoe luidt de naam of de omschrijving van de verwerking van persoonsgegevens?
Maximaal 1 verwerking van persoonsgegevens per formulier melden.

1 | Klantenbestand

Vraag 5

Het doel van de verwerking

Er kunnen meerdere doelen omschreven worden.
Let op: het doel of de doelen moet(en) betrekking hebben op de bij vraag 4.1 ingevulde naam of omschrijving van de verwerking.

Een precieze en duidelijke omschrijving van het doel (of de samenhangende doeleinden) van de verwerking is van belang, omdat aan de hand van het doel van de verwerking de hoeveelheid, de soort, de kwaliteit en de bewaartermijn van de gegevens worden getoetst.

| TOELICHTING VRAAG 5 | *Doel of doeleinden van de verwerking* | *Voorbeelden* | *Meerdere doeleinden* |

5.1

Voor welk doel of voor welke samenhangende doeleinden verwerkt de verantwoordelijke persoonsgegevens?

1 | Uitvoeren van overeenkomst met klant
2 | Versturen van informatie over verantwoordelijke en producten van de verantwoordelijke waaronder promotionele acties
3 | Doen van marktonderzoek en onderzoek naar positie van klanten.
4 | Verzamelen van informatie over klanten en het opstellen van profielen van klanten (o.b. naar regio, markt, specifieke producten).
5 | Onderhouden van contacten met klanten en voeren van correspondentie
6 | Versturen van informatie over derden en producten van derden aan klanten
7 | Administratie van debiteuren in verband met leveringen
8 |
9 |
10 |

Vraag 6

Categorieën van betrokkenen

Indien er meerdere categorieën van betrokkenen zijn, dan dienen alle categorieën van betrokkenen apart volgens de opzet van vraag 6 opgegeven te worden. De oningevulde bladzijden met vraag 6.1 t/m 6.5 kunnen daarvoor zo vaak als nodig gekopieerd worden en dan voorzien worden van een opeenvolgende letter, beginnend bij een A. Per letter mag maar één categorie van betrokkenen gemeld worden. Bij vraag 6.5 kunt u meerdere antwoorden aankruisen.

Bij deze vraag dient u aan te geven over wie persoonsgegevens worden verwerkt ('de betrokkenen'), welke soorten van gegevens er per categorie van betrokkenen worden verwerkt en voor welk doel of doelen de omschreven soorten van gegevens zijn verzameld. Tevens wordt gevraagd of er zogenaamde 'bijzondere persoonsgegevens' worden verwerkt. Verwerking hiervan is alleen toegestaan in een aantal expliciet in de WBP opgesomde gevallen.

| **TOELICHTING VRAAG 6** | *Algemeen* | **VRAAG 6.2** | *Categorie van betrokkenen* | *Meerdere categorieën van betrokkenen* | **VRAAG 6.3** | *Persoonsgegevens* | **VRAAG 6.4** | *Doel van het verzamelen van persoonsgegevens* | **VRAAG 6.5** | *Bijzondere persoonsgegevens* |

6.1 **Hoeveel categorieën van betrokkenen zijn er voor deze verwerking?**

● 1 | *ga naar vraag 6.2* |

○ meer dan 1, namelijk | | | *kopieer de bladzijden* |

6.2 **Over welke categorie van betrokkenen verwerkt u gegevens?** *Let op: de categorie van betrokkenen moet betrekking hebben op de bij vraag 4.1 ingevulde naam en het bij vraag 5.1 ingevulde doel van de verwerking.*

Klanten

6.3 **Welke gegevens of categorieën van gegevens die betrekking hebben op de genoemde categorie van betrokkenen (*vraag 6.2*) worden verwerkt?**

1	naw. gegevens klant	11	
2	naam en contactgegevens	12	
3	contactpersoon (tel.nr/fax/e-mail)	13	
4	bedrijfsgegevens	14	
5		15	
6		16	
7		17	
8		18	
9		19	
10		20	

6.4 **Voor welk doel of samenhangende doeleinden zijn/worden de (categorieën van) gegevens die zijn ingevuld bij vraag 6.3, verzameld?** *De nummering correspondeert met die van vraag 6.3.*

1 | alle doeleinden onder 5.1

2 | alle doeleinden onder 5.1.

3 | (en onderzoek)
doen van marktonderzoek naar de positie van klanten
verzamelen van informatie over klanten opstellen van profielen klantkan

4 |

5 |

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

6.5 **Welke bijzondere gegevens die betrekking hebben op de genoemde categorie van betrokkenen worden verwerkt?**

- ● Geen | *ga naar vraag 7* |
- ○ Gegevens betreffende godsdienst en levensovertuiging
- ○ Gegevens betreffende ras of etniciteit
- ○ Gegevens betreffende politieke gezindheid
- ○ Gegevens betreffende de gezondheid
- ○ Gegevens betreffende het sexuele leven
- ○ Gegevens betreffende het lidmaatschap van een vakvereniging
- ○ Strafrechtelijke gegevens
- ○ Gegevens betreffende onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag

Vraag 7

Verstrekking van gegevens

U kunt hier meerdere categorieën van ontvangers invullen.

Bij deze vraag moet worden ingevuld aan welke ontvangers of categorieën van ontvangers de gegevens worden verstrekt. De WBP verstaat onder het begrip ontvanger: degene aan wie de persoonsgegevens worden verstrekt.

| **TOELICHTING VRAAG 7** | *Ontvanger* | *Degenen die belast zijn met de verwerking van de gegevens* | *Leidinggevenden* | *Bewerker* | *Wettelijke verplichtingen tot verstrekking* |

7.1

Aan welke ontvangers of categorieën van ontvangers worden de gegevens verstrekt?

1 | Leidinggevenden op de afdeling Commercie
2 | Groepsmaatschappijen van de verantwoordelijke
3 | Enkele bravoerijen die contactgegevens van klanten van
4 | de verantwoordelijke ontvangen
5 | Zakelijke relaties, zoals Grouthandels, die contactgegevens
6 | van klanten, zoals horecagelegenheden, van de verantwoordelijke
7 | ontvangen
8 | Touch Incentive Marketing B.V.
9 |
10 |
11 |
12 |
13 |
14 |
15 |
16 |
17 |
18 |
19 |
20 |

Vraag 8

Beveiliging van persoonsgegevens

Bij vragen 8.2 en 8.4 tot en met 8.6 kunt u meerdere antwoorden aankruisen.

Deze vraag is bedoeld om het CBP een indruk te geven van de beveiligingsmaatregelen. De door u ingevulde gegevens worden niet in het openbaar meldingenregister geplaatst.

| TOELICHTING VRAAG 8 | *Beveiliging van de gegevens* |

8.1

Beveiligt u de persoonsgegevens?

- ○ Nee | *ga naar vraag 9* |
- ● Ja

8.2

Welke maatregelen heeft u genomen om de persoonsgegevens te beschermen?

- ○ Vastgesteld beveiligingsbeleid dat ook is geïmplementeerd
- ○ Fysieke maatregelen voor toegangsbeveiliging, inclusief organisatorische controle
- ○ Inbraakalarm
- ○ Kluis voor opslag van gegevensbestanden
- ● Logische toegangscontrole m.b.v. iets wat iemand weet (wachtwoord of pincode)
- ○ Logische toegangscontrole m.b.v. iets wat iemand bij zich draagt (pasje)
- ○ Logische toegangscontrole m.b.v. iets wat bij iemand hoort (biometrisch kenmerk)
- ○ Overige logische toegangscontrole
- ○ Automatische logging van toegang tot gegevens, incl. een controleprocedure
- ○ Controle van toegekende bevoegdheden
- ○ Overige beveiligingsmaatregelen | *a.u.b. specificeren* |

8.3

Is er sprake van een bewerker? *Slechts één antwoord mogelijk.*

- ○ Nee
- ● Ja, en er zijn met de bewerker(s), d.w.z. met elke bewerker, schriftelijke afspraken gemaakt over beveiliging
- ○ Ja, en er zijn géén schriftelijke afspraken over beveiliging gemaakt met de bewerker of met één van de bewerkers

8.4

Wie heeft toegang tot de persoonsgegevens?

- ● Personeel dat onder leiding van de verantwoordelijke staat
- ● Personeel dat onder leiding van de bewerker staat
- ● Derden | *a.u.b. specificeren* | Zie vraag 7.1

8.5

Verzendt u gegevens langs elektronische weg?

- ○ Nee
- ● Ja, via een eigen netwerk
- ○ Ja, via een publiek netwerk

8.6

Gebruikt u encryptie?

- ○ Ja, de persoonsgegevens worden versleuteld tijdens verzending
- ○ Ja, de gegevensopslag is versleuteld
- ● Nee

Vraag 9

Doorgifte naar landen buiten de Europese Unie

Deze vragen gaan over doorgifte van gegevens naar landen buiten de Europese Unie.
N.B.: doorgifte naar landen buiten de Europese Unie is alleen toegestaan in bepaalde gevallen. Zie de toelichting.

| **TOELICHTING VRAAG 9** | *Doorgifte van persoonsgegevens binnen de Europese Unie* | *Doorgifte van persoonsgegevens naar landen buiten de Europese Unie* |

9.1 **Geeft u bij uw gegevensverwerking persoonsgegevens door naar één of meer landen buiten de Europese Unie?**

- ○ Nee | *ga naar vraag 10* |
- ● Ja

9.2 **Worden persoonsgegevens uitsluitend doorgegeven naar landen buiten de Europese Unie waarvan de Minister van Justitie heeft bepaald dat die landen een passend beschermingsniveau waarborgen?**

- ● Nee, maar uitsluitend aan Groepsmaatschappij in VS
- ○ Ja

Vraag 10

Voorafgaand onderzoek

Voor een beperkt aantal categorieën van gegevensverwerkingen vereist de WBP dat er, voordat u met de verwerking start, een onderzoek plaatsvindt: het voorafgaand onderzoek. Het gaat daarbij om gegevensverwerkingen die specifieke risico's met zich meebrengen voor de rechten en vrijheden van de betrokkenen.
Aan de hand van onderstaande vragen kunt u bepalen of daarvan sprake is.
N.B.: de inlichtingen die zijn verkregen aan de hand van deze vragen worden niet in het openbaar meldingenregister geplaatst.

| TOELICHTING VRAAG 10 | *Algemeen* | *Nader onderzoek?* | *Opschorting van de gegevensverwerking* | *Persoonlijk identificatienummer* | *Heimelijke waarneming* | *Strafrechtelijke gegevens en gegevens over hinderlijk of onrechtmatig gedrag* |

Bij vraag 10.4 moet u de juiste conclusie aankruisen.

10.1.A

Bent u van plan om een <u>persoonlijk identificatienummer</u> van de betrokkene(n) te verwerken voor een <u>ander doel</u> dan waarvoor het nummer specifiek is bestemd, met het doel de gegevens in verband te brengen (te koppelen) met gegevens die door een andere verantwoordelijke worden verwerkt?

● Nee | *ga naar vraag 10.2* |
○ Ja | *ga naar vraag 10.1.B* |

10.1.B

Is het persoonlijk identificatienummer voorgeschreven bij wet en gebruikt u het nummer alleen ter uitvoering van die wet of een andere wet?

○ Nee | *ga naar vraag 10.2* |
○ Ja | *ga naar vraag 10.2* |

10.2

Bent u van plan gegevens van de betrokkene(n) vast te leggen die u door <u>eigen waarneming</u> hebt verkregen, <u>zonder</u> de betrokkene(n) van die vastlegging op de hoogte te stellen?

● Nee | *ga naar vraag 10.3.A* |
○ Ja | *ga naar vraag 10.3.A* |

10.3.A

Bent u van plan <u>voor derden</u> strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag van de betrokkene(n) te verwerken?

● Nee | *ga naar vraag 10.4* |
○ Ja | *ga naar vraag 10.3.B* |

10.3.B

Heeft u een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus?

● Nee | *ga naar vraag 10.4* |
○ Ja | *ga naar vraag 10.4* |

10.4

Wat is de conclusie aan de hand van bovenstaande vragen?
Voor het bepalen van de juiste conclusie geldt onderstaande keuzetabel.

vraag 10.1.B	=	Nee	en/of	in alle overige gevallen
vraag 10.2	=	Ja	en/of	
vraag 10.3.B	=	Nee		

Conclusie 1

○ **U vraagt het CBP om een voorafgaand onderzoek.**
Dit verzoek geschiedt automatisch door het aankruisen van dit hokje en het inzenden van dit formulier.

Conclusie 2

● **U vraagt het CBP niet om een voorafgaand onderzoek.**

Ondergetekende verklaart bevoegd te zijn tot het doen van deze melding en dat de in de melding verstrekte inlichtingen juist zijn.

Alle velden moeten worden ingevuld.

Naam | K.M. Sturms

Functie | legal counsel

Plaats | Rotterdam

Datum | 07-10-2012

Handtekening | K. Sturms

Dit formulier na invulling en ondertekening zenden aan het CBP, t.a.v. Afdeling Bestandsbeheer, Postbus 93374, 2509 AJ Den Haag.

Let op: u dient het meldingsformulier op te sturen, voorzien van de handtekening van de verantwoordelijke(n) of een persoon die door de verantwoordelijke(n) is gemachtigd. Zonder een volledig ingevuld en ondertekend meldingsformulier kan de melding niet als verricht beschouwd worden.

Bijlage 5: brief van het ministerie 20 oktober 2014

Dienst Justis
Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20300 2500 EH Den Haag

Aan Coca-Cola Enterprises Nederland B.V.
T.a.v. de heer/mevrouw K. van der Kwast
Postbus 8775
3009 AT ROTTERDAM

Justitiële uitvoeringsdienst Toetsing, Integriteit en Screening
Verlening & Toetsing (V&T)

Postbus 20300
2500 EH Den Haag
www.justis.nl

Contactpersoon
Klant Contact Centrum
T 088 998 2288
F 070 370 6047
frontdesk.justis@minvenj.nl

Ons kenmerk
WBP 1200055

Uw kenmerk
-

Bijlagen
-

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen?

Datum 20 oktober 2014
Onderwerp Vergunning artikel 77, lid 2, Wbp

Geachte heer/mevrouw Van der Kwast,

Op 15 oktober 2014 heb ik uw aanvraag van 2 oktober 2014 ontvangen. U vraagt "Coca-Cola Enterprises Nederland B.V." een vergunning als bedoeld in art 77, tweede lid, van de Wet bescherming persoonsgegevens, voor de doorgifte van persoonsgegevens aan "Capgemini India Private Limited", gevestigd te Mumbay, India. Ik heb besloten uw aanvraag toe te wijzen. Hieronder kunt u lezen hoe ik tot deze beslissing ben gekomen.

Voorgeschiedenis

- Het College bescherming persoonsgegevens (CBP) heeft mij uw aanvraag op 14 oktober 2014 toegezonden;
- "Coca-Cola Enterprises Nederland B.V.", gevestigd te Rotterdam en "Capgemini India Private Limited", gevestigd te Mumbay, India hebben de bij bovengenoemd advies van het CBP gevoegde "Application form for a permit as defined in article 77.2 Wet bescherming persoonsgegevens (Wbp)" ingevuld en ondertekend;
- Tussen voornoemde partijen is een overeenkomst gesloten (hierna Overeenkomst) die is opgesteld op basis van de modelcontractsbepalingen vastgelegd in de Beschikking van de Europese Commissie betreffende modelcontractsbepalingen voor de doorgifte van persoonsgegevens naar derde landen krachtens Richtlijn 95/46/EG (2010/87/EU);
- De Overeenkomst is gevoegd bij bovengenoemd advies van het CBP;

Relevante regelgeving

Artikel 77, tweede lid, van de Wet bescherming persoonsgegevens bepaalt dat de minister, gehoord het College bescherming persoonsgegevens, een vergunning kan geven voor een doorgifte of een categorie doorgiften van persoonsgegevens naar een derde land dat geen waarborgen voor een passend beschermingsniveau biedt. Aan de vergunning worden de nadere voorschriften verbonden die nodig zijn om de bescherming van de persoonlijke levenssfeer en de fundamentele rechten en vrijheden van personen, alsmede de uitoefening van de daarmee verband houdende rechten te waarborgen.

Relevante feiten en omstandigheden
Het CBP heeft op 14 oktober 2014 positief geadviseerd ten aanzien van de vergunningaanvraag.

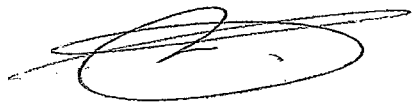
Beoordeling
Uw aanvraag voldoet aan alle voorwaarden. Daarom zal ik uw aanvraag toewijzen.

Beslissing
Ik wijs uw aanvraag toe.

Ik verleen "Coca-Cola Enterprises Nederland B.V.", gevestigd te Rotterdam, toestemming voor de doorgifte van de categorieën persoonsgegevens van de categorieën personen zoals aangegeven in het aanvraagformulier van 2 oktober 2014 aan "Capgemini India Private Limited", gevestigd te Mumbay, India. De toestemming voor de doorgifte verleen ik voor het in vorengenoemde aanvraagformulier aangegeven doel en de daarin aangegeven periode, conform de Overeenkomst.

Eventuele wijzigingen van naam en adres van de verschillende ondernemingen dient u terstond aan mij door te geven.
Indien zich wijzigingen in de doorgifte van persoonsgegevens voordoen dient u daarvoor opnieuw vergunning aan te vragen.

Hoogachtend,
De Staatssecretaris van Veiligheid en Justitie,
namens deze,



S.M.A.C. van Weert
Afdelingsmanager V&T

Bezwaar maken
U kunt bij de Staatssecretaris van Veiligheid en Justitie tegen deze beslissing bezwaar maken. U doet dit door een gemotiveerd bezwaarschrift in te dienen binnen zes weken na bekendmaking van deze beslissing. U kunt uw bezwaarschrift sturen naar het volgende adres:

Dienst Justis
Afdeling V&T
Postbus 20300
2500 EH Den Haag

U kunt uw bezwaarschrift ook door uw gemachtigde laten indienen. Als de gemachtigde geen advocaat is, voeg dan een machtiging bij uw bezwaarschrift.

Zorg ervoor dat uw bezwaarschrift in elk geval het volgende bevat:

- uw naam en adres;
- de datum waarop u het bezwaarschrift schrijft;
- een omschrijving van de beslissing waartegen u bezwaar wilt maken. U kunt ook een kopie van de beslissing meesturen;
- de gronden van uw bezwaar;
- uw handtekening of de handtekening van uw gemachtigde.

Voor meer informatie kunt u op www.rijksoverheid.nl de brochure "Bezwaar en beroep tegen beslissingen van de overheid" downloaden.

Bijlage 6: Vergunning voor data uitwisselen met de VS

Justitie

Ministerie van Justitie

Dienst Justis
Justitiële uitvoeringsdienst Toetsing, Integriteit en Screening

Postadres Postbus 20300, 2500 EH Den Haag

Bezoekadres
Juliana van Stolberglaan 10
2595 CL Den Haag
Telefoon (070) 3 70 45 42
Fax (070) 3 70 60 47

Aan Coca Cola Enterprises Nederland B.V.
T.a.v. mevrouw K. van der Kwast
Postbus 8775
3009 AT Rotterdam

Onderdeel: Team Bevoegdheven, Toetsing en Registers (BTR)
Contactpersoon: Mw. P.M.T. Damsteeg
Doorkiesnummer(s): 070 -370 4542
Datum: 20 februari 2009
Ons kenmerk: WBP 0900001
Bijlage(n): 1
Onderwerp: Vergunning in de zin van artikel 77, lid 2 Wbp

Bij beantwoording de datum en ons kenmerk vermelden.

Geachte mevrouw Van der Kwast,

Met verwijzing naar uw verzoek van 19 februari 2008 zend ik u hierbij mijn beschikking van vandaag, betreffende het verlenen van een vergunning op grond van artikel 77, tweede lid van de Wet bescherming persoonsgegevens aan "Coca-Cola Enterprises Nederland B.V.", gevestigd te Rotterdam, voor het doorgeven van persoonsgegevens aan "Coca-Cola Enterprises Inc.", gevestigd in de Verenigde Staten van Amerika.

Eventuele wijzigingen van naam en adres van de verschillende ondernemingen dient u terstond aan mij door te geven. Indien zich wijzigingen in de doorgifte van persoonsgegevens voordoen dient u daarvoor opnieuw vergunning aan te vragen.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

De Minister van Justitie,
namens deze,
de teammanager BTR,

P.W.C. Collard

Justitie

Ministerie van Justitie

Dienst Justis

Justitiële uitvoeringsdienst Toetsing, Integriteit en Screening

WBP 0900001

DE MINISTER VAN JUSTITIE

Gezien het door het College Bescherming Persoonsgegevens ontvangen verzoek d.d. 19 februari 2008 van "Coca-Cola Enterprises Nederland B.V.", gevestigd te Rotterdam, om een vergunning als bedoeld in art 77, tweede lid van de Wet bescherming persoonsgegevens, voor de doorgifte van persoonsgegevens aan "Coca-Cola Enterprises Inc.", gevestigd in de Verenigde Staten van Amerika;

Gezien het advies d.d. 8 januari 2009 van het College Bescherming Persoonsgegevens (CBP);

Gezien het door beide partijen ingevulde en ondertekende "Application form for a permit as defined in article 77.2 Wet bescherming persoonsgegevens (Wbp)" zoals dat bij bovengenoemd advies van het CBP is gevoegd;

Gezien de tussen de partijen gesloten overeenkomst die is opgesteld op basis van de modelcontractsbepalingen vastgelegd in de Beschikking van de Europese Commissie betreffende modelcontractsbepalingen voor de doorgifte van persoonsgegevens naar derde landen krachtens Richtlijn 95/46/EG (2001/497/EG), zoals die bij bovengenoemd advies van het CBP is gevoegd;

Overwegende dat het CBP positief heeft geadviseerd ten aanzien van de vergunningaanvraag;

BESLUIT

"Coca-Cola Enterprises Nederland B.V.", gevestigd te Rotterdam, toestemming te verlenen voor de doorgifte van de in het bovengenoemde aanvraagformulier aangegeven categorieën persoonsgegevens van de daarin aangegeven categorieën personen aan "Coca-Cola Enterprises Inc.", gevestigd in de Verenigde Staten van Amerika voor het in het aanvraagformulier aangegeven doel en de daarin aangegeven periode, conform de bovengenoemde overeenkomst;

Den Haag, 20 februari 2009,

De Minister van Justitie,
namens de Minister,
de teammanager BTR,

P.W.C. Collard

Justitie

Bezwaar

Eenieder die door een beschikking rechtstreeks in zijn belangen is getroffen kan hiertegen ingevolge de Algemene wet bestuursrecht bezwaar maken. Ingevolge de artikelen 6:7 en 6:8 van deze wet kan een gemotiveerd bezwaarschrift worden ingediend binnen zes weken na de dag waarop de beschikking bekend is gemaakt. Dit bezwaarschrift dient te worden gericht aan het Ministerie van Justitie, Dienst Justis, Postbus 20300, 2500 EH te Den Haag.

Bijlage 7: Policy voor Acceptabel IT-gebruik

Coca-Cola Enterprises, Inc.

Policy voor Acceptabel IT-gebruik

Datum:	27 januari 2015	Release:	1
Auteur:	IT Governance, Risk and Compliance		
Eigenaar:	IT Governance, Risk and Compliance		
IT-gebied:	Naleving	**Doelgroep:** Alle medewerkers	

Versie	Datum van revisie	Beschrijving van revisie	Auteur	Goedkeuring
1	27 januari 2015	Archiveren van e-mails toegevoegd	IT GRC	IT Security

Coca-Cola Enterprises, Inc.

Inhoud

1. Inleiding

1.1. Doel

Coca-Cola Enterprises Inc. (CCE of het 'Bedrijf') heeft een Policy voor Acceptabel IT-gebruik vastgelegd waarin de doelstellingen van het Bedrijf voor het beheer van het programma rond voorlichting met betrekking tot gegevensbeveiliging zijn bepaald om de informatiemiddelen van ons Bedrijf te helpen beschermen. In het beleid wordt bepaald dat het gegevensbeveiligingsprogramma ervoor moet zorgen dat het handvest van het CCE-gegevensbeveiligingsprogramma en de bijbehorende beleidsmaatregelen, normen, richtlijnen en procedures goed worden doorgegeven en door iedereen goed worden begrepen door een programma rond voorlichting met betrekking tot de beveiliging van gegevens op te zetten. Een doeltreffend programma rond voorlichting met betrekking tot gegevensbeveiliging is essentieel voor het welslagen van de initiatieven voor ondernemingsbeveiliging, omdat het kan helpen om gewenst gedrag te bekrachtigen en ongewenst gedrag bij te sturen om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatiemiddelen van CCE te helpen beschermen.

Daarnaast omvat dit beleid regels en richtlijnen om je te helpen meer te begrijpen over wat je wel en niet mag doen bij het gebruik van het CCE-intranet, internet en e-mail van vestigingen en kantoren van CCE, en bij het thuis gebruiken van apparatuur, software, telefoonapparatuur en laptops (of pc's) van CCE. Het is echter geen uitputtend of definitief overzicht van wat je wel en niet kunt doen en je moet je te allen tijde op een betrouwbare en passende manier gedragen, zodat je CCE of haar medewerkers niet in diskrediet brengt of schaadt.

1.2. Omvang

Alle medewerkers, deeltijds medewerkers en uitzendkrachten, externe aannemers, leveranciers en agenten die toegang hebben tot de systemen van het Bedrijf, alsook hun management, vallen onder de *Policy voor acceptabel IT-gebruik* en moeten de bijbehorende procedures en richtlijnen naleven.

2. Vereisten

2.1. Persoonlijk gebruik

Soms kan het nodig zijn om internet voor persoonlijke zaken te gebruiken en deze praktijk is aanvaardbaar, mits het persoonlijk gebruik:

- redelijk en beperkt is;
- geen invloed heeft op de uitvoering van je taken of die van je collega's en deze ook niet verstoort;
- vooral plaatsvindt in je eigen tijd (hoewel een snelle en redelijke toegang tijdens de werktijd acceptabel is).

Toegang tot internet via de systemen van CCE is niet ontworpen voor zwaar persoonlijk gebruik, bijv. het opzetten en beheren van een persoonlijke website, webpagina, persoonlijk profiel op sociale netwerksites en blogs.

2.2. Apparatuur

CCE stelt de apparatuur die je nodig hebt om je werk uit te voeren ter beschikking, maar het is soms mogelijk, voor zover dat wettelijk toegestaan is, dat je je eigen apparatuur gebruikt om werk uit te voeren voor CCE.

2.2.1. Geleverd door het Bedrijf

Het kan gaan om desktop- of mobiele apparatuur. Mobiele computer- en opslagapparaten omvatten, maar zijn niet beperkt tot, laptopcomputers, mobiele telefoons en smartphones, PDA's, plug-ins, Universal Serial Bus-poortapparaten (USB), Compact Discs (cd's), Digital Versatile Discs (dvd's), flash-schijven, modems, draadloze handheldapparaten, draadloze netwerkkaarten en alle andere bestaande of toekomstige mobiele computer- of opslagapparatuur in persoonlijk bezit of eigendom van het Bedrijf die verbonden kan worden met of toegang kan krijgen tot de informatiesystemen van het bedrijf (de 'Mobiele computerapparatuur').

2.2.2. Apparatuur in eigen bezit

Persoonlijke mobiele computerapparaten mag worden gebruikt om verbinding te maken met het netwerk van CCE, zolang deze wordt gescand om ervoor te zorgen dat ze veilig zijn voor gebruik en vooraf goedgekeurd door de Europese Support Desk.

CCE verleent geen steun voor enige mobiele computerapparatuur in eigen bezit.

2.2.3. Verloren of gestolen apparatuur

Als je apparatuur verloren of gestolen is, moet je dit onmiddellijk melden aan je lijnmanager en Field IT-contactpersoon.

2.3. Veiligheid

Bij CCE gebruiken we controles om het risico op fraude te voorkomen en ons netwerk, onze gegevens en onze toepassingen te beschermen. We moeten er ook op kunnen rekenen dat ons netwerk en ons communicatiesystemen optimaal werken.

Opmerking: Open geen websites op het internet die grote foto- of videobestanden bevatten, want dit kan de netwerkprestaties negatief beïnvloeden.

Om toegang te krijgen tot ons netwerk krijg je een persoonlijk wachtwoord en gebruikersnaam. Je moet ook een wachtwoord instellen om elk mobiele computerapparaat te beschermen, zodat het niet kan worden geopend zonder een dergelijk wachtwoord. Wachtwoorden en gebruikersnamen zijn ontworpen om de informatie van het Bedrijf te beschermen tegen onbevoegde toegang.

Je bent verantwoordelijk voor het beschermen van je wachtwoord en mag dit met niemand anders binnen of buiten CCE delen.

- Het is strikt verboden de identiteit of het wachtwoord van iemand anders te gebruiken om toegang te verkrijgen tot het internet of het e-mail- of intranetsysteem van CCE.
- Je moet de informatie die je krijgt beschermen, dus is het volgende niet toegestaan:
    - acties ondernemen die het functioneren van het systeem direct of indirect kunnen veranderen, verstoren of wijzigen;
    - bijlagen openen die per e-mail verzonden zijn, afkomstig van een onbekende afzender
    - het internet aan laten staan wanneer je het niet gebruikt, of het op de achtergrond laten draaien.

Als je vermoedt dat je apparatuur geïnfecteerd is met een virus, moet je je Field IT- of Helpdesk-contactpersoon onmiddellijk op de hoogte brengen.

2.3.1. Beveiligingsincidenten melden

Als je op de hoogte bent van een beveiligingszwakte, -kwetsbaarheid of -incident of deze/dit vermoedt, dien je dit onmiddellijk via e-mail te melden aan het Computer Incident Response Team (CIRT) op ccecirt@cokecce.com.

2.4. Toezicht op gebruik

CCE kan toezicht houden op de systemen die van het Bedrijf zijn en op de informatie die door het netwerk gaat (d.w.z. navigatie op internet/verzenden en ontvangen van e-mails en berichten) en het gebruik door medewerkers van een systeem of informatie van het Bedrijf (afhankelijk van de toepasselijke lokale wetgeving). Verwijzingen naar medewerkers in dit beleid gelden ook voor alle andere personen die voor of namens CCE werken.

CCE behoudt zich het recht voor om de mate van gebruik van de e-mails van CCE en internet van de medewerkers te controleren in overeenstemming met de plaatselijke wetgeving om:

- de effectieve en/of veilige werking van alle systemen te waarborgen
- transacties vast te leggen waarbij het Bedrijf betrokken is
- ervoor te zorgen dat de medewerkers zich houden aan de geldende wetten en de richtlijnen of procedures van het Bedrijf

Er zal toezicht worden uitgevoerd met behulp van de procedures van het Bedrijf en in overeenstemming met de lokale wetgeving. Gegevens verzameld als gevolg van de bewakingsactiviteiten worden verwerkt in overeenstemming met de toepasselijke wetgeving en mogen buiten het Bedrijf worden bekendgemaakt ter ondersteuning of als onderdeel van de officiële onderzoeken of juridische procedures. Communicatie via hardwareapparatuur in handen van het Bedrijf of in eigen bezit waarop Bedrijfsinformatie staat of verwerkt wordt, is niet privé, tenzij anders bepaald in de lokale wetgeving. Je toegang tot de informatiesystemen kan worden opgeschort als je je niet aan deze regels houdt en er kan een onderzoek plaatsvinden, wat zou kunnen leiden tot disciplinaire maatregelen.

Bepaalde websites worden geblokkeerd door de afdeling Corporate Security. Websites worden op gezette tijden geëvalueerd en kunnen op ieder moment zonder verdere aankondiging worden geblokkeerd. Als je toegang tot een dergelijke website probeert te krijgen, zal een CCE-bericht weergegeven worden met de melding dat de website is geblokkeerd.

2.5. Aanvaardbaar gebruik van internet, e-mail en sociale media

We maken in ons dagelijkse leven steeds meer gebruik van elektronische communicatie. Er zijn regels die je moet volgen wanneer je informatie verzendt of openbaar maakt (zowel binnen als buiten CCE) en wanneer je je toegang verschaft tot informatie of websites. Met name:

- Je bent verantwoordelijk voor veilig werken en moet vermijden dat je potentieel 'onveilige' websites bezoekt die ertoe kunnen leiden dat je een 'virus' binnenhaalt. Open bijvoorbeeld geen e-mailbijlagen tenzij je de bron kent en vertrouwt, aangezien onbekende bijlagen virussen kunnen bevatten.
- Je mag je professionele adres niet inschrijven op niet-professionele distributielijsten of je professionele e-mailadres niet delen voor niet-professionele doeleinden.
- Je mag geen websites bezoeken met materiaal dat kan worden beschouwd als gênant, discriminerend, seksueel expliciet, obsceen, intimiderend, lasterlijk, gewelddadig, 'volwassen' of frauduleus van aard.
- Je mag geen gebruik maken van internet, e-mail van CCE of sociale media om ongepaste activiteiten uit te voeren, waaronder, maar niet beperkt tot, dating, verzenden van ongepaste of beledigende grappen of kettingbrieven, spam, deelnemen in chatrooms. Het is ook strikt verboden om e-mails te verzenden die bedreigend of agressief, grof, asociaal, seksueel bevooroordeeld, obsceen of beledigend, racistisch, seksueel expliciet, pornografisch, gewelddadig, 'volwassen' of frauduleus van aard zijn. Bekijken, verzenden of downloaden van foto's van pornografische aard is verboden.
- Het Bedrijf tolereert geen discriminatie of intimidatie van welke aard dan ook. Je mag het intranet van CCE of de toegang tot internet niet gebruiken om materiaal te communiceren of door te sturen waarin wordt gediscrimineerd of waarin mensen worden aangezet tot discriminatie op grond van ras of etnische gronden of op grond van geslacht, seksuele geaardheid, burgerlijke staat, leeftijd, etnische afkomst, huidskleur, nationaliteit, ras, religie, geloof of handicap.
- Als je obsceen, onfatsoenlijk, beledigend, opruiend, lasterlijk, beledigend, gewelddadig, 'volwassen', frauduleus, discriminerend of sociaal aanstootgevend materiaal ontvangt of daarvan op de hoogte bent, moet je je manager dit meteen vertellen zodat passende maatregelen kunnen worden genomen. Als het niet passend is om het probleem te bespreken met je manager, kun je de zaak voorleggen aan het HeRe!- team.

- Je moet te allen tijde tijdens het gebruik van de CCE-systemen (e-mail, internet en intranet) het CCE-beleid inzake de concurrentiewet naleven (je kunt hierover meer informatie aanvragen bij je manager en/of de juridische afdeling).
- Het is niet toegestaan om toegang te krijgen of proberen te krijgen tot privé- of vertrouwelijke websites als je daarvoor geen aanmeldingsgegevens hebt.
- Je mag geen auteursrechtelijk beschermd of gelicentieerd materiaal (bijv. muziek, games of boeken) uploaden, downloaden of verspreiden.

- Je mag geen materiaal met betrekking tot CCE of verkregen van CCE, dat al dan niet vertrouwelijk is, publiceren op internet zonder eerst de toestemming te verkrijgen van de juridische afdeling van CCE en je lijnmanager.
- Als je per ongeluk toegang krijgt tot een ongepaste website, moet je direct contact opnemen met de IT-afdeling om je machine te laten controleren op 'cookies', enz.

2.5.1. Internet

CCE zal voorzien in internettoegang voor alle apparatuur met een Secure Access Zone (SAZ). Je mag geen commerciële internet serviceprovider gebruiken om van binnen het bedrijf toegang tot internet te verkrijgen. Bezoek ook geen websites met grote foto- of video-inhoud die de netwerkprestaties van CCE negatief kunnen beïnvloeden.

2.5.2. Sociale media

In specifieke omstandigheden kun je toegang verkrijgen tot sociale mediasites (bijv. sociale netwerken/Content Shares/discussiewebsites/microblogging, publicatie- en andere websites waarmee individuele gebruikers of bedrijven eenvoudige publicatiehulpmiddelen kunnen gebruiken), zodat je contact kunt opnemen met klanten, gemeenschappen en belanghebbenden of andere taken kunt uitvoeren die betrekking hebben op je functie bij CCE. Je mag geen opmerkingen over CCE of haar producten posten die niet zijn goedgekeurd door je lokale management. Je mag ook geen persoonlijke gegevens over jezelf of anderen delen in deze posts.

Acceptabele sociale mediahulpmiddelen bij CCE zijn, maar zijn niet beperkt tot:

- Sociale netwerken zoals Facebook, MySpace, Yammer en LinkedIn.
- Websites voor het delen van inhoud zoals Flickr, YouTube, Crowdstorm en LastFM
- Discussiewebsites zoals Google Groups en Yahoo! Groepen
- **Microbloggingsites** zoals Twitter, Identi.ca, Tumblr en Jaiku
- **Publicatiewebsites** waaronder blogs (gerund door particulieren, bedrijven en traditionele mediabedrijven) en online encyclopedieën zoals Wikipedia

2.5.3. Acceptabele Disclaimerverklaring

Als je toestemming hebt om op het werk sociale netwerksites te gebruiken, moet je de volgende verklaring toevoegen:
"De meningen in dit bericht zijn van mij en komen niet noodzakelijk overeen met de standpunten van Coca-Cola Enterprises, Inc."

2.5.4. Elektronische post

Als je een e-mail schrijft, moet je dit op dezelfde manier doen als wanneer je een brief opstelt of iets op een CCE-mededelingenbord zet (d.w.z. net zoals bij traditionele schriftelijke communicatie). Alle verklaringen die je via elektronische communicatie doet, kunnen juridisch bindend zijn.

Wel doen:

- Als je per abuis een e-mailbericht toegezonden krijgt met daarin geheime informatie, breng dan de afzender op de hoogte van de fout en verwijder het bericht.
- Als je een bericht ontvangt dat illegale of concurrentievervalsende, bedrijfsgerelateerde informatie of informatie die een overtreding is van de CCE-beleidsrichtlijnen of -procedures bevat, neem dan onmiddellijk contact op met een lid van het juridische team, of voor een schending van de Code of Business Conduct, met Compliance & Risk, die je zal helpen een geschikt antwoord (dat CCE zal beschermen) op te stellen.
- Volg te allen tijde de beleidsrichtlijnen en procedures van CCE
- Archiveringsregels voor emails- Wanneer dien je emails te bewaren :
  - **Om aan wettelijke verplichtingen te beantwoorden** - emails moeten worden bewaard worden in overeenstemming met de van toepassing zijnde lokale document retentie policy.
  - **Op uitdrukkelijk verzoek van het juridisch departement** - alle relevante bestanden en e-mails dienen onmiddellijk en blijvend te worden bewaard
  - **Om aan de kritische noden van het bedrijf te beantwoorden:**
  - Emails betreffende de interactie tussen interne of externe partijen die nodig is als bewijs of voor het begrijpen van de details van de gearchiveerde documenten.
  - E-mails met betrekking tot je hoedanigheid van medewerker van CCE (communicatie tussen manager en medewerker en tussen CCE HR en medewerker)

Niet doen:

- Beveiligingsgerelateerde berichten verzenden of doorsturen die niet zijn opgesteld door IT Security & Compliance, Corporate Internal Audit Department, Corporate Security of de Compliance & Risk (bijv. waarschuwingen over computervirussen), tenzij gedaan ter ondersteuning van een onderzoek
- Handmatige regels of regels voor automatisch doorsturen gebruiken om zakelijke e-mail van het bedrijf buiten het systeem te zenden
- Regels voor automatisch doorsturen worden gedefinieerd als alle instellingen in een e-mailsysteem die kunnen worden gebruikt voor het automatisch doorsturen van binnenkomende e-mail naar een ander e-mailadres
- Bedrijfsinformatie doorgeven via persoonlijke internetgebaseerde e-maildiensten (zoals Hotmail, Yahoo, Gmail, enz.)

2.6. Policy Schoon bureau

- Je moet vertrouwelijke bestanden en alle apparatuur (met name voor gebruikers van mobiele telefoons) veilig bewaren
- Alle geheime informatie moet worden beschermd, en geheime gegevens moeten voor het verzenden worden gecodeerd.
- Je mag geen IT-apparatuur (diskette, cd-rom, enz.) met vertrouwelijke gegevens achterlaten in een open kantoor. Vergeet niet gevoelige om documenten mee te nemen die moeten worden verzonden, afgedrukt of gekopieerd na gebruik van een fax, printer of kopieerapparaat
- Verwijder alle vertrouwelijke informatie uit printers, kopieerapparaten en faxapparaten.
- Tokens of wachtwoorden mogen niet worden opgeslagen in open gebieden die kunnen worden bekeken door anderen.

2.7. Policy Schoon scherm

Je moet een schermbeveiligingswachtwoord instellen, zodat je scherm wordt vergrendeld wanneer je de computer niet gebruikt. Vergrendel je werkstation voordat je je bureau verlaat (door op CTRL-ALT-DELETE te drukken en de optie Computer vergrendelen te kiezen).

2.8. Het bedrijf in diskrediet brengen

Als een internetsite die jij hebt opgezet of waartoe jij hebt bijgedragen (bijv. een pagina op een sociale netwerksite of een persoonlijke blog) of jouw gebruik van het internet het bedrijf in diskrediet brengt of in

diskrediet dreigt te brengen, of indien de reputatie van het bedrijf erdoor wordt geschaad, wordt dat beschouwd als een ernstige disciplinaire zaak die kan leiden tot ontslag, afhankelijk van de plaatselijke wetgeving. Hieronder kan worden verstaan het plaatsen van onbevoegde opmerkingen over CCE of haar producten.

2.9. Schending van beleid

Elke schending van de regels en richtlijnen die in dit beleid zijn uiteengezet, waaronder misbruik van het internet voor zakelijke en/of persoonlijke doeleinden of van het e-mailsysteem van CCE, zal worden beschouwd als een ernstige strafbare zaak en kan leiden tot weigering van internettoegang en/of disciplinaire maatregelen in overeenstemming met de lokale beleidsrichtlijnen en/of voorschriften.

2.10. Bewustzijn rond beveiliging

In het programma rond voorlichting met betrekking tot gegevensbeveiliging worden beleidslijnen en procedures rond gegevensbeveiliging doorgegeven die moeten worden gevolgd. De gebruikers moeten weten wat van hen wordt verwacht. Alleen als het personeel goed ingelicht en opgeleid is en zich bewust is van de regels, kan erop worden gerekend dat ze zich verantwoordelijk gedragen. Individuele medewerkers moeten vanaf hun introductie in het bedrijf tot op het moment dat ze het bedrijf verlaten goed op de hoogte zijn van hun verantwoordelijkheid op het vlak van beveiliging; dit moet goed geïntegreerd zijn in de cultuur van de organisatie. Iedereen met tijdelijke toegangsrechten tot informatiemiddelen en ook vaste medewerkers moeten bewustzijn rond beveiliging hebben en zich verantwoordelijk gedragen op het vlak van beveiliging.

Deze vereisten moeten geïntegreerd zijn in CCE's programma rond voorlichting met betrekking tot gegevensbeveiliging.

2.10.1. Bewustzijn rond beveiliging bij nieuw aangenomen medewerkers

Nieuw aangenomen medewerkers zullen voorlichting krijgen over gegevensbeveiliging, waarbij ze kennismaken met het beveiligingsbeleid van CCE en te horen krijgen wat van hen wordt verwacht met betrekking tot beveiliging.

Het programma voor voorlichting over beveiliging voor nieuw aangenomen medewerkers moet zo worden opgesteld dat nieuw aangenomen medewerkers kennismaken met het CEE-beveiligingsbeleid en -normenkader met betrekking tot het acceptabel gebruik van de verschillende computerhulpmiddelen van CCE (bijv. e-mail, internet), de procedures voor activaclassificatie en de bescherming van deze activa. Daarnaast worden nieuwe medewerkers op de hoogte gebracht waar ze het beleid rond informatiebeveiliging en de documenten met de normen kunnen vinden op het intranet van CCE.

2.10.2. Bewustzijn rond beveiliging bij derde partijen

Alle externe partijen die het computersysteem moeten gebruiken (alle aannemers, vertegenwoordigers van leveranciers en agenten) zullen eerst worden voorgelicht over informatiebeveiliging voordat ze toegang krijgen tot computerhulpmiddelen. IT Security moet een ondertekende netwerktoegangsovereenkomst verkrijgen waarin de derde partij verklaart dat hij op de hoogte is van het beveiligingsbeleid. De overeenkomst moet voor elke derde partij worden bewaard.

2.10.3. Permanente voorlichting over gegevensbeveiliging

Door voortdurend activiteiten te organiseren waardoor medewerkers op de hoogte blijven van het beleid rond gegevensbeveiliging kunnen de kosten van incidenten op het vlak van beveiliging worden verminderd, kan de ontwikkeling van nieuwe toepassingssystemen worden versneld en kan ervoor worden gezorgd dat de controlemiddelen voor informatiesystemen in de hele organisatie consistent worden geïmplementeerd. Alle gebruikers zullen voorlichting en training krijgen over informatiebeveiliging, in verhouding tot hun verantwoordelijkheden voor het verwerken van en het omgaan met informatie. Het management moet zich

ervan bewust zijn dat de vereisten op het vlak van informatiebeveiliging erg kunnen verschillen binnen de organisatie, conform de verantwoordelijkheden van de specifieke taken van medewerkers. Het management moet er dus voor zorgen dat de toegang tot informatie voor medewerkers en externe aannemers naar behoren wordt aangepast naarmate ze andere verantwoordelijkheden krijgen binnen de organisatie. Het management en de medewerkers moeten op de hoogte worden gebracht van het potentieel van bekendmaking, risico's en verlies, en van wettelijke en auditvereisten binnen hun respectieve functie in het bedrijf.

De naleving van de richtlijnen is gebaseerd op het feit dat gebruikers het beleid en de procedures rond gegevensbeveiliging kennen, wat een essentieel element is voor een veilige omgeving voor gegevensverwerking. In de voortdurende activiteiten waarmee medewerkers op de hoogte blijven van het beleid rond gegevensbeveiliging moeten de relevante vereisten rond gegevensbeveiliging, hun verantwoordelijkheden als gevolg van wetgeving en voorschriften en de relevante bedrijfscontroles opgenomen zijn. Mogelijke communicatiemethoden die kunnen worden gebruikt voor initiatieven rond voorlichting over gegevensbeveiliging zijn onder andere:

- Memo's per e-mail
- TV in de pauzeruimte
- Flyers via CCE-mail
- WEB-presentatie
- Intranet
- Extra onderwerp op agenda van andere vergaderingen
- Klassikale training
- Open forums
- LMS-opleiding

2.10.4. Toegankelijkheid van gegevensbeveiligingsvoorlichting

Om de voorlichting op het gebied van gegevensbeveiliging te bevorderen, is het belangrijk dat het beleid en de normen rond gegevensbeveiliging van CCE toegankelijk zijn voor alle medewerkers en externe gebruikers. Daarom moeten alle beleidslijnen en normen met betrekking tot gegevensbeveiliging op het Bedrijfsintranet worden gepubliceerd, zodat ze online kunnen worden bekeken en mogelijk gedownload om ze later te raadplegen. Voor gebruikers die geen toegang hebben tot het Bedrijfsintranet moet het management een afgedrukte versie voorzien van het beleid en de normen met betrekking tot gegevensbeveiliging, zodat ze die later kunnen raadplegen. De functie IT Security Governance is verantwoordelijk voor de coördinatie van de algemene toegankelijkheid van alle beleidsrichtlijnen en normen rond gegevensbeveiliging.

3. Verantwoordelijkheid

IT Security and GRC is verantwoordelijk voor de ontwikkeling, de implementatie en het onderhoud van de Policy voor Acceptabel IT-gebruik met de steun van de Director – IT Security and GRC.

Het IT-management draagt de verantwoordelijkheid om de Policy voor Acceptabel IT-gebruik naar behoren door te geven aan alle partijen binnen hun respectieve organisatie-eenheden en om te waarborgen dat die partijen het beleid goed begrijpen. Het IT-management is ook verantwoordelijk voor het bepalen, het goedkeuren en het implementeren van procedures in de organisatie-eenheden, en voor de consistentie daarvan met de Policy voor Toegangsbeveiliging.

Alle individuele personen, groepen of organisaties die onder dit beleid vallen, dragen de verantwoordelijkheid om zich vertrouwd te maken met de Policy voor Acceptabel IT-gebruik en de bijbehorende procedures voorzien door het IT-management, en om deze na te leven. Elke individuele persoon is ook verantwoordelijk voor het melden van potentiële overtredingen van dit beleid aan het IT-management.

4. Handhaving van het beleid en omgaan met uitzonderingen

Wie de Policy voor Acceptabel IT-beleid en de bijbehorende procedures niet naleeft, kan disciplinaire maatregelen opgelegd krijgen, mogelijk zelfs de beëindiging van het dienstverband voor medewerkers of de beëindiging van het contract voor aannemers, adviseurs of andere entiteiten. Indien nodig, kunnen ook juridische stappen worden ondernomen voor overtredingen van de relevante voorschriften en wetten.

Verzoeken tot uitzonderingen op de Policy voor Acceptabel IT-beleid moeten via een wijzigingsaanvraag worden ingediend bij IT Security and GRC. Uitzonderingen worden uitsluitend toegestaan met een bewijs van goedkeuring door de Director – IT Security and GRC.

IT Security and GRC en het IT-management bewaken de naleving van de richtlijnen en de handhaving van het beleid via het proces voor acceptabel IT-gebruik.

5. Geschiedenis

De Policy voor Acceptabel IT-gebruik wordt jaarlijks opnieuw bekeken en aangepast in overeenstemming met het bedrijfsbeleid.

5.1. Nieuw
5.2. Revisie 1:

Bijlage 8: Voorbereiding meldingsformulier Wbp: "WebEx meetings (incidenteel) opnemen"

Deze ruimte niet beschrijven

0 E Meldingsnr. | | | | | | | | |

0 M

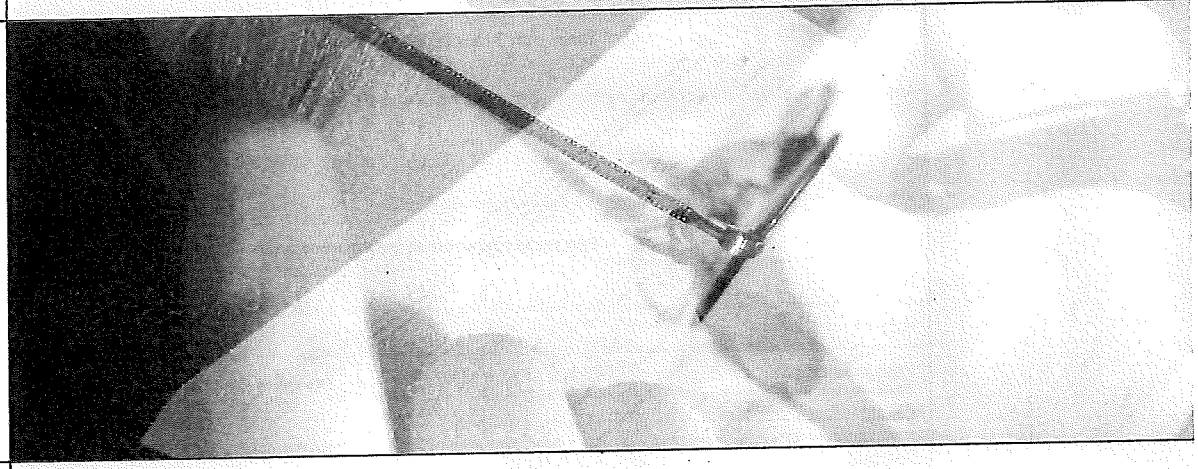
Datum .

Deze melding betreft een:

0 Eerste WBP-melding | *ga naar vraag 1* |

0 Mutatie | *vul hier uw toegekende meldingsnummer in* |

| | | | | | | | |



Meldingsformulier verwerking persoonsgegevens

Met dit formulier kan een verwerking van persoonsgegevens gemeld worden bij het College bescherming persoonsgegevens (CBP). Het betreft de melding bij het CBP die op grond van de Wet bescherming persoonsgegevens (WBP) geldt voor niet van melding vrijgestelde verwerkingen van persoonsgegevens. Tevens kunt u door middel van dit formulier wijzigingen op een eerder gedane WBP-melding doorgeven.

De melding dient te geschieden door of namens de verantwoordelijke. Zijn er meer verantwoordelijken, dan moet de melding geschieden door of namens elk van de betrokken verantwoordelijken. Vergeet u niet in bovenstaand invulvak aan te geven of het een eerste melding onder de WBP of een mutatie inclusief meldingsnummer betreft.

Let bij het invullen vooral goed op de schuingedrukte groene invulinstructies en de instructies | *ga naar vraag ..* |

Vraag 1

Verantwoordelijke

*De antwoordvelden die zijn voorzien van een * moeten altijd worden ingevuld.*

De verantwoordelijke is degene die het doel en de middelen voor de verwerking vaststelt. Dit kan een rechtspersoon of bestuursorgaan of een natuurlijk persoon zijn. Indien er meerdere verantwoordelijken voor een melding zijn, dienen deze apart opgegeven te worden.

| TOELICHTING VRAAG 1 | *Wie is de verantwoordelijke?* | *Voorbeelden* | *Meerdere verantwoordelijken* | *SBI-nummer* | *Vestiging verantwoordelijke in Nederland* |

1.1 **Hoeveel verantwoordelijken zijn er voor deze verwerking?** *Om meer dan één verantwoordelijke te kunnen melden, dient u deze bladzijde oningevuld evenzoveel maal te kopiëren als er verantwoordelijken zijn.*

(●) 1 | *ga naar vraag 1.3* |

( ) meer dan 1, namelijk | | *kopieer de bladzijde* |

1.2 **Voor welk deel van de verwerking is de onderstaande (mede) verantwoordelijke verantwoordelijk?**

1.3 **De verantwoordelijke is:** *Slechts één van beide categorieën invullen.*

(●) **Een rechtspersoon of bestuursorgaan**

Naam*	Coca-Cola Enterprises Nederland B.V.
Adres*	Watermanweg 30
Postcode en plaats*	3067GG Rotterdam
Land*	Nederland
Postbus	8775
Postcode en plaats	3000GAT Rotterdam
Land	Nederland
Telefoonnummer*	010 2455400
Faxnummer	010 2455537
E-mailadres	
SBI-nummer	

( ) **Een natuurlijk persoon**

Achternaam*	
Voorvoegsel(s)	
Voorletter(s)*	
De heer of mevrouw*	( ) M ( ) V
Adres*	
Postcode en plaats*	
Land*	
Postbus	
Postcode en plaats	
Land	
Telefoonnummer*	
Faxnummer	
E-mailadres	
SBI-nummer	

Vraag 2

Contactpersoon

*De antwoordvelden die zijn voorzien van een * moeten altijd worden ingevuld.*

Bij deze vraag moet u aangeven wie de contactpersoon is voor deze melding. Alle correspondentie over de melding zal naar de contactpersoon worden gestuurd. Het CBP neemt ook contact op met deze persoon indien er vragen zijn over de melding.

| TOELICHTING VRAAG 2 | *Contactpersoon* |

2.1

Wie is de contactpersoon voor deze melding?

Achternaam*	Wijbenga
Voorvoegsel(s)	
Voorletter(s)*	J.
De heer of mevrouw*	M V
Organisatie*	Coca-Cola Enterprises Nederland B.V.
Afdeling	Legal
Functie*	Legal Counsel
Adres*	Wetteranweg 30
Postcode*	3067GG
Plaats*	Rotterdam
Postbus	8775
Postcode	3009AT
Plaats	Rotterdam
Telefoonnummer*	010-2455
Faxnummer	010-2455537
E-mailadres	

Vraag 3

Bewerker

*De antwoordvelden die zijn voorzien van een * moeten altijd worden ingevuld, als u de bewerker meldt.*

Een bewerker is een persoon of organisatie aan wie de verantwoordelijke de verwerking van persoonsgegevens heeft uitbesteed. Het invullen van deze vraag is niet verplicht, maar is wel van belang om inzicht te krijgen in de wijze waarop de verwerking verloopt. Indien er meerdere bewerkers voor een melding zijn, dienen deze apart opgegeven te worden.

| TOELICHTING VRAAG 3 | *Bewerker* | *Meerdere bewerkers* |

3.1.

Door hoeveel bewerkers worden de persoonsgegevens die in deze melding worden beschreven, verwerkt?
Om meer dan één bewerker te kunnen melden, dient u deze bladzijde oningevuld evenzoveel maal te kopiëren als er bewerkers zijn.

0 geen | *ga naar vraag 4* |

0 1 | *ga naar vraag 3.2* |

0 meer dan 1, namelijk | | *kopieer de bladzijde* |

3.2

De bewerker is: *Slechts één van beide categorieën invullen.*

0 **Een rechtspersoon of bestuursorgaan**

Naam*	
Adres*	
Postcode*	
Plaats*	
Land*	
Postbus	
Postcode	
Plaats	
Land	
Telefoonnummer*	
Faxnummer	
E-mailadres	

0 **Een natuurlijk persoon**

Achternaam*	
Voorvoegsel(s)	
Voorletters*	
De heer of mevrouw*	0 M 0 V
Adres*	
Postcode*	
Plaats *	
Land*	
Postbus	
Postcode	
Plaats	
Land	
Telefoonnummer*	
Faxnummer	
E-mailadres	

Vraag 4

Wat meldt u aan?

Hier dient de verwerking van persoonsgegevens omschreven te worden. Dat kan door de naam van de verwerking of het systeem te vermelden zoals deze binnen de organisatie(s) van de verantwoordelijke(n) bekend is, bijvoorbeeld 'personeelsadministratie' of 'klachtenregistratie'.

| TOELICHTING VRAAG 4 | *Wat moet u melden?* | *Incidentele verwerking* |

4.1

Hoe luidt de naam of de omschrijving van de verwerking van persoonsgegevens?

Maximaal 1 verwerking van persoonsgegevens per formulier melden.

'Web-Ex meetings (incidenteel) opnemen.

Vraag 5

Het doel van de verwerking

Er kunnen meerdere doelen omschreven worden.
Let op: het doel of de doelen moet(en) betrekking hebben op de bij vraag 4.1 ingevulde naam of omschrijving van de verwerking.

Een precieze en duidelijke omschrijving van het doel (of de samenhangende doeleinden) van de verwerking is van belang, omdat aan de hand van het doel van de verwerking de hoeveelheid, de soort, de kwaliteit en de bewaartermijn van de gegevens worden getoetst.

| TOELICHTING VRAAG 5 | *Doel of doeleinden van de verwerking* | *Voorbeelden* | *Meerdere doeleinden* |

5.1

Voor welk doel of voor welke samenhangende doeleinden verwerkt de verantwoordelijke persoonsgegevens?

1 |

2 |

3 |

4 |

5 |

6 |

7 |

8 |

9 |

10 |

Vraag 6

Categorieën van betrokkenen

Indien er meerdere categorieën van betrokkenen zijn, dan dienen alle categorieën van betrokkenen apart volgens de opzet van vraag 6 opgegeven te worden. De oningevulde bladzijden met vraag 6.1 t/m 6.5 kunnen daarvoor zo vaak als nodig gekopieerd worden en dan voorzien worden van een opeenvolgende letter, beginnend bij een A. Per letter mag maar één categorie van betrokkenen gemeld worden. Bij vraag 6.5 kunt u meerdere antwoorden aankruisen.

Bij deze vraag dient u aan te geven over wie persoonsgegevens worden verwerkt ('de betrokkenen'), welke soorten van gegevens er per categorie van betrokkenen worden verwerkt en voor welk doel of doelen de omschreven soorten van gegevens zijn verzameld. Tevens wordt gevraagd of er zogenaamde 'bijzondere persoonsgegevens' worden verwerkt. Verwerking hiervan is alleen toegestaan in een aantal expliciet in de WBP opgesomde gevallen.

| **TOELICHTING VRAAG 6** | *Algemeen* | **VRAAG 6.2** | *Categorie van betrokkenen* | *Meerdere categorieën van betrokkenen* | **VRAAG 6.3** | *Persoonsgegevens* | **VRAAG 6.4** | *Doel van het verzamelen van persoonsgegevens* | **VRAAG 6.5** | *Bijzondere persoonsgegevens* |

6.1 **Hoeveel categorieën van betrokkenen zijn er voor deze verwerking?**

0 1 | *ga naar vraag 6.2* |

0 meer dan 1, namelijk | | | *kopieer de bladzijden* |

6.2 **Over welke categorie van betrokkenen verwerkt u gegevens?** *Let op: de categorie van betrokkenen moet betrekking hebben op de bij vraag 4.1 ingevulde naam en het bij vraag 5.1 ingevulde doel van de verwerking.*

|

6.3 **Welke gegevens of categorieën van gegevens die betrekking hebben op de genoemde categorie van betrokkenen (*vraag 6.2*) worden verwerkt?**

1	11
2	12
3	13
4	14
5	15
6	16
7	17
8	18
9	19
10	20

6.4 **Voor welk doel of samenhangende doeleinden zijn/worden de (categorieën van) gegevens die zijn ingevuld bij vraag 6.3, verzameld?** *De nummering correspondeert met die van vraag 6.3.*

1 |

|

2 |

|

3 |

|

4 |

|

5 |

|

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

6.5 **Welke bijzondere gegevens die betrekking hebben op de genoemde categorie van betrokkenen worden verwerkt?**

0 Geen | *ga naar vraag 7* |

0 Gegevens betreffende godsdienst en levensovertuiging

0 Gegevens betreffende ras of etniciteit

0 Gegevens betreffende politieke gezindheid

0 Gegevens betreffende de gezondheid

0 Gegevens betreffende het sexuele leven

0 Gegevens betreffende het lidmaatschap van een vakvereniging

0 Strafrechtelijke gegevens

0 Gegevens betreffende onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag

Vraag 7

Verstrekking van gegevens

U kunt hier meerdere categorieën van ontvangers invullen.

Bij deze vraag moet worden ingevuld aan welke ontvangers of categorieën van ontvangers de gegevens worden verstrekt. De WBP verstaat onder het begrip ontvanger: degene aan wie de persoonsgegevens worden verstrekt.

| **TOELICHTING VRAAG 7** | *Ontvanger* | *Degenen die belast zijn met de verwerking van de gegevens* | *Leidinggevenden* | *Bewerker* | *Wettelijke verplichtingen tot verstrekking* |

7.1

Aan welke ontvangers of categorieën van ontvangers worden de gegevens verstrekt?

1 |

2 |

3 |

4 |

5 |

6 |

7 |

8 |

9 |

10 |

11 |

12 |

13 |

14 |

15 |

16 |

17 |

18 |

19 |

20 |

Vraag 8

Beveiliging van persoonsgegevens

Bij vragen 8.2 en 8.4 tot en met 8.6 kunt u meerdere antwoorden aankruisen.

Deze vraag is bedoeld om het CBP een indruk te geven van de beveiligingsmaatregelen. De door u ingevulde gegevens worden niet in het openbaar meldingenregister geplaatst.

| TOELICHTING VRAAG 8 | *Beveiliging van de gegevens* |

8.1 **Beveiligt u de persoonsgegevens?**

- 0 Nee | *ga naar vraag 8.3* |
- 0 Ja

8.2 **Welke maatregelen heeft u genomen om de persoonsgegevens te beschermen?**

- 0 Vastgesteld beveiligingsbeleid dat ook is geïmplementeerd
- 0 Fysieke maatregelen voor toegangsbeveiliging, inclusief organisatorische controle
- 0 Inbraakalarm
- 0 Kluis voor opslag van gegevensbestanden
- 0 Logische toegangscontrole m.b.v. iets wat iemand weet (wachtwoord of pincode)
- 0 Logische toegangscontrole m.b.v. iets wat iemand bij zich draagt (pasje)
- 0 Logische toegangscontrole m.b.v. iets wat bij iemand hoort (biometrisch kenmerk)
- 0 Overige logische toegangscontrole
- 0 Automatische logging van toegang tot gegevens, incl. een controleprocedure
- 0 Controle van toegekende bevoegdheden
- 0 Overige beveiligingsmaatregelen | *a.u.b. specificeren* |

8.3 **Is er sprake van een bewerker?** *Slechts één antwoord mogelijk.*

- 0 Nee
- 0 Ja, en er zijn met de bewerker(s), d.w.z. met elke bewerker, schriftelijke afspraken gemaakt over beveiliging
- 0 Ja, en er zijn géén schriftelijke afspraken over beveiliging gemaakt met de bewerker of met één van de bewerkers

8.4 **Wie heeft toegang tot de persoonsgegevens?**

- 0 Personeel dat onder leiding van de verantwoordelijke staat
- 0 Personeel dat onder leiding van de bewerker staat
- 0 Derden | *a.u.b. specificeren* |

8.5 **Verzendt u gegevens langs elektronische weg?**

- 0 Nee
- 0 Ja, via een eigen netwerk
- 0 Ja, via een publiek netwerk

8.6 **Gebruikt u encryptie?**

- 0 Ja, de persoonsgegevens worden versleuteld tijdens verzending
- 0 Ja, de gegevensopslag is versleuteld
- 0 Nee

Vraag 9

Doorgifte naar landen buiten de Europese Unie

Deze vragen gaan over doorgifte van gegevens naar landen buiten de Europese Unie.
N.B.: doorgifte naar landen buiten de Europese Unie is alleen toegestaan in bepaalde gevallen. Zie de toelichting.

| **TOELICHTING VRAAG 9** | *Doorgifte van persoonsgegevens binnen de Europese Unie* | *Doorgifte van persoonsgegevens naar landen buiten de Europese Unie* |

9.1

Geeft u bij uw gegevensverwerking persoonsgegevens door naar één of meer landen buiten de Europese Unie?

0 Nee | *ga naar vraag 10* |

0 Ja

9.2

Worden persoonsgegevens uitsluitend doorgegeven naar landen buiten de Europese Unie waarvan de Minister van Justitie heeft bepaald dat die landen een passend beschermingsniveau waarborgen?

0 Nee

0 Ja

Vraag 10

Voorafgaand onderzoek

Voor een beperkt aantal categorieën van gegevensverwerkingen vereist de WBP dat er, voordat u met de verwerking start, een onderzoek plaatsvindt: het voorafgaand onderzoek. Het gaat daarbij om gegevensverwerkingen die specifieke risico's met zich meebrengen voor de rechten en vrijheden van de betrokkenen. Aan de hand van onderstaande vragen kunt u bepalen of daarvan sprake is.
N.B.: de inlichtingen die zijn verkregen aan de hand van deze vragen worden niet in het openbaar meldingenregister geplaatst.

| TOELICHTING VRAAG 10 | *Algemeen* | *Nader onderzoek?* | *Opschorting van de gegevensverwerking* | *Persoonlijk identificatienummer* | *Heimelijke waarneming* | *Strafrechtelijke gegevens en gegevens over hinderlijk of onrechtmatig gedrag* |

Bij vraag 10.6 moet u de juiste conclusie aankruisen.

10.1 **Bent u van plan om een <u>persoonlijk identificatienummer</u> van de betrokkene(n) te verwerken voor een <u>ander doel</u> dan waarvoor het nummer specifiek is bestemd, met het doel de gegevens in verband te brengen (te koppelen) met gegevens die door een andere verantwoordelijke worden verwerkt?**

0 Nee | *ga naar vraag 10.3* |

0 Ja | *ga naar vraag 10.2* |

10.2 **Is het persoonlijk identificatienummer voorgeschreven bij wet en gebruikt u het nummer alleen ter uitvoering van die wet of een andere wet?**

0 Nee | *ga naar vraag 10.3* |

0 Ja | *ga naar vraag 10.3* |

10.3 **Bent u van plan gegevens van de betrokkene(n) vast te leggen die u door <u>eigen waarneming</u> hebt verkregen, <u>zonder</u> de betrokkene(n) van die vastlegging op de hoogte te stellen?**

0 Nee | *ga naar vraag 10.4* |

0 Ja | *ga naar vraag 10.4* |

10.4 **Bent u van plan <u>voor derden</u> strafrechtelijke gegevens of gegevens over onrechtmatig of hinderlijk gedrag van de betrokkene(n) te verwerken?**

0 Nee | *ga naar vraag 10.6* |

0 Ja | *ga naar vraag 10.5* |

10.5 **Heeft u een vergunning op grond van de Wet particuliere beveiligingsorganisaties en recherchebureaus?**

0 Nee | *ga naar vraag 10.6* |

0 Ja | *ga naar vraag 10.6* |

10.6 **Wat is de conclusie aan de hand van bovenstaande vragen?**

Voor het bepalen van de juiste conclusie geldt onderstaande keuzetabel.

vraag 10.2	=	Nee	en/of	in alle overige gevallen
vraag 10.3	=	Ja	en/of	
vraag 10.5	=	Nee		

Conclusie 1

0 **U vraagt het CBP om een voorafgaand onderzoek.** Dit verzoek geschiedt automatisch door het aankruisen van dit hokje en het inzenden van dit formulier.

Conclusie 2

0 **U vraagt het CBP niet om een voorafgaand onderzoek.**

Ondergetekende verklaart bevoegd te zijn tot het doen van deze melding en dat de in de melding verstrekte inlichtingen juist zijn.

Alle velden moeten worden ingevuld.

Naam

Functie

Plaats

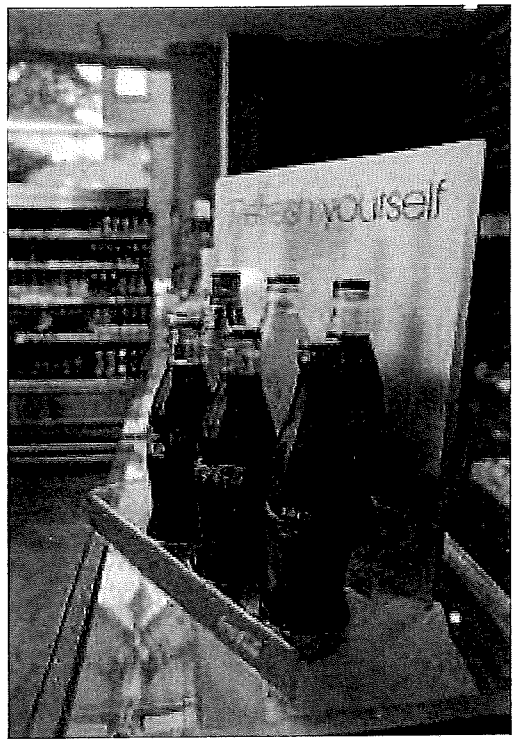
Datum

Handtekening

Dit formulier na invulling en ondertekening zenden aan het CBP, t.a.v. Afdeling Bestandsbeheer, Postbus 93374, 2509 AJ Den Haag.

Let op: u dient het meldingsformulier op te sturen, voorzien van de handtekening van de verantwoordelijke(n) of een persoon die door de verantwoordelijke(n) is gemachtigd. Zonder een volledig ingevuld en ondertekend meldingsformulier kan de melding niet als verricht beschouwd worden.

Bijlage 9: Code of Business Conduct, p. 14



Intellectuele eigendom

De intellectuele eigendomrechten van ons bedrijf, in eigendom of in licentie, behoren tot de meest kostbare activa. Wij moeten de intellectuele eigendomsrechten van ons bedrijf beschermen. "Intellectuele eigendom" refereert aan iets dat wij tijdens kantoortijd op kosten van CCE of binnen onze taakomschrijvingen creëren. CCE bezit de rechten op alles wat wij creëren door onze werkzaamheden bij CCE voor zover toegestaan door de wetgeving, ongeacht of deze eigendom octrooieerbaar is of wordt beschermd door auteursrecht, bedrijfsgeheim of handelsmerk. Voorbeelden van intellectuele eigendom omvatten auteursrechten, patenten, handelsmerken, bedrijfsgeheimen, ontwerprechten, logo's, softwareprogramma's, bedrijfsprocessen en leverings- of productiemethodes.

Persoonsgegevens

Wij hebben de taak om vertrouwelijke persoonsgegevens die aan ons worden toevertrouwd door onze collega's, klanten, leveranciers en anderen, te beschermen conform de plaatselijke wetgeving en de bedrijfsrichtlijnen. Niemand mag toegang hebben tot toekomstige, huidige of voormalige personeelsgegevens of deze verwerken, gebruiken of bekendmaken, zoals onder meer salarisbestanden, bestanden inzake collectieve verzekeringen, extralegale voordelen en werkbestanden - zonder de vereiste toestemming.

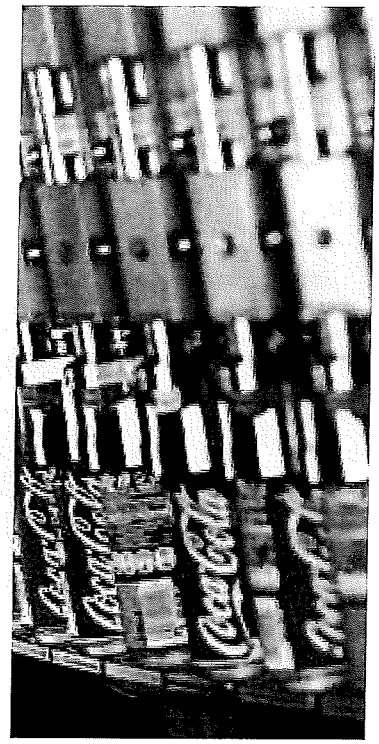
Voor meer gedetailleerd advies raadpleeg de richtlijnen van CCE die voor uw locatie inzake management betreffende werknemersgegevens van toepassing zijn.

Gepast gebruik van technologie

Wij moeten de computerhardware en software van CCE, alsmede de opgeslagen gegevens op de computersystemen van het bedrijf beschermen tegen schade, veranderingen, diefstal, fraude en onbevoegde toegang. Om dit doel te bereiken, moeten we de specifieke veiligheidsmaatregelen en interne controles voor de computersystemen waartoe wij toegang hebben in acht nemen. Wij hebben een verantwoordelijkheid om deze middelen te gebruiken op een veilige, ethische, wettige en efficiënte wijze. Dit betekent onder meer dat wij nooit de bedrijfstechnologieën (waaronder computers en andere elektronische apparatuur die toegang heeft tot het internet, zoals PDA of mobiele telefoons) of computersystemen mogen gebruiken voor het downloaden of het versturen van ongepaste, discriminerende, seksueel expliciete of beledigende uitspraken of bestanden. Daarnaast mogen we deze systemen niet gebruiken voor toegang tot illegaal materiaal, het verzenden van niet geautoriseerde verzoeken of het uitvoeren van zaken voor een ander bedrijf.

Let op dat elektronische berichten (zoals e-mailberichten en tekstberichten) en plaatsingen op openbare fora (zoals blogs en sociale netwerkpagina's) permanente overdraagbare communicatiegegevens zijn die de reputatie van ons bedrijf kunnen beïnvloeden. Neem extra voorzorgsmaatregelen bij het opstellen van dergelijke items. Bij het gebruik van CCE-technologieën, mag uitsluitend voor zakelijke doeleinden informatie op openbare fora worden geplaatst. Vergeet niet dat de communicaties die u opstelt en verzendt met gebruik van CCE-technologieën en computersystemen niet noodzakelijkerwijze privé zijn. Voor zover toegelaten onder de geldende wetgeving en richtlijnen, kunnen uw elektronische communicaties worden gecontroleerd en worden gebruikt voor bedrijfsdoeleinden.

Voor meer gedetailleerd advies raadpleeg de richtlijnen van CCE die voor uw locatie inzake het gebruik van CCE-technologieën en computersystemen van toepassing zijn.



Vraag:
Claudia is nauw betrokken bij de politiek en heeft een blog over de plaatselijke kandidaten die zij ondersteunt. Nu de lokale verkiezingen naderen, gaat zij bloggen tijdens haar lunchpauze op de laptop van CCE. Is dit in orde, aangezien ze dit niet doet tijdens de kantooruren?

Antwoord:
Nee. Claudia moet niet vergeten dat alles wat zij plaatst op publieke websites en daarbij gebruik maakt van CCE-computersystemen, kan worden getraceerd naar ons bedrijf. Dit betekent dat anderen de zienswijzen van Claudia kunnen beschouwen als zijnde afkomstig van CCE of dat CCE ze ondersteunt. Waak erover dat bij het gebruik van CCE-systemen of technologieën bedrijfsinformatie uitsluitend op toegestane wijze wordt geplaatst.

Bijlage 10: Gesprek met IT-specialist Rob Franken en Perry Wetsteijn

Bijlage 10: Gesprek met IT-specialist Rob Franken en Perry Wetsteijn

Naar aanleiding van mijn scriptie over privacywet- en regelgeving heb ik een aantal vragen over het IT-gedeelte van de beveiliging van persoonsgegevens.

Hoe wordt er invulling gegeven aan de beveiligingsmaatregelen uit de Code
Er zijn ontelbaar veel manieren waarop wij data beschermen binnen CCE-NL. Denk bijvoorbeeld aan encryptie, firewalls, beschermde servers en wachtwoorden die op regelmatige basis worden gewijzigd.

Het informatiebeveiligingsbeleid waarnaar verwezen wordt in de richtlijn GP, kan ik niet terugvinden op het intranet. Waar wordt dan vermeld hoe medewerkers met informatiebeveiliging moeten omgaan?
In de 'Acceptabel IT-gebruik-policy'. Typ maar gewoon IT-richtlijnen in bij het intranet van CCE-NL en dan moet deze policy naar voren komen. Hierin wordt vermeld hoe medewerkers met informatie en de beveiliging daarvan moeten omgaan. Er wordt in deze policy tevens verwezen naar de Retention Policy waarin staat hoelang bepaalde gegevens bewaard moeten blijven.

Bijlage 11: Privacy Policy

PRIVACY POLICY

INHOUD

Coca-Cola Enterprises Nederland B.V. (**"CCE-NL"**) beschikt in het kader van haar dienstverlening over persoonsgegevens van [=]. CCE-NL gaat zorgvuldig met uw gegevens om en zorgt ervoor dat elke verwerking van uw gegevens voldoet aan de toepasselijke wet- en regelgeving. In deze privacy policy beschrijft zij welke gegevens zij van u verwerkt, hoe zij dat doet en hoe u hiertegen bezwaar kunt maken. Deze privacy policy geldt voor alle bezoekers van websites van CCE-NL. Deze privacy policy kan van tijd tot tijd wijzigen als daarvoor aanleiding is. Op [WEBSITE] vindt u de actuele versie van de privacy policy.

1. WANNEER IS DEZE PRIVACY POLICY VAN TOEPASSING?

1.1 Deze privacy policy is van toepassing op alle gegevens die CCE-NL van u verwerkt in het kader van de diensten en producten die CCE-NL in Nederland op de markt brengt. Op de verwerking van uw gegevens via websites van CCE-NL zijn verder onze Gebruikersvoorwaarden van toepassing.

2. WIE IS VERANTWOORDELIJK VOOR UW GEGEVENS?

2.1 De verantwoordelijke voor de verwerking van de persoonsgegevens is CCE-NL, gevestigd te (3067 GG) Rotterdam, aan de Watermanweg 30.

3. WELKE GEGEVENS VERWERKT CCE-NL?

3.1 Als u contact met CCE-NL opneemt of als u zich registreert als bezoeker van een van haar websites, verwerkt CCE-NL mogelijk uw persoonsgegevens. Persoonsgegevens zijn gegevens die zijn te herleiden tot u persoonlijk zoals uw naam, adres, woonplaats, e-mailadres en bankrekeningnummer. CCE-NL verwerkt ook uw gebruikersnaam en password. Ook nadat u zich heeft geregistreerd, worden gegevens van u verwerkt, bijvoorbeeld uw voorkeuren voor bepaalde producten en diensten.

- *[Optioneel] Melding CBP*
  CCE-NL heeft haar verwerkingen van persoonsgegevens aangemeld bij het College Bescherming Persoonsgegevens in Den Haag. Bij de aanmelding is precies omschreven welke gegevens CCE-NL van u verwerkt, voor welke doeleinden CCE-NL uw gegevens verwerkt en aan welke personen en of instanties uw gegevens worden verstrekt. U kunt de meldingen van CCE-NL vinden op www.cbpweb.nl, onder het tabblad "openbare registers".

4. VOOR WELK DOEL GEBRUIKT CCE-NL UW GEGEVENS?

4.1 <u>Dienstverlening</u>
CCE-NL verwerkt uw persoonsgegevens in de eerste plaats om haar diensten aan u te kunnen leveren. Zij gebruikt deze gegevens om haar diensten te verlenen,

meer specifiek [BIJVOORBEELD] is voor het verwerken van een bestelling of het versturen van een factuur verwerking van uw gegevens noodzakelijk. Zonder verwerking van uw gegevens kan CCE-NL haar diensten niet aan u leveren.

4.2 Verstrekken aan klanten van CCE-NL

De klanten van CCE-NL zijn de bedrijven en instellingen [=].CCE-NL kan uw gegevens aan de klanten verstrekken om haar klanten in staat te stellen om [=]. De gegevens worden alleen aan haar klanten verstrekt als u daar van tevoren toestemming voor hebt verleend. U kunt deze toestemming ook steeds weer intrekken. CCE-NL heeft met haar klanten de vereiste contractuele en organisatorische maatregelen getroffen om te verzekeren dat uw gegevens uitsluitend worden verstrekt en verwerkt door een beperkt aantal personen.

4.3 Inschakelen derden

CCE-NL kan derde partijen inschakelen bij het uitvoeren van haar diensten. Voor zover deze derden bij het uitvoeren van de betreffende diensten toegang hebben tot persoonsgegevens heeft CCE-NL de vereiste contractuele en organisatorische maatregelen getroffen om te verzekeren dat uw gegevens uitsluitend voor de in dit privacy statement genoemde doeleinden worden verwerkt.

4.4 Het voldoen aan wettelijke verplichtingen

CCE-NL kan op grond van de wet in een voorkomend geval verplicht zijn om uw gegevens aan derden te verstrekken. U kunt daarbij denken aan de verstrekking van gegevens in het kader van een strafrechtelijk onderzoek, aan bevoegde autoriteiten.

4.5 Rapportage en analyses

CCE-NL gebruikt geaggregeerde combinaties van persoonsgegevens van bezoekers voor het maken van trendanalyses, benchmarking en klantprofielen ten behoeve van andere bedrijven of instellingen. Hiervoor gebruikt zij alleen geanonimiseerde persoonsgegevens. Deze gegevens zijn niet herleidbaar tot u.

4.6 Marketing- en verkoopactiviteiten

Als klant van CCE-NL doet CCE-NL u graag aanbiedingen voor haar producten en diensten (ook na beëindiging van het contract met u). Dit doet zij per telefoon, e-mail of post, tenzij u hier bezwaar tegen maakt. CCE-NL kan uw NAW-gegevens verkopen aan derden die deze kunnen gebruiken voor direct marketing activiteiten, als u hier van tevoren uitdrukkelijk toestemming voor hebt gegeven.

4.7 Verwerking van uw gegevens op websites van CCE-NL

CCE-NL verzamelt en gebruikt uw persoonlijke gegevens op haar websites in de eerste plaats om haar (web)diensten aan u te kunnen leveren en om met u te communiceren.

Uw gegevens worden daarnaast gebruikt voor het doen van onderzoek en het uitvoeren van analyses, met als doel om onze diensten en onze websites te verbeteren.

Tenslotte kan CCE-NL uw gegevens op haar websites gebruiken om

- informatie en advertenties af te beelden die aansluiten bij uw persoonlijke interesses en voorkeuren en
- u in bepaalde gevallen (commerciële) informatie per e-mail te kunnen sturen over andere producten of services die beschikbaar zijn bij CCE-NL, tenzij u hebt aangegeven daartegen bezwaar te hebben.

4.8 CCE-NL verwerkt op haar websites de volgende gegevens van u:

– *Inloggegevens*
Wanneer u toegang wenst tot bepaalde websites en daarop aangeboden diensten, wordt u gevraagd om u aan te melden met een gebruikersnaam en een wachtwoord (inloggegevens). In een aantal gevallen kunt u zich met deze inloggegevens bij meerdere websites en daarop aangeboden diensten aanmelden.

– *Informatie die u achterlaat op websites*
Op sommige websites vraagt CCE-NL u om aanvullende persoonlijke informatie, zoals uw e-mailadres, naam, thuis- of werkadres of een telefoonnummer. Wanneer u een aankoop doet of een abonnement neemt op een betaalde dienst, vraagt CCE-NL u om aanvullende informatie, zoals uw bankrekeningnummer of nummer van een identificatiebewijs. Daarnaast zal soms gevraagd worden naar profiel- of demografische gegevens, zoals uw postcode, leeftijd, geslacht, voorkeuren, interesses en favorieten.

– *Surf- en klikgedrag*
CCE-NL kan informatie verzamelen over uw bezoek aan haar websites, inclusief de pagina's die u daarop bekijkt, de koppelingen (links) waarop u klikt en de andere acties die u onderneemt. Daarnaast verzamelt CCE-NL bepaalde standaardinformatie die uw browser naar elke website verzendt die u bezoekt, zoals uw IP-adres, het type en de taal van de browser, de tijd van uw bezoek en het webadres van waaruit u de website van CCE-NL bereikte.

– *Cookies*
De websites van CCE-NL maken gebruik van cookies. Cookies zijn kleine tekstbestanden die op uw computer worden gezet door de server van een

webpagina. Lees meer in de cookies policy van CCE-NL [hyperlink naar cookies policy].

– *Page tagging*
De webpagina's van CCE-NL maken gebruik van page tagging. Hierbij wordt er een plaatje (van één pixel) of een stukje Javascript op elke pagina van de site geplaatst. Pagetagging wordt gebruikt bij de aflevering van cookies op websites.

Page Tagging stelt CCE-NL in staat om de gebruikers te tellen die haar websites hebben bezocht, gegevens over gebruik van haar sites te verzamelen en de effectiviteit van reclamecampagnes te bepalen. Page tagging stelt CCE-NL daarnaast in staat om bijvoorbeeld gegevens te verzamelen over hoe vaak het klikken op een advertentie van een derde op een website van CCE-NL leidt tot een aankoop op de website van die derde.

Wij verbieden het gebruik van page tags op onze websites door derden. Het is derden dus niet toegestaan om op onze websites via page tags persoonlijke gegevens te verzamelen.

Wanneer u nieuwsbrieven of reclamemail ontvangt van CCE-NL, kan zij soms gebruik maken van page tagging om te bepalen of de e-mail werd geopend en op welke koppelingen u klikt, zodat CCE-NL in de toekomst beter gerichte e-mail- of andere communicatie kunnen verzorgen.

5. KOPPELING MET INTERNE EN EXTERNE BESTANDEN

5.1 Om u een meer consistente en persoonlijke ervaring te kunnen bieden bij uw contacten met CCE-NL, kan CCE-NL de informatie die zij heeft verzameld in het kader van een door haar aan u geleverde dienst combineren met informatie die zij heeft verkregen via andere door CCE-NL aan u geleverde diensten.

5.2 Daarnaast kan CCE-NL de informatie die zij verzamelt aanvullen met informatie die zij van andere bedrijven heeft verkregen.
Zo kan zij bijvoorbeeld gebruik maken van de diensten van andere bedrijven die haar in staat stellen een algemeen beeld te krijgen van uw geografische gebied op basis van uw IP-adres, zodat CCE-NL haar dienstverlening daaraan kan aanpassen.

6. HOE LANG BEWAART CCE-NL UW GEGEVENS?

6.1 CCE-NL bewaart uw gegevens niet langer dan wettelijk is toegestaan en noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor uw gegevens worden verwerkt. Hoe lang bepaalde gegevens worden bewaard is afhankelijk van

de aard van de gegevens en de doeleinden waarvoor zij worden verwerkt. De bewaartermijn kan dus per gebruik verschillen.

7. WACHTWOORD

7.1 Het is uw eigen verantwoordelijkheid om uw wachtwoord vertrouwelijk te houden. Deel dit soort informatie nooit met anderen. Als u een computer deelt met anderen, moet u zich altijd afmelden wanneer u een website of een service verlaat om te voorkomen dat mensen die na u de computer gebruiken toegang hebben tot uw informatie.

8. INZAGE IN UW PERSOONSGEGEVENS

8.1 U heeft recht op inzage van uw persoonsgegevens. Dit houdt in dat u kunt opvragen welke persoonsgegevens er van u zijn geregistreerd en voor welke doeleinden die gegevens worden gebruikt. Een verzoek tot inzage kunt u indienen door een brief, voorzien van uw naam, adres, vaste- en/of mobiele telefoonnummer en een kopie van een geldig legitimatiebewijs, te sturen aan het hieronder onder "contact' aangegeven adres. CCE-NL kan u maximaal EUR 4,50 aan administratiekosten in rekening te brengen.

9. CORRECTIE VAN UW PERSOONSGEGEVENS

9.1 U heeft het recht om uw persoonsgegevens te laten corrigeren, als deze onjuistheden bevatten. U kunt hiervoor contact met CCE-NL opnemen (Coca-Cola Enterprises Nederland B.V., Watermanweg 30 (3067 GG) Rotterdam). U ontvangt dan uiterlijk binnen 4 weken schriftelijk antwoord.

10. RECHT VAN VERZET

10.1 Als bezoeker van [=] heeft u wettelijk een aantal mogelijkheden om u te verzetten tegen gebruik van uw gegevens. Ook als u in een eerder stadium toestemming hebt gegeven, kunt u zich verzetten tegen verder gebruik van uw gegevens. Tegen het gebruik van uw persoonsgegevens kunt u bezwaar maken indien uw persoonsgegevens worden gebruikt voor andere doeleinden dan noodzakelijk voor de uitvoering van een overeenkomst of noodzakelijk voor het nakomen van een wettelijke verplichting. Zo kunt u bijvoorbeeld bezwaar maken tegen gebruik van uw gegevens voor direct marketingdoeleinden en/of verstrekking van uw gegevens aan derden zoals de bedrijven of instellingen waarover u feedback hebt gegeven. Als u bezwaar wilt maken tegen het gebruik van uw gegevens dan kunt u ons dit laten weten per brief, gericht aan Coca-Cola Enterprises Nederland B.V., Watermanweg 30 (3067 GG) Rotterdam. Indien u bezwaar wilt maken vermeld dan in de brief duidelijk tegen welk gebruik van uw gegevens u bezwaar maakt. U ontvangt binnen 4 weken na uw bezwaar van CCE-NL een schriftelijk

antwoord. Mocht u er bezwaar tegen hebben om door CCE-NL benaderd te worden dan kun u dat ook aan haar laten weten. U kunt bezwaar maken tegen verschillende vormen van benadering. CCE-NL zal uw bezwaar zo spoedig mogelijk verwerken. Er kan echter enige tijd voorbij gaan voordat uw bezwaar in alle bestanden is verwerkt. In die periode kan het zijn dat u nog wordt benaderd.

11. MELDEN BEVEILIGINGSLEKKEN

11.1 Als u denkt dat u een zwakke plek in één van de diensten van CCE-NL hebt gevonden, wil CCE-NL graag met u samenwerken om deze situatie zo spoedig mogelijk op te lossen. Daarom verzoekt zij u deze informatie met haar te delen. Om misbruik van het beveiligingslek door anderen te voorkomen, vraagt CCE-NL u een beveiligingslek niet met anderen te delen.

Bijlage 12: Richtlijn Gegevens Privacy

HeRe! Online@ iConnect

0 0 0

Gegevensprivacy

Coca-Cola Enterprises (CCE) is volgens de wet vereist haar verplichtingen na te leven krachtens de relevante wetgeving betreffende gegevensprivacy. Daarom zijn CCE en haar medewerkers vereist zich aan verschillende verplichtingen te houden die in dit beleid worden genoemd.

CCE's verplichting
Coca-Cola Enterprises (CCE) is volgens de wet vereist haar verplichtingen na te leven krachtens de relevante wetgeving betreffende gegevensprivacy. Daarom zijn CCE en haar medewerkers vereist zich aan verschillende verplichtingen te houden die in dit beleid worden genoemd.

Toepassing
Dit beleid is van toepassing in combinatie met de Safe Harbor-overeenkomst, de Code of Business Conduct, lokaal CCE-beleid en lokale CCE-procedures betreffende gegevensbescherming, informatiebeveiligingsbeleid en alle toepasselijke landelijke gegevensbeschermingswetten.
Dit beleid is van toepassing op alle vaste en tijdelijke medewerkers van CCE, inclusief uitzendkrachten en zelfstandigen, tenzij anders is aangegeven in de ondersteunende processen en/of procedures.

Richtlijnen
Bij CCE willen we er zeker van zijn dat de opgeslagen persoonlijke gegevens van onze medewerkers nauwkeurig zijn, of dat nu op papier of in een elektronisch bestand is. We verwerken alleen gegevens voor het doel waarvoor ze zijn verzameld. We hebben een reeks principes ontwikkeld om er zeker van te zijn dat CCE voldoet aan de noodzakelijke wetgeving met betrekking tot de verwerking van persoonlijke gegevens.

Algemene definities en regels
Dit beleid regelt de verwerking van persoonlijke gegevens door CCE. De verwerking zal hoofdzakelijk worden uitgevoerd in de hoofdfunctie en de functies HR, Financiën, Fleet en BIS.
De verwijzingen "CCE", "het Bedrijf" of "Wij" in de context van dit beleid betreffen de CCE-groep van bedrijven in het land waarop het beleid van toepassing is.
"Persoonlijke gegevens" betekent informatie over de persoonlijke of materiële omstandigheden van een geïdentificeerd of te identificeren persoon, zoals zijn/haar naam, adres en alle relevante contactgegevens, zoals telefoonnummer, faxnummers en e-mailadressen; en
"Verwerking" betekent het verkrijgen, opnemen, bewaren of uitvoeren van bewerkingen op de gegevens. Het omvat, zonder beperking, het organiseren, aanpassen, veranderen, ophalen, openbaar maken, verspreiden, opnieuw rangschikken of vernietigen van de informatie of gegevens. Bijna elke activiteit met betrekking tot gegevens zal enige vorm van verwerking met zich meebrengen.

Er zijn acht kernprincipes van toepassing volgens de gegevensbeschermingswetten van de EU
Persoonlijke gegevens moeten:
1.1 Eerlijk en wettig worden verwerkt
1.2 Alleen worden verwerkt voor het opgegeven en wettige doel
1.3 Voldoende, relevant en niet overmatig zijn met betrekking tot het doel waarvoor ze worden verwerkt
1.4 Nauwkeurig en actueel zijn
1.5 Niet langer dan noodzakelijk worden bewaard
1.6 In overeenstemming met de rechten van een persoon worden verwerkt
1.7 Veilig worden bewaard
1.8 Niet worden overgebracht naar een land of gebied buiten de EER, tenzij het land een voldoende mate van bescherming kan garanderen
CCE streeft ernaar onze verplichtingen na te leven zoals is uiteengezet onder de toepasselijke wetten voor gegevensbescherming, met name met betrekking tot:

- verzoeken van medewerkers om persoonlijke gegevens in te zien; en
- de nauwkeurigheid, opslag en beveiliging van gegevens die door ons worden bewaard

Samenvatting van het beleid

De volgende voorwaarden en gerelateerde procedures garanderen dat CCE de wetgeving naleeft bij het verwerken van gegevens:

- U kunt aanvragen (onderhevig aan bepaalde juridische beperkingen) de meeste gegevens in te zien die over u worden bewaard door een schriftelijk verzoek in te dienen
- Om er zeker van te zijn dat de gegevens die we bewaren actueel zijn, moet u elke wijziging in uw persoonlijke gegevens doorgeven
- U moet volledig en op de juiste wijze worden geïnformeerd over de verwerking van uw gegevens indien u hiervan nog niet op de hoogte bent, op het moment waarop de informatie over u wordt verzameld, rechtstreeks of via derde partijen
- Het bewaren en beveiligen van gegevens moet worden uitgevoerd in overeenstemming met de Code of Business Conduct van CCE, lokaal CCE-beleid en lokale CCE-procedures betreffende gegevensbescherming, informatiebeveiligingsbeleid en alle toepasselijke wetgeving over gegevensbescherming.

Het is de verantwoordelijkheid van alle managers hun verplichtingen wat betreft de gegevensprivacy van medewerkers te lezen en te begrijpen.

Tegen elke medewerker die dit beleid overtreedt, kunnen disciplinaire maatregelen worden getroffen.

Dit beleid verwijst naar een reeks principes die door de lokale wetgeving worden ondersteund en de nietnaleving ervan zal worden afgehandeld volgens deze lokale wetten.

Verwerking van persoonlijke gegevens

CCE leeft het Safe Harbor-kader na dat is overeengekomen met het Amerikaanse Ministerie van Economische Zaken en de EU.

Persoonlijke gegevens kunnen om uiteenlopende redenen worden verwerkt. Gegevens van medewerkers worden bijvoorbeeld vereist voor een aantal zaken (hoewel dit geen uitputtelijke lijst is en mogelijk niet in alle gebieden van toepassing is) zoals:

- Beheren en onderhouden van persoonlijke gegevens
- Uitbetalen en herzien van het salaris en andere vergoedingen en secundaire arbeidsvoorwaarden
- Voorzien in en beheren van secundaire arbeidsvoorwaarden (waaronder, indien van toepassing, pensioen, levensverzekering, ziektekostenverzekering en medische verzekering)
- Uitvoeren van prestatiebeoordelingen en -evaluaties
- Bijhouden van het ziekteverzuim en andere verzuim en beheren van de aanwezigheid
- Verstrekken van informatie, indien nodig, aan overheidsinstanties
- Verwerken van informatie met betrekking tot gelijke kansen en behandeling van gegevensonderwerpen in overeenstemming met lokale wetgeving over wat wel of niet kan worden verwerkt.
- Uitvoeren van procedures voor discipline/gedrag en klachten/conflictoplossing in overeenstemming met lokale wetgeving en bedrijfsprocessen
- Beheren van het wervingsproces, de promoties en wijzigingen in de voorwaarden en bepalingen voor een medewerker of functie.

Als u vindt dat informatie die we over u bewaren niet strikt noodzakelijk is om aan deze administratieve behoeften te voldoen, moet u uw bezwaren schriftelijk kenbaar maken bij uw leidinggevende of het HeRe-team voor doorverwijzing naar een ER-specialist.

Kennisgeving en registraties

Het is mogelijk dat CCE passende registraties voor gegevensbescherming moet onderhouden. Als u met een nieuwe verwerkingsactiviteit (zoals een nieuwe marketingdatabase) of bedrijf begint, moet u de juridische afdeling raadplegen om te controleren of hiervoor bestaande

gegevensbeschermingsregistraties gelden.

Toegang tot persoonlijke gegevens

Alle medewerkers kunnen een verzoek indienen voor inzage van de persoonlijke gegevens die CCE over hen bewaart. Er zijn uitzonderingen die van toepassing kunnen zijn waarbij informatie kan worden achtergehouden onder bepaalde omstandigheden, waaronder, maar niet beperkt tot informatie die ook betrekking heeft op een derde partij, waarbij het niet redelijk is onder alle omstandigheden de informatie openbaar te maken zonder toestemming van die derde partij.

Elke medewerker die toegang tot relevante gegevens wil, moet een schriftelijk verzoek indienen bij het HeRe-team en hierin exact vermelden welke informatie wordt aangevraagd. Het aanvraagformulier voor persoonlijke gegevens moet hiervoor worden gebruikt.

Medewerkers die toegangsverzoeken van derde partijen ontvangen, moeten deze onmiddellijk naar hun leidinggevende en de juridische afdeling doorverwijzen.

CCE zal binnen 28 dagen op uw verzoek reageren. Er zullen redelijke administratiekosten in rekening worden gebracht voor elk verzoek (voor meer informatie over of u deze kosten wel of niet moet betalen, kunt u contact opnemen met uw leidinggevende of het HeRe!-team.

Nauwkeurigheid van gegevens

Bij CCE bewaren en verwerken we persoonlijke gegevens. Medewerkers die toegang hebben tot persoonlijke gegevens moeten ervoor zorgen dat de gegevens die in de systemen zijn opgeslagen in orde en bijgewerkt zijn.

Informatie die wordt bewaard is belangrijk voor de correcte administratie van secundaire arbeidsvoorwaarden. Andere gegevens, zoals telefoonnummer en contactpersoon in geval van nood zijn ook nodig om gezondheids- en veiligheidsredenen.

Om deze en andere redenen omtrent het dienstverband moeten alle wijzigingen in de omstandigheden van een medewerker worden bijgewerkt via de zelfbediening voor medewerkers. Als dit niet mogelijk is, moet u het HeRe-team zo snel als praktisch is op de hoogte stellen, zodat de gegevens kunnen worden bijgewerkt.

Alle medewerkers moeten ervoor zorgen dat de persoonlijke gegevens van derde partijen nauwkeurig en actueel zijn.

Voordat persoonlijke gegevens worden opgeslagen, moet hiervoor toestemming worden verkregen van het juridische team in uw land, dat ervoor zal zorgen dat het in overeenstemming met het beleid en de relevante wetgeving is.

Kennisgeving van verwerking

Als u informatie verzamelt over personen, moet u hen hiervan op de hoogte stellen. Vragen over de formulering van kennisgevingen van verwerking en/of het verkrijgen van toestemming dienen te worden gesteld aan de juridische afdeling.

U zult worden geïnformeerd wanneer de informatie over u wordt verzameld.

Bewaren van gegevens

Alle medewerkers kunnen een verzoek indienen voor inzage van de persoonlijke gegevens die CCE over hen bewaart. Er zijn uitzonderingen die van toepassing kunnen zijn waarbij informatie kan worden achtergehouden onder bepaalde omstandigheden, waaronder, maar niet beperkt tot informatie die ook betrekking heeft op een derde partij, waarbij het niet redelijk is onder alle omstandigheden de informatie openbaar te maken zonder toestemming van die derde partij

Elke medewerker die toegang tot relevante gegevens wil, moet een schriftelijk verzoek indienen bij het HeRe! Team en hierin exact vermelden welke informatie wordt aangevraagd. Het aanvraagformulier voor persoonlijke gegevens moet hiervoor worden gebruikt.

Medewerkers die toegangsverzoeken van derde partijen ontvangen, moeten deze onmiddellijk naar hun leidinggevende en de juridische afdeling doorverwijzen.

CCE zal binnen 28 dagen op uw verzoek reageren. Er zullen redelijke administratiekosten in rekening worden gebracht voor elk verzoek (voor meer informatie over of u deze kosten wel of niet moet betalen, kunt u contact opnemen met uw leidinggevende of het HeRe! Team.

Beveiliging

U moet de Code of Business Conduct van CCE en het informatiebeveiligingsbeleid naleven, alsmede specifiek beleid en specifieke procedures en richtlijnen die van tijd tot tijd worden uitgegeven in uw business unit.

Bedrijfsbeleidsrichtlijnen zijn grotendeels gebaseerd op de geldende wet- en regelgeving, en zijn daarom onderhevig aan veranderingen en kunnen variëren afhankelijk van de locatie. Als u ooit onzeker bent over welke regel of welk beleid u moet volgen, of als u bang bent dat er mogelijk een conflict bestaat tussen het toepasselijke recht en de richtlijnen binnen ons beleid, neem dan contact op met het HeRe!-team.