



AANTEKENEN

Ons kenmerk:

Uw kenmerk:

Datum:

Betreft:

E-mail:

30 oktober 2025

Reactie op uw Woo-verzoek

kcb@kcb.nl

Plaats:

Zoetermeer

Geachte

Hiermee reageer ik inhoudelijk op uw verzoek gedateerd 15 juli 2025. Gegeven de hoeveelheid documenten die ik naar aanleiding van uw verzoek openbaar maak, stuur ik u mijn antwoord alleen per post, ondanks uw eerdere verzoek per e-mail te corresponderen.

U verzoekt om openbaarmaking voor eenieder van informatie die het KCB onder zich heeft op het gebied van haar eigen AVG-compliance in de periode van 2018 tot heden. Op basis van de door u op mijn verzoek gegeven nadere specificatie van uw oorspronkelijke verzoek heb ik in de archieven van het KCB gezocht naar de documenten waar het u om gaat.

Ik heb een drietal beleidsterreinen geïdentificeerd die over documenten zouden kunnen beschikken waar uw verzoek op doelt:

1. Directiestukken;
2. PZ-stukken, incl. OR;
3. Kwaliteitsmanagement, incl. FG.

U treft als bijlagen aan de documenten die ik in de drie genoemde directories gevonden heb. Daarbij gevoegd een inventarislijst waarbij vermeld is onder welke van de drie terreinen het document valt, welke zoektermen gebruikt zijn en een volgnummer per document.

Op verzoek van de Rechtbank, aan wie ik deze brief incl. het bijgevoegde ook stuur in verband met uw beroepsschrift, is de set documenten op chronologische volgorde (van oud naar nieuw) gelegd. De volgnummers zijn (daardoor) niet opvolgend.

Daar waar ik dat nodig achtte, heb ik de documenten geanonimiseerd/gelakt. Het betreft dan zaken die ik als persoonsgegevens zie, gegevens die naar een persoon herleidbaar (kunnen) zijn. Concreet gaat het daarbij onder andere om namen, functies (wanneer er daar maar één bekleeder van is binnen het KCB), telefoonnummers en e-mailadressen.

Verder heb ik in enkele documenten, zoals de risico-matrix en directie-beoordelingen, passages weggelaten/gelakt die geen onderdeel uitmaken van uw verzoek.



Het KCB is niet aanbestedingsplichtig. Daardoor kan ik daarover geen documenten openbaar maken. Ten aanzien van de door u gevraagde documenten DPIA en PIA: deze moeten opgesteld worden wanneer daar aanleiding voor is. Daarvoor is tot op heden bij het KCB evenwel geen aanleiding geweest. Daardoor maak ik daarover ook geen documenten openbaar.

Met vriendelijke groet,

KWALITEITS-CONTROLE-BUREAU

Bijlagen: openbaar gemaakte stukken naar aanleiding van uw Woo-verzoek met bijbehorende inventarislijst

Wanneer u het niet eens bent met dit besluit, dan kunt u hiertegen bezwaar aantekenen. Dit bezwaar dient binnen zes (6) weken na dagtekening van deze brief schriftelijk ingediend te zijn bij Stichting KCB, t.a.v. de afdeling bezwaarschriften, postbus 420, 2700 AK Zoetermeer. Voor meer informatie over het indienen van een bezwaarschrift zie de website van het KCB (www.kcb.nl): type in het zoekvak 'bezwaar' in.

[illegible]

KWALITEITS CONTROLE BUREAU			
Titel: Rolomschrijving Functionaris Gegevensbescherming			
Doc.nr.: Roms 04	Versie 01	Datum: 30.03.2018	Blad 1 van 2

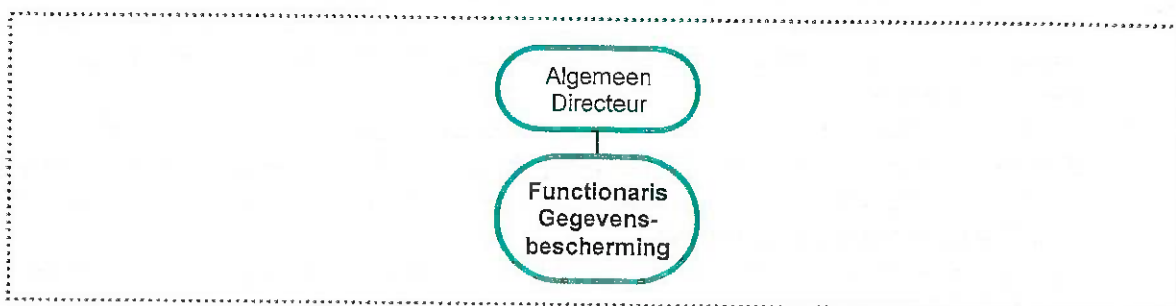


1. Doel

Doel van de rol is het toezicht houden op de toepassing en naleving van de Algemene Verordening Gegevensbescherming (AVG).

2. Plaats in de organisatie

De Functionaris Gegevensbescherming (FG) heeft primair een andere functie waarbij de hiërarchische lijn al is vastgesteld. In de rol van FG wordt de functionaris operationeel aangestuurd door de Algemeen Directeur.



3. Verantwoordelijkheden

De Functionaris Gegevensbescherming is verantwoordelijk voor het uitvoeren van maatregelen gericht op de toepassing en naleving van de Algemene Verordening Gegevensbescherming binnen het KCB.

4. Werkzaamheden

- Het informeren en adviseren van de verwerkingsverantwoordelijke en/of de medewerkers die verwerken, over hun verplichtingen m.b.t. de AVG
- Het toezien op naleving (meldplicht datalekken; verwerkersovereenkomst) van de AVG en andere regelgeving en van het beleid van de organisatie met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking (privacy by design) en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- Het verstrekken van advies met betrekking tot de gegevensbeschermingseffect-beoordeling en toezien op de uitvoering
- met de toezichthoudende autoriteit samenwerken;
- optreden als contactpunt voor de toezichthoudende autoriteit

5. Bevoegdheden

	Datum	Naam	Paraaf
Goedgekeurd door proceseigenaar:			
Getekend voor gezien/akkoord door functionaris:			

KWALITEITS CONTROLE BUREAU			
Titel: Rolomschrijving Functionaris Gegevensbescherming			
Doc.nr.: Roms 04	Versie 01	Datum: 30.03.2018	Blad 2 van 2



De Functionaris Gegevensbescherming is bevoegd tot:

- Het aanspreken van collega's met betrekking tot de AVG;
- Het geven van voorlichting en instructies, bijvoorbeeld in een werkoverleg.

6. Bijzondere omstandigheden

De rol van Functionaris Gegevensbescherming heeft een onafhankelijke en zelfstandige positie ten opzichte van de werkgever.

- De FG ontvangt geen instructies met betrekking tot de uitvoering van die taken.
- Het KCB zorgt ervoor dat de Functionaris Gegevensbescherming naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.
- Het KCB ondersteunt de Functionaris Gegevensbescherming bij de vervulling van zijn/haar taken door hem toegang te verschaffen tot persoonsgegevens en verwerkingsactiviteiten en door hem de benodigde middelen ter beschikking te stellen voor het vervullen van deze taken en het in stand houden van zijn deskundigheid.
- De Functionaris Gegevensbescherming wordt door het KCB niet ontslagen of gestraft voor de uitvoering van zijn taken.

7. Functie-eisen:

- HBO werk- en denkniveau.
- Diploma/certificaat van Privacy Officer.
- Kennis van ter zake gestelde regelgeving op het gebied van privacy.
- Kennis van de ICT systemen.
- De risico's kunnen herkennen.
- Uitstekende sociale vaardigheden.
- Uitstekende schriftelijke en mondelinge uitdrukkingsvaardigheden.
- Uitstekende beheersing van de Nederlandse taal in woord en geschrift.
- Discreet om kunnen gaan met vertrouwelijke gegevens.
- Flexibiliteit en stressbestendigheid.
- Nauwkeurigheid en accuratesse.
- Affiniteit met de agrosector.
- Rijbewijs B.

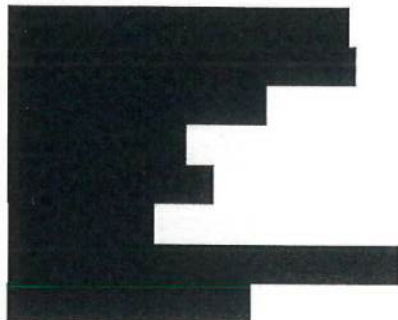
	Datum	Naam	Paraaf
Goedgekeurd door proceseigenaar:			
Getekend voor gezien/akkoord door functionaris:			



KWALITEITS-CONTROLE-BUREAU

Betreft: verslag vergadering bestuur KCB
Datum: 15 mei 2018
Locatie: kantoor KCB te Zoetermeer

Aanwezig:



Afwezig:



1. Opening

█ opent de vergadering en heet de aanwezigen welkom. Van de █ en █ is een bericht van verhindering ontvangen. █ staat stil bij het feit, dat █ voor de laatste keer deelneemt aan de bestuursvergadering.

< alleen de AVG relevante passage is laten staan >

• *Hoofdthema's in 2018; jaarplan*

█ licht toe, dat het document 'Hoofdthema's in 2018; jaarplan' ter informatie is toegezonden. Het document is opgesteld ten behoeve van de communicatie met bijvoorbeeld de pers en het bestuur.

Op een vraag van de █ licht █ toe, dat de eisen vanuit de AVG de aandacht hebben. Er vindt een toets plaats door █. Beseft moet worden, dat het KCB met name werkt met bedrijfsgegevens en zeer beperkt met persoonsgegevens. Hij waakt ervoor, dat de problematiek niet groter wordt gemaakt dan nodig is. Desalniettemin heeft het onderwerp de aandacht en is het van belang te voldoen aan de eisen.

- Export Russische Federatie Export China
- Export Japan
- Export VS
- Ketenmonitoring Citrus ZA
- Import rozen

De hierboven genoemde onderwerpen geven geen aanleiding tot het stellen van vragen of het maken van opmerkingen.



KWALITEITS-CONTROLE-BUREAU

Hoofdthema's in 2018; jaarplan

Inleiding

In 2018 is er sprake van een aantal ingrijpende interne en externe ontwikkelingen die van invloed zijn op de werkzaamheden van het KCB. Van het besluit van Groot-Brittannië om eind maart 2019 de Europese Unie te verlaten, de implementatie van de nieuwe EU-plantgezondheidsverordening tot de ontwikkeling van een nieuw softwaresysteem ter vervanging van het huidige IBP.

In dit jaarplan wordt in hoofdlijnen ingegaan op de wijze waarop het KCB met deze ontwikkelingen zal omgaan. Naast deze 'nieuwe' zaken, zal het KCB gefocust zijn om de standaardprocessen goed te laten verlopen. Centraal hierbij staan de kernwaarden van het KCB: deskundig en betrokken, onafhankelijk, integer en transparant en faciliterend. Het KCB investeert in een efficiënte dienstverlening, kwaliteitszorg en in de kennis en vaardigheden van medewerkers. Hierbij zijn we alert op de ontwikkelingen in een dynamische en professionele markt en sluit het KCB zoveel mogelijk aan bij de logistieke stromen in de keten.

< alleen de AVG relevante passage is weergegeven >

AVG

Per 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Vanaf die datum geldt dezelfde privacywetgeving in de hele EU. Nu hebben de lidstaten nog hun eigen nationale wetten, gebaseerd op de Europese privacyrichtlijn uit 1995.

Het KCB zal de benodigde maatregelen gaan nemen om te kunnen voldoen aan de eisen van de AVG.

5.3

23 mei 2018

[REDACTED]
Verzonden: woensdag 23 mei 2018 09:45

[REDACTED]
Onderwerp: FW: Aanmelding Functionaris voor de gegevensbescherming

Ter info

Met vriendelijke groet,
[REDACTED]

Van: Autoriteit Persoonsgegevens <FG@autoriteitpersoonsgegevens.nl>

Verzonden: woensdag 23 mei 2018 07:43

Aan: Admin [REDACTED]

Onderwerp: Aanmelding Functionaris voor de gegevensbescherming

Geachte heer/mevrouw,

U heeft een functionaris voor de gegevensbescherming (FG) voor uw organisatie Stg. Kwaliteits Controle Bureau aangemeld. Hartelijk dank voor deze aanmelding. Het aan u toegekende FG-nummer is [REDACTED].

Meer informatie over de FG vindt u op <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming>. Zoekt u aanvullende informatie? Dan kunt u hiervoor terecht bij het Nederlands Genootschap voor de Functionaris voor de Gegevensbescherming, het NGFG. Meer informatie over het NGFG vindt u op www.ngfg.nl.

Graag geven wij u nog aanvullende informatie over de positie van de FG binnen uw organisatie:

- u moet de FG genoeg middelen ter beschikking stellen om zijn taken goed te vervullen.
- u mag de FG geen instructies geven over het uitvoeren van de FG-taken; de FG voert zijn taken en verplichtingen onafhankelijk uit.
- de FG mag naast zijn FG-taken eventueel andere taken of functies vervullen, maar er mag geen sprake zijn van belangenverstrengeling.
- u bent verplicht de contactgegevens van uw FG openbaar te maken.

Met vriendelijke groet,



Directeur Systeemtoezicht, beveiliging en technologie



AUTORITEIT
PERSOONSGEGEVENS

FG@autoriteitpersoonsgegevens.nl

T 070 8888 500 - F 070 8888 501

Prins Clauslaan 60, 2595 AJ Den Haag

Postbus 93374, 2509 AJ Den Haag

autoriteitpersoonsgegevens.nl

Rol	Aard gegevens	Vorm (Analoog/ Digitaal)	Interne/ Externe opslag	Bijzondere Persoons gegevens	Grondslag	Risico	Verwerker
Facturatie	Financiële gegevens bedrijven	Digitaal	Intern	Nee	Bedrijfsbelang: Het uitvoeren en financieel afhandelen inspectieaanvragen.	L	
Tijdverantwoording	Tijdregistratie medewerkers	Digitaal	Intern	Nee	Bedrijfsbelang: 1. Het berekenen van tarieven. 2. Het berekenen van toeslagen van overwerk/weekenddiensten. 3. Het genereren van managementinformatie. 4. Verlofadministratie.	L	
Relatiebeheer	NAW gegevens bedrijven en medewerkers	Digitaal	Intern/ Extern	Nee	Wetgeving: Registratie van marktdeelnemers Bedrijfsbelang: Het uitvoeren en financieel afhandelen inspectieaanvragen	L	
Financiële administratie	Financiële gegevens bedrijven en medewerkers	Digitaal	Extern	Nee	Bedrijfsbelang: Financiële verantwoording naar de stakeholders van het KCB (waaronder het Ministerie van LNV)	L	
Beheer wagenpark	NAW gegeven medewerkers, voertuiggegevens, vervoersgegevens	Digitaal	Extern	Nee	Bedrijfsbelang: Beheer van het wagenpark van het KCB.	L	
Salarisadministratie	NAW-gegevens debiteuren	Digitaal	Extern	Nee	Bedrijfsbelang: Het correct uitbetalen van salaris en onkosten Wetgeving: Het inhouden van de premies sociale verzekeringen en belastingen	L	
Mobiele communicatie	Naam, telecom verbruiks- verkeersgegevens	Digitaal	Extern	Nee	Wetgeving: De provider heeft een wettelijke verplichting verkeersgegevens te bewaren. Bedrijfsbelang: Het controleren en verrekenen van privégebruik telefoon	M	
Toegangscontrole KCB locaties	Naam, tijdstip in- en/of uitgaande medewerkers (bij gebruik tag)	Digitaal	Intern	Nee	Bedrijfsbelang: Het gecontroleerd toegang verlenen tot de KCB-locaties.	L	
Toegangscontrole Zoetermeer	Naam, tijdstip in- en/of uitgaande medewerkers (bij gebruik tag)	Digitaal	Intern	Nee	Bedrijfsbelang: Het, in opdracht van de gebouw eigenaar, gecontroleerd toegang verlenen tot de locatie [REDACTED] in Zoetermeer.	L	
Personeelsadministratie	HRM - gegevens	Analoog en digitaal	Intern	Nee	Wetgeving:	H	
Werving- en selectie	CV sollicitanten	Analoog en digitaal	Intern	Nee	Bedrijfsbelang:	H	

Elektronische leeromgeving	Naam, toets resultaten	Digitaal	Extern	Nee	Bedrijfsbelang: Het bijbrengen en toetsen van de kennis van inspecteurs welke noodzakelijk is om inspecties te kunnen uitvoeren.	L	
Papierloos vergaderen	Agenda, verslagen, actie- en besluitenlijsten interne vergaderingen	Ja	Extern	Nee	Bedrijfsbelang: Het papierloos kunnen vergaderen en het archiveren van vergaderstukken.	L	
Smoeleboek	Naam, Foto	Digitaal	Intern	Nee	Bedrijfsbelang: Het herkennen van medewerkers van het KCB.	L	

11 juli 2018

Privacyverklaring

Dit is de privacyverklaring van het Kwaliteits Controle Bureau. In deze privacyverklaring leggen wij uit welke persoonsgegevens wij verzamelen en gebruiken en met welk doel. Wij raden u aan deze verklaring zorgvuldig te lezen. Deze privacyverklaring is voor het laatst aangepast op 29 mei 2018.

Als u naar aanleiding van deze privacyverklaring contact met ons wilt opnemen, dan kan dat via deze contactgegevens:

[REDACTED] is de Functionaris Gegevensbescherming van het KCB. [REDACTED] is te bereiken

[REDACTED]

Het wettelijk kader

- Wet bescherming persoonsgegevens (Wbp). Hierin zijn de belangrijkste regels vastgelegd voor de omgang met persoonsgegevens in Nederland. De Autoriteit Persoonsgegevens houdt toezicht op handhaving van deze wet. Sinds 1 januari 2016 bestaat er ook een verplichting om datalekken te melden.
- Algemene Verordening Gegevensbescherming (AVG). Dit is de EU-verordening die de Wbp vervangt vanaf mei 2018.

Persoonsgegevens die wij verwerken

Het KCB verwerkt uw persoonsgegevens doordat u gebruik maakt van onze (wettelijke) diensten en/of omdat u deze zelf aan ons verstrekt, al dan niet in de functie van werkgever/werknemer. Hieronder vindt u een overzicht van de persoonsgegevens die wij verwerken (indien van toepassing):

- Volledige naam;
- Geslacht;
- Adres;
- Telefoonnummers;
- E-mailadres;
- Geboortedatum;
- Uw betalingsgegevens zoals bankrekening;
- BTW-nummer
- Kamer van Koophandelnummer
- Van (nieuwe) medewerkers: Een kopie van uw identiteitsbewijs;
- Van (nieuwe) medewerkers: uw CV;
- Van (nieuwe) medewerkers: uw motivatiebrief;
- Van (nieuwe) medewerkers: uw opleiding;
- Van (nieuwe) medewerkers: uw BSN-nummer;
- Van medewerkers gegevens over functioneren en beoordelen.

Met welk doel verwerken wij persoonsgegevens

Wij verwerken bovenstaande gegevens voor een of meer van de volgende doeleinden (mede afhankelijk van welke dienst of functionaliteit u gebruikt) om:

- uw betaling af te handelen
- contact met u op te nemen via telefoon of e-mail als dit nodig is om onze dienstverlening uit te kunnen voeren
- u te informeren over wijzigingen van onze diensten en producten
- uw vragen te beantwoorden of uw klachten te behandelen via social media, e-mail, per post of telefonisch
- u een certificaat of bewijs van deelname na een training toe te sturen
- intern beheer van de organisatie
- Uitvoeren van betalingen aan crediteuren;
- Berekening van inkomsten en uitgaven en het laten uitvoeren van accountantscontrole;
- Voeren van salarisadministratie;
- Voeren van medewerkers administratie;
- Nakomen van wettelijke verplichtingen;
- Verwerken van sollicitaties;
- Verwerken van een klacht over een bedrijf of een reactie op een klacht te verwerken;

Geautomatiseerde besluitvorming

Wij nemen op basis van geautomatiseerde verwerkingen geen besluiten over zaken die (aanzienlijke) gevolgen kunnen hebben voor personen. Het gaat hier om besluiten genomen door computerprogramma's of -systemen, zonder dat daar een mens (bijvoorbeeld een medewerker van KCB) tussen zit.

Hoe lang bewaren we persoonsgegevens

Wij bewaren persoonsgegevens niet langer dan noodzakelijk is voor het doel van de gegevensverwerking dan wel op grond van de Archiefwet is vereist. Indien gegevens niet meer worden bewaard worden deze vernietigd.

Delen van persoonsgegevens met derden

KCB gebruikt de verzamelde persoonsgegevens voor de eigen bedrijfsvoering. Daarvoor kan het nodig zijn om persoonsgegevens te delen met organisaties die voor ons werkzaamheden verrichten of waarmee we samenwerken, zoals bijvoorbeeld de arbodienst of het kan zijn dat de NVWA uw gegevens bij ons opvraagt in het kader van onderzoek of rapportage. Met bedrijven die uw gegevens verwerken in onze opdracht, sluiten wij een bewerkersovereenkomst om te zorgen voor eenzelfde niveau van beveiliging en vertrouwelijkheid van uw gegevens. Het KCB blijft verantwoordelijk voor deze verwerkingen.

(Vermoeden van) datalekken

In het geval van een (vermoedelijk) datalek dient u dit direct te melden bij de privacy officer, in dit geval de [REDACTED] van het KCB.

Gegevens inzien, aanpassen of verwijderen

U heeft het recht om uw persoonsgegevens in te zien, te corrigeren of te verwijderen. Daarnaast heeft u het recht om uw eventuele toestemming voor de gegevensverwerking in te trekken of bezwaar te maken tegen de verwerking van uw persoonsgegevens door het KCB en heeft u het recht op gegevensoverdraagbaarheid. Dat betekent dat u bij ons een verzoek kunt indienen om de persoonsgegevens die wij van u hebben in een computerbestand naar u of een ander, door u

genoemde organisatie, te sturen.

U kunt een verzoek tot inzage, correctie, verwijdering, gegevensoverdraging van uw persoonsgegevens of verzoek tot intrekking van uw toestemming of bezwaar op de verwerking van uw persoonsgegevens sturen naar de functionaris gegevensbescherming.

Om er zeker van te zijn dat het verzoek tot inzage door u is gedaan, vragen wij u een kopie van uw identiteitsbewijs met het verzoek mee te sturen. Maak in deze kopie uw pasfoto, MRZ (de strook met nummers onderaan het paspoort), paspoortnummer en Burgerservicenummer (BSN) zwart. Dit ter bescherming van uw privacy. We reageren zo snel mogelijk, maar binnen vier weken, op uw verzoek.

Het KCB wil u er ook op wijzen dat u de mogelijkheid heeft om een klacht in te dienen bij de nationale toezichthouder, de Autoriteit Persoonsgegevens.

Hoe wij persoonsgegevens beveiligen

Wij nemen alle noodzakelijke organisatorische en technische beveiligingsmaatregelen die nodig zijn om misbruik van en ongeautoriseerde toegang tot persoonsgegevens te voorkomen.

Wijzigingen in deze privacyverklaring

Wij kunnen deze privacyverklaring van tijd tot tijd wijzigen. Wijzigingen publiceren wij op onze website. Uw gegevens gebruiken wij nooit zonder toestemming voor andere doeleinden dan waarvoor u ze hebt afgegeven.

© 2018 KCB

Van: [REDACTED]
Verzonden: dinsdag 31 juli 2018 13:32
Aan: [REDACTED]

Onderwerp: update AVG bij het KCB

Beste bestuursleden van het KCB,

In de afgelopen bestuursvergadering is kort gesproken over de implementatie AVG bij het KCB. Het leek mij daarom goed om ter informatie een overzicht te geven, zie bijlage, van de stand van zaken met betrekking tot dit onderwerp.

Met vriendelijke groet,

[REDACTED]



KWALITEITS-CONTROLE-BUREAU

Louis Pasteurlaan 6, 2719 EE Zoetermeer
Postbus 420, 2700 AK Zoetermeer

[REDACTED]

w: www.kcb.nl

Implementatie AVG bij het KCB.

In het kader van de implementatie van de nieuwe AVG per 25 mei 2018 heeft het KCB de volgende zaken ingeregeld.

De wet op de bescherming van persoonsgegevens, de Nederlandse voorloper van deze verordening, bevatte al een heleboel elementen die terugkomen in de nieuwe AVG.

- Er is een beleidsverklaring in het kader van de bescherming van persoonsgegevens opgesteld door directie van het KCB waaruit blijkt dat de privacy belangrijk gevonden wordt. Deze wordt opgenomen in het kwaliteitshandboek.
- De kwaliteitsmanager is tevens als Functionaris gegevensbescherming aangesteld. De functionaris heeft een aparte status binnen het KCB en zal de directie gevraagd en ongevraagd adviseren m.b.t. privacy-aangelegenheden. Tevens is deze persoon geregistreerd als functionaris gegevensbescherming bij de Autoriteit Persoonsgegevens (AP).
- Privacy by design; Het KCB zal bij het ontwerpen en inrichten van procedures en informatiesystemen en gegevensverzamelingen rekening houden met de privacy van personen. Nieuwe procedures, informatiesystemen en/of gegevensverzamelingen zullen worden getoetst op de bescherming van persoonsgegevens alvorens in gebruik genomen te worden.
- Bewustwording van het personeel; De directie van het KCB zal bij het personeel blijvend aandacht vragen voor privacy middels weekbericht of andere (digitale) bulletins.
- Er is een inventarisatie van de KCB-gegevensverzamelingen uitgevoerd. Van elke gegevensverzameling die persoonsgegevens bevat is de rechtmatigheid beoordeeld en indien gerechtvaardigd, het doel, de grondslag en de bewaartermijnen vastgelegd. Daarnaast zijn passende beschermingsmaatregelen genomen. Het KCB heeft slechts een beperkt aantal persoonsgegevens van (oud)medewerkers vastgelegd. Deze gegevens worden op grond van wetgeving verzameld of op basis van een bedrijfsbelang (accreditatie, kwalificatie van de inspecteurs, beheer van het wagenpark). Papieren dossiers (HRM) worden in een afgesloten kast bewaard. Er is een vastgestelde procedure voor inzage in de dossiers en de bewaartermijnen. In de nabije toekomst zullen de dossiers gedigitaliseerd worden middels HRM-software. Dit is onderdeel van het vervangingstraject IBP (inspectie2020). De HRM-gegevens die digitaal zijn vastgelegd zijn versleuteld. Alleen de personeelsfunctionaris/hoofd F&P hebben toegang tot deze bestanden. Persoonsgegevens mbt kwalificatie (toets resultaten) en wagenparkbeheer (gebruik dienstauto's) liggen vast in externe systemen. Ook met deze verwerkers zijn overeenkomsten afgesloten.
- Indien gegevens andere bedrijven gegevens verwerken voor het KCB (bewerken, opslaan, beheren etc.) worden met deze partijen verwerkersovereenkomsten afgesloten. Laatste stand van zaken is dat op 1 na alle partijen die gegevens verwerken (bewerken, opslaan en/of beheren een getekende overeenkomst heeft met KCB.
- Indien het KCB voor andere bedrijven gegevens verwerkt zal het KCB als verwerker ook een overeenkomst af moeten sluiten met de verwerking. Het KCB beheert het toegangssysteem voor de locaties van het KCB. Voor het hoofdkantoor doet het KCB dit ook voor andere in het pand gevestigde organisatie. Dit is op verzoek van FrugiVast. Het KCB zal als verwerker met FrugiVast een verwerkersovereenkomst afsluiten.

[REDACTED]
[REDACTED]

Kwaliteits Controle Bureau	
Kwaliteitssysteem KHB 05.06 Beheer vertrouwelijke (persoons) gegevens	Revisie: 001 Revisiedatum: 24.07.2018 Goedgekeurd door [REDACTED] [REDACTED] Pagina : 1 van 2

1. Doel

In dit document wordt ingegaan op de bescherming van vertrouwelijke (persoons) gegevens in het kader van de Algemene Verordening Gegevensbescherming (AVG).

Het KCB vindt de bescherming van (vertrouwelijke)(persoons)gegevens erg belangrijk en neemt alle redelijke voorzorgsmaatregelen om deze gegevens te beschermen tegen verlies en oneigenlijk/onrechtmatig gebruik. Hierbij worden de te lopen risico's, de inzet van middelen en het effect van de maatregelen afgewogen. Het KCB heeft een aantal richtlijnen opgesteld die ervoor moeten zorgen dat het risico op verlies en oneigenlijk/onrechtmatig gebruik/wijzigen van vertrouwelijke gegevens tot een minimum wordt beperkt.

2. Toepassingsgebied

Het KCB is door de Nederlandse overheid aangewezen als toezichthouder op de naleving van de landbouwkwaliteitswet/ EU-verordening. Om invulling te kunnen geven aan deze opdracht verzamelt het KCB-gegevens van zogenaamde "marktdeelnemers" zijnde producerende en/of in groenten en fruit handelende bedrijven. Ook zijn de KCB-inspecteurs gemandateerd door de Nederlandse Voedsel en Warenautoriteit voor het uitvoeren van fytosanitaire Importinspecties en ontvangt het KCB, ten behoeve van facturatie en processturing, dagelijks gegevens van de, door het KCB, uitgevoerde import- en exportinspecties. Daarnaast beheert het KCB persoonsgegevens ten behoeve van de uitvoering van o.a. Wettelijke bepalingen zoals personeelsbeleid en salarisverwerking en in het kader van de bedrijfsvoering (zoals kwalificatie en opleidingsgegevens).

3. Proceseigenaar

[REDACTED]

4. Verwijzing naar andere documenten (in bezit functionaris gegevensbescherming)

- Document 'bescherming van (vertrouwelijke (persoons) gegevens bij het KCB' (waarin is opgenomen de risico analyse en een overzicht van de naar aanleiding hiervan genomen maatregelen)
- Verwerkingsregister gegevens
- KHB 7.05-bijlage 1 Reglement gebruik ICT faciliteiten van het KCB

5. Werkwijze

5.1 Risico analyse

Het KCB zal bij gewijzigde omstandigheden een risicoanalyse uitvoeren op de verwachte risico's van het verlies en/of oneigenlijk gebruik van (vertrouwelijke)(persoons)gegevens, de mogelijke (imago) schade die het KCB hierbij oploopt en de omvang van de ingezette middelen. Op basis van de uitkomsten van deze risicoanalyse wordt door de directie bepaald welke maatregelen genomen moeten worden en/of het beveiligingsbeleid aangepast dient te worden.

5.2 Functionaris gegevensbescherming (FG)

Kwaliteits Controle Bureau	
Kwaliteitssysteem KHB 05.06 Beheer vertrouwelijke (persoons) gegevens	Revisie: 001 Revisiedatum: 24.07.2018 Goedgekeurd door [REDACTED] [REDACTED] Pagina : 2 van 2

Het KCB heeft een medewerker aangesteld als functionaris gegevensbescherming ([REDACTED]). De functionaris gegevensbescherming beoordeelt gevraagd en ongevraagd of het KCB voldoet aan de bepalingen zoals genoemd in de AVG en rapporteert dit aan de directie. Tevens is de functionaris gegevensbescherming aanspreekpunt bij calamiteiten en coördineert bij incidenten de communicatie met de toezichthouder, de Autoriteit persoonsgegevens en getroffen personen.

5.3 Externe informatiebewerkers

Het KCB sluit met alle externe bewerkers van (vertrouwelijke)(persoons)gegevens waarover het KCB de verantwoordelijkheid draagt een verwerkingsovereenkomst af. Indien externe partijen geen verwerkingsovereenkomst kunnen/willen afsluiten zal het KCB geen toegang verlenen tot (vertrouwelijke)(persoons)gegevens c.q. overdragen van (vertrouwelijke)(persoons)gegevens aan betreffende partij. Periodiek zal het KCB de bewerkers (laten) beoordelen/ garanties vragen aan de bewerkers of zij voldoen aan de voorwaarden zoals beschreven in de verwerkingsovereenkomst.

5.4 Privacy by design

Het KCB zal bij de aanschaf en/of ontwikkeling van ICT-systemen en het aanleggen van gegevensverzamelingen direct de bescherming van (vertrouwelijke)(persoons)gegevens als toetsingscriteria toepassen.

5.5 Bewustwording medewerkers KCB

Het KCB is zich ervan bewust dat, alle technische maatregelen ten spijt, de bescherming van (vertrouwelijke) (persoons) gegevens vooral een zaak is van bewustwording en gedrag van de medewerkers. Het KCB zal daarom de intern aandacht blijven vestigen op het belang van bescherming van (vertrouwelijke) (persoons) gegevens bij de medewerkers van het KCB.

5.6 (Vermoeden van) datalekken

In het geval van een (vermoedelijk) datalek dient dit direct te worden gemeld bij de functionaris gegevensbescherming, in dit geval de [REDACTED]

5.7 Toetsing naleving regels

Toetsing op naleving van de beleidsregels zal worden meegenomen in de interne audits die het KCB jaarlijks uitvoert op het kwaliteitssysteem.

Jaarlijks worden er bij het KCB-audits uitgevoerd door de Raad voor Accreditatie, de accountant en de Nederlandse Voedsel en Warenautoriteit. Op- en aanmerkingen voortvloeiend uit deze audits zullen door het KCB verwerkt worden in de beleidsbepalingen.

Het KCB zal jaarlijks een extern bureau de opdracht verstrekken het beveiligingsniveau van de IT-systemen (technische infrastructuur) te controleren. Het KCB zal de uitkomsten van deze controle gebruiken om het beveiligingsbeleid waar nodig aan te scherpen.

Datum: 6 september 2018

Age Group	Should Take Action (%)	Should Not Take Action (%)
18-29	80	20
30-49	80	20
50-69	80	20
70+	80	20

Response	Percentage
Yes, the U.S. should take action to address climate change	95%
No, the U.S. should not take action to address climate change	5%

[illegible][illegible]



[REDACTED]

- [REDACTED]

- [illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



- [illegible]

- [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]
 [REDACTED]

- [illegible]



- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]

9. Privacy scan

In verband met de nieuwe privacywetgeving dient een privacy scan te worden uitgevoerd.

seft deze scan

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

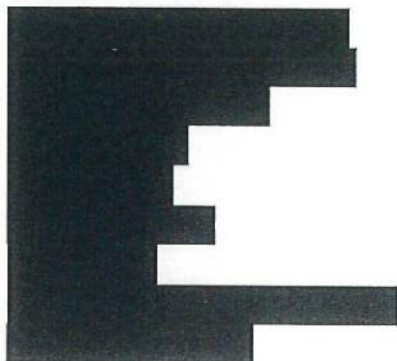
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]



KWALITEITS-CONTROLE-BUREAU

Betreft: verslag vergadering bestuur KCB
Datum: 18 september 2018
Locatie: kantoor KCB te Zoetermeer

Aanwezig:



Afwezig:



1. Opening

█ opent de vergadering en heet de aanwezigen welkom. Een bericht van verhuizing is ontvangen van █.

< alleen de AVG relevante passage is toegevoegd >

2. Verslag vergadering d.d. 6 maart 2018 (BE/5/2018)

Naar aanleiding van:

Pagina 3, onder agendapunt 3 (Ingekomen stukken / uitgegane stukken / mededelingen), 4^e alinea, onder 'Hoofdthema's in 2018; jaarplan', 2^e alinea. █ licht toe, dat hij in de zomer het bestuur via de e-mail een update heeft gegeven over de wijze waarop het KCB de AVG-verplichtingen heeft geïmplementeerd. Vanuit █ is er geen behoefte om aanvullend onderzoek te laten verrichten door een extern bureau.

In relatie tot de AVG merkt █ op, dat het versturen van e-mails naar meerdere personen, waarbij de personen onderling kunnen zien aan wie de e-mail is gestuurd, ook een aandachtspunt is.



KWALITEITS-CONTROLE-BUREAU

Beoordeling van het kwaliteitssysteem door de directie

Beoordelingsperiode: 1 januari 2019 tot en met 31 december 2019

Beoordeling uitgevoerd door [REDACTED], en [REDACTED]

Datum verslag: 15 juni 2020

Informatiebronnen voor de toetsing

Beleidsinformatie

- Kwaliteitshandboek;
 - Statuten en reglementen KCB;
 - Bestuursnotities;
 - Beschrijving controlesystematiek;
 - Reglement Interne Kwaliteitscontrole (RIK) en bijbehorende KCB-kwaliteitscode; •
- Meerjarenovereenkomst Plantkeur.

Concrete bronnen

- Rapportages van de accountantsdienst E&Y;
 - Kwartaalrapportages afdelingen; • Rapportages MT-leden/proceseigenaren;
 - Verslagen bestuursvergaderingen;
 - Verslagen MT-vergaderingen;
 - Verslagen PTO-vergaderingen;
 - Verslagen interne audits;
 - Rapportages audits NVWA;
 - Verslag controlebezoek Raad voor Accreditatie;
 - Aanvraagformulieren corrigerende maatregelen; • Geregistreerde klachten/bezwaren; •
- Uitgevoerde interne controles.

< alleen pagina 6 paragraaf 4d is relevant i.v.m. AVG >

1. INLEIDING [REDACTED]

Het voorliggende rapport is een weergave van de directiebeoordeling van het kwaliteitssysteem en heeft betrekking op de verslagperiode 1 januari 2019 tot en met 31 december 2019. Enkele zaken,

die in de directiebeoordeling zijn beschreven, zijn gebeurtenissen, die na de verslagperiode, doch vóór het schrijven van de directiebeoordeling hebben plaatsgevonden. Hoewel deze zaken na de verslagperiode hebben plaatsgevonden is er omwille van de volledigheid voor gekozen deze zaken toch op te nemen in de directiebeoordeling.

d. Bescherming persoonsgegevens (AVG) [REDACTED]

Het KCB vindt de bescherming van (vertrouwelijke) (persoons)gegevens erg belangrijk en neemt alle redelijke voorzorgsmaatregelen om deze gegevens te beschermen tegen verlies en oneigenlijk/onrechtmatig gebruik. Het KCB heeft in 2018 een aantal richtlijnen opgesteld die ervoor moeten zorgen dat het risico op verlies en oneigenlijk/onrechtmatig gebruik/wijzigen van vertrouwelijke gegevens tot een minimum worden beperkt. In 2019 is een begin gemaakt met de digitalisering van de personeelsdossiers (inscannen files). Hiervoor is met het betreffende bedrijf een verwerkingsovereenkomst afgesloten conform de richtlijnen. In 2020 zal een risicoanalyse worden uitgevoerd m.b.t. de mogelijke risico's van het verlies en/of oneigenlijk gebruik van (vertrouwelijke) (persoons)gegevens door invoering van het nieuwe HR systeem. Nadien zal worden bekeken of de interne richtlijnen moeten worden aangepast. De jaarlijkse controle van het beveiligingssysteem van de IT-systemen is in 2019 uitgevoerd. Naar aanleiding van deze controle zijn er maatregelen genomen.

P1

2019/04/09

Verzoek om instemming voor de digitalisering van personele gegevens

[Redacted text block]

Gevolgen voor de medewerkers en te nemen maatregelen

Beveiliging

Raet heeft in verband met de AVG voor het salarispakket een verwerkingsovereenkomst getekend. Ook voor het HRM pakket zal [Redacted] en verwerkingsovereenkomst tekenen, waardoor 'garandeert dat hun gegevensbeheer aan de AVG voldoet.

[Redacted text block]

[Redacted text block]

[illegible][illegible][illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Aan: [REDACTED]

Van: Directie

Betreft: Integriteit en omgang met persoonsgegevens

Datum: 8 mei 2019

Geachte [REDACTED],

Naar aanleiding van u w brief d.d. 4 april 2019 betreffende integriteit en omgang met persoonsgegevens berichten wij u als volgt.

In verband met de vertrouwelijkheid van uw brief kunnen wij de betrokken medewerkers niet benaderen en het beschreven voorval daardoor niet onderzoeken.

Hieronder is beschreven hoe de privacy bij het KCB wordt geborgd en welke acties op dat vlak zullen worden ondernomen naar aanleiding van uw brief.

Het KCB geeft aan de bescherming van persoonsgegevens een hoge prioriteit. Dat blijkt uit het feit dat dit is vastgelegd in verschillende procedures. Het KCB zal er zorg voor dragen dat de ze procedures bij alle medewerkers bekend zijn. Speciaal bij sollicitatieprocedures zal strikt worden nageleefd dat ieder lid van de sollicitatiecommissie tekent voor geheimhouding. Het belang van geheimhouding zal zowel bij de start als bij het einde van de sollicitatieprocedure nogmaals wordt en benadrukt door de aanwezige medewerker van PZ. Ook zal worden benadrukt dat documenten/gegevens m.b.t. de sollicitatie niet mogen worden verspreid en na afloop van de procedure moeten worden vernietigd of teruggegeven aan PZ.

Gegevens van afgewezen sollicitanten, zowel intern als extern, worden direct na afloop van de sollicitatieprocedure vernietigd door PZ. Alle en van AB -sollicitanten worden de gegevens van sollicitanten die wel geschikt zijn, maar waarvoor op dat moment geen plek is, in portefeuille gehouden. Dit gebeurt na toestemming van de betreffende sollicitant. Deze procedure moet nog worden beschreven, maar de werkwijze wordt feitelijk al toegepast. De te bewaren persoonsgegevens mogen alleen worden bewaard op het hoofdkantoor door PZ. Het is niet toegestaan persoonsgegevens te bewaren op andere plekken binnen de organisatie.

Binnenkort zal de personeelsadministratie worden geautomatiseerd en worden alle zaken

digitaal bewaard en benaderbaar. In dit systeem is een autorisatiematrix van toepassing. Hierover heeft de OR al eerder een instemmings aanvraag ontvangen. De huidige procedure geheimhouding in het kwaliteitshandboek beschrijft nog niet volledig hoe de geheimhouding van personeelsgegevens dient te zijn.

Het in de brief genoemde schaduw dossier van medewerkers dat 1 er kennelijk op naield, zal worden opgevraagd en vernietigd door PZ.

Bij het in gebruik nemen van het I HR-systeem zal erop worden toegezien dat alle punten voldoen aan de AVG.

Wij verwachten hiermee uw vragen afdoende te hebben beantwoord.

Met vriendelijke groet,

[Redacted signature block]



KWALITEITS-CONTROLE-BUREAU

Beoordeling van het kwaliteitssysteem door de directie

Beoordelingsperiode: 1 januari 2019 tot en met 31 december 2019

Beoordeling uitgevoerd door [REDACTED], en [REDACTED]
[REDACTED]

Datum verslag: 15 juni 2020

Informatiebronnen voor de toetsing

Beleidsinformatie

- Kwaliteitshandboek;
 - Statuten en reglementen KCB;
 - Bestuursnotities;
 - Beschrijving controlesystematiek;
 - Reglement Interne Kwaliteitscontrole (RIK) en bijbehorende KCB-kwaliteitscode; •
- Meerjarenovereenkomst Plantkeur.

Concrete bronnen

- Rapportages van de accountantsdienst E&Y;
 - Kwartaalrapportages afdelingen; • Rapportages MT-leden/proceseigenaren;
 - Verslagen bestuursvergaderingen;
 - Verslagen MT-vergaderingen;
 - Verslagen PTO-vergaderingen;
 - Verslagen interne audits;
 - Rapportages audits NVWA;
 - Verslag controlebezoek Raad voor Accreditatie;
 - Aanvraagformulieren corrigerende maatregelen; • Geregistreerde klachten/bezwaren; •
- Uitgevoerde interne controles.

< alleen pagina 6 paragraaf 4d is relevant i.v.m. AVG >

1. INLEIDING [REDACTED]

Het voorliggende rapport is een weergave van de directiebeoordeling van het kwaliteitssysteem en heeft betrekking op de verslagperiode 1 januari 2019 tot en met 31 december 2019. Enkele zaken,

die in de directiebeoordeling zijn beschreven, zijn gebeurtenissen, die na de verslagperiode, doch vóór het schrijven van de directiebeoordeling hebben plaatsgevonden. Hoewel deze zaken na de verslagperiode hebben plaatsgevonden is er omwille van de volledigheid voor gekozen deze zaken toch op te nemen in de directiebeoordeling.

d. Bescherming persoonsgegevens (AVG) [REDACTED]

Het KCB vindt de bescherming van (vertrouwelijke) (persoons)gegevens erg belangrijk en neemt alle redelijke voorzorgsmaatregelen om deze gegevens te beschermen tegen verlies en oneigenlijk/onrechtmatig gebruik. Het KCB heeft in 2018 een aantal richtlijnen opgesteld die ervoor moeten zorgen dat het risico op verlies en oneigenlijk/onrechtmatig gebruik/wijzigen van vertrouwelijke gegevens tot een minimum worden beperkt. In 2019 is een begin gemaakt met de digitalisering van de personeelsdossiers (inscannen files). Hiervoor is met het betreffende bedrijf een verwerkingsovereenkomst afgesloten conform de richtlijnen. In 2020 zal een risicoanalyse worden uitgevoerd m.b.t. de mogelijke risico's van het verlies en/of oneigenlijk gebruik van (vertrouwelijke) (persoons)gegevens door invoering van het nieuwe HR systeem. Nadien zal worden bekeken of de interne richtlijnen moeten worden aangepast. De jaarlijkse controle van het beveiligingssysteem van de IT-systemen is in 2019 uitgevoerd. Naar aanleiding van deze controle zijn er maatregelen genomen.