Privacybeeld CIP-Netwerk
en suggesties voor versterking Privacy Governance

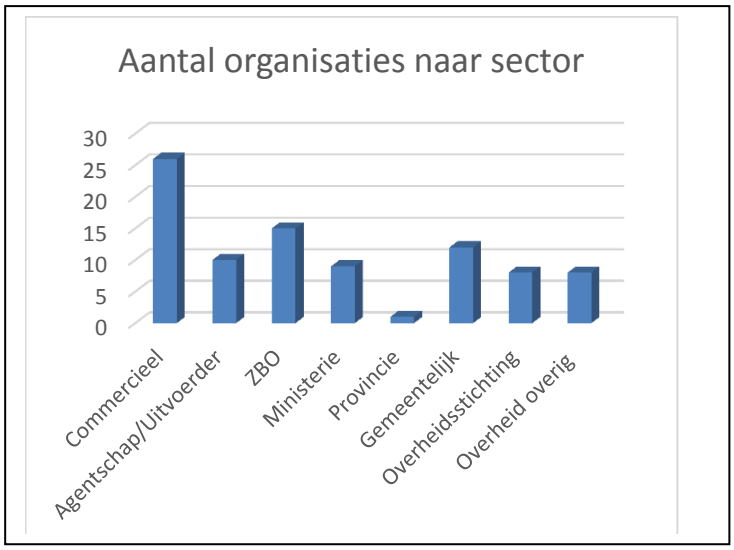
Versie: 1.0

Auteur	CIP
Opdrachtgever	A. Reuijl
Classificatie	Publiek
Status	Afgerond
Datum	5 januari 2016
Filenaam	20160105 Privacy Enquete Analyse-Suggesties/pdf

Inleiding

In november 2015 heeft het CIP, onder zowel overheidsorganisaties als marktpartijen binnen het CIP-netwerk, een enquête uitgezet met vragen over de wijze waarop het thema privacybescherming gestalte krijgt.

Het doel was een beeld op te bouwen van de huidige stand van zaken wat betreft de maatregelen rond de bescherming van persoonsgegevens bij de organisaties in ons netwerk. De uitvraag was daarnaast ook bedoeld om een beeld te krijgen van de behoefte aan de CIP-producten/handreikingen binnen Grip-op-Privacy', zodat daarmee in de jaarplanning rekening kan worden gehouden.



Ca. 40% van de aangeschreven organisaties deden mee: 89 vulden de enquête in (64 overheidsorganisaties en 25 marktpartijen).

De invullingen zijn gedaan door organisaties in verschillende sectoren. Zie het diagram hiernaast voor de aantallen.

Elke respondent hanteert bij het invullen, vanuit de eigen functie en de eigen bedrijfscultuur cq. waardenpatroon zijn eigen referentiekader. De resultaten van de enquête kunnen daardoor niet zo maar op een hoop worden gegooid. Uitspraken met een statistisch onderbouwde pretentie zijn dan ook niet mogelijk.

Uit de antwoorden kan echter wél een algemeen beeld van de situatie worden opgemaakt. En uit dit beeld kunnen ook suggesties worden ontleend om de governance op privacy te verbeteren binnen de eigen organisatie. Hieronder volgt dan ook per hoofdthema van de enquête een korte duiding van de cijfers en suggesties voor aanvullende maatregelen t.b.v. de versterking van de privacy-governance.

De kwantitatieve uitkomsten van de enquête zijn als overzicht van cijfers en grafieken in de bijlage opgenomen. Daarin zijn overheid en markt steeds apart zichtbaar.

Bestuurlijk bewustzijn en Privacybeleid.

Dit hoofdthema betreft een aantal vragen over de verankering van privacy in het beleid en verantwoording.

Wat opvalt, is dat marktorganisaties vaker dan overheidsorganisaties aangeven dat privacy een plaats heeft in beleid en de vertaling naar acties/maatregelen.

Bij de vraag naar het gebruik van normenkaders of gedragscodes, valt op dat vrijwel alle organisaties ofwel volstaan met een verwijzing naar de Wbp, ofwel een eigen normenkader gebruiken. Onder degenen die aangeven een branche-specifieke gedragscode te hanteren (11 stuks) verwijzen de meesten naar kaders als BIR en BIG. Feitelijk zijn dat geen kaders met duidelijke privacy-richtlijnen.

De feitelijke afwezigheid van breder bruikbare kaders, wordt weerspiegeld in de behoefte daaraan, zoals blijkt in de laatste vraagcategorie: de peiling naar de behoefte aan ondersteuning.

Uitzonderlijk weinig organisaties besteden aandacht aan Privacy in hun jaarverslag. Ook verantwoording naar de toezichthouder gebeurt slechts in een derde van de situaties.

Wel volgt bijna iedereen de ontwikkelingen in de wetgeving. Uit het totaalbeeld valt echter op te maken dat de vertaling naar zichtbare concrete maatregelen in veel gevallen achter blijft.

Suggesties
Voor het zichtbaar maken adviseren we de verantwoordelijkheid op te hangen in één van de bestuursportefeuilles. Ook het opnemen in het jaarverslag van een paragraaf, over hoe aandacht wordt gegeven aan de bescherming van persoonsgegevens, draagt hieraan bij.

Voor het privacy-bewust handelen is het nodig om van het privacy-beleid vertalingen te maken voor de mensen die daar elke dag mee te maken hebben. Weliswaar wordt de wetgeving juridisch op de voet gevolgd, de vertaling naar en sturing op het handelen in de organisatie kan in veel gevallen nog verbeteren.

CIP-handvatten die om niet gebruikt kunnen worden zijn:
- Privacy Baseline;
- Meldplicht Datalekken;
- Enkele practices over hoe meldplicht in de organisatie te regelen.

- Veranker de verantwoordelijkheid voor privacy in één van de bestuursportefeuilles.
- Neem een paragraaf over privacy op in het jaarverslag.
- Maak privacy hanteerbaar door concrete vertalingen van privacy-beleid te gebruiken. Beschikbare handvatten van CIP:
  - Privacy Baseline
  - Meldplicht Datalekken.

Privacy-organisatie

Ca. 40% van de respondenten geeft aan dat een privacy-organisatie is ingericht met vastgelegde verantwoordelijkheden. Een Functionaris Gegevensbescherming is slechts bij 29 van de 89 respondenten aangesteld. In overheid en markt is deze verhouding ongeveer gelijk.

Slechts een kwart van de respondenten geeft aan dat er gerapporteerd wordt of voldaan wordt aan een normenkader voor de verwerking van persoonsgegevens. De voorzichtige conclusie mag getrokken worden dat de governance op privacy bij het overgrote deel van de organisaties nog niet werkend is ingericht.

Suggesties
Nu de wet meldplicht datalekken in werking in gegaan en ook tot de Europese Algemene Verordening Gegevensbescherming (AVG) is besloten, nemen de risico's van nalatig handelen drastisch toe. De boetes zijn aanzienlijk en kunnen bij bekendwording ook tot behoorlijke imagoschade leiden.

Het komt erop aan privacy te gaan beschouwen als een expliciet te managen thema. Zorgvuldig handelen vereist een goed 'Privacy Management'. Een datalek is op zichzelf niet boetewaardig, maar onzorgvuldig handelen, kan snel de vraag naar verwijtbaarheid doen rijzen.

We raden dus aan om zowel een zichtbare privacy-organisatie in te richten als ook het toezicht intern te verankeren, bij voorkeur door het benoemen van een Functionaris Gegevensbescherming (in AVG-termen: een Privacy Officer) en het vaststellen en hanteren van een normenkader.

- Richt een zichtbare privacy-organisatie in en veranker het toezicht, bij voorkeur door
  - het benoemen van een Functionaris Gegevensbescherming (Privacy Officer)
  - en het vaststellen en hanteren van een normenkader. Hiervoor kan de Privacy Baseline dienst doen of als basis gehanteerd worden.

Risicomanagement, incident- en crisisbeheersing.

Ruim 60% van de respondenten geeft aan dat bewuste risico-afwegingen worden gemaakt d.m.v. inzet van PIA's en - meer algemeen – bij de beleidsvorming.

Crisisplannen zijn er bij iets minder dan de helft van de respondenten. De oefening met die plannen vindt slechts plaats bij een kwart van de organisaties.

Suggesties

We raden aan om privacy uitdrukkelijk mee te nemen in bestaande crisisplannen/crisisorganisaties. Bijvoorbeeld die van Business Continuity of Cyber Security. Die zullen in veel gevallen wel moeten worden uitgebreid.

Regelmatig oefenen is nodig om te kunnen schakelen bij crisis. Voorkomen moet worden dat er dan allerlei onduidelijkheden blijken. CIP heeft hiervoor een handzame Serious Game ontwikkeld, die om niet gebruikt kan worden.

- Neem privacy mee in bestaande crisisplannen/crisisorganisaties
- Oefen regelmatig. Voor een laagdrempelige oefening: CIP-Serious Game 'Crisis'.

Leren en ontwikkelen

55% van de overheidsorganisaties geeft aan in te zetten op leren en ontwikkelen. Marktorganisaties scoren deze vraag aanmerkelijk positiever: ca. 85% geeft aan te investeren in leren en ontwikkelen.

De werkvormen in volgorde van meest frequent gebruikt (overheid en markt samen).

1. Publicaties (42 keer genoemd)
2. Meenemen in het werkoverleg (40 keer genoemd)
3. Trainingen (24 keer genoemd)
4. Workshops (23 keer genoemd)
5. E-Learning (18 keer genoemd).

Suggesties

Middelen als workshops, werkoverleg en training (dus met direct, persoonlijk contact) zien we als het effectiefst. Zaken als publicaties en e-Learning zijn vooral nuttig in combinatie met meer persoonlijke interventies.

De effectiviteit van de ingezette middelen, kan verder versterkt worden als het thema privacy ook wordt geadresseerd in de HR-/Beoordelingscyclus. Daarmee houdt je het ook individueel op de agenda.

- Kies zoveel mogelijk voor leerinterventies met persoonlijke impact en ondersteun die met schriftelijk materiaal.
- Neem Privacy-bewust handelen op als beoordelingscriterium in de HR-Cyclus.

Inhoudelijke ondersteuning

In deze vraagcategorie wordt de behoefte aan reeds aanwezige of toekomstige CIP-producten gepeild. De beantwoording maakt duidelijk dat de producten wel in de behoefte van een flink deel van de organisaties voorzien. Ca. 60% geeft aan een normenkader en een handreiking voor privacy governance te wensen; 65% geeft aan behoefte te hebben aan een handreiking Privacy by Design.

Meer dan 80% van de respondenten ziet een vraagbaakfunctie als welkome dienst. Een kleine 40% geeft aan daar ook wel op beperkte schaal aan te willen meewerken.

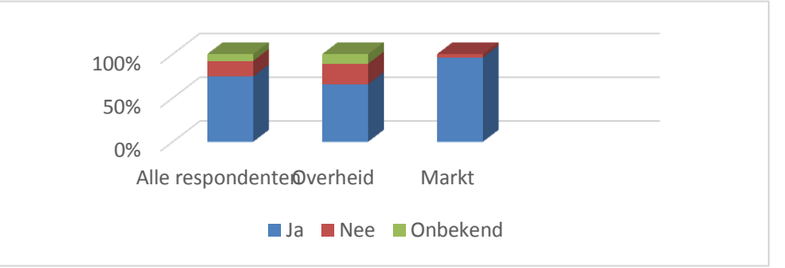
Het voornemen van CIP is dan ook dat wij doorgaan met de genoemde producten en diensten. In 2016 zullen wij ook de nodige sessies beleggen om deze onder de aandacht te brengen.

Bijlage: Privacy Enquête / Cijfers en grafieken

BESTUURLIJK BEWUSTZIJN / PRIVACYBELEID

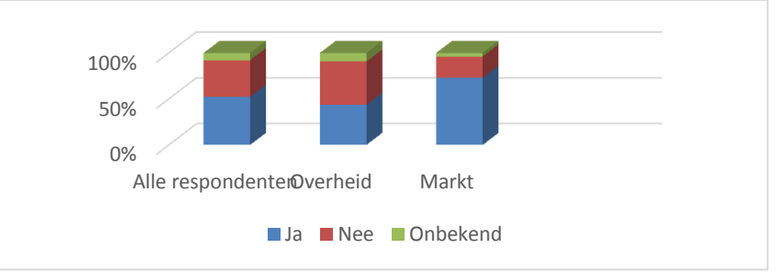
Maakt privacy onderdeel deel uit van de missie, visie en het beleid van uw organisatie?

	Ja	Nee	Onbekend
Alle respondenten	67	16	7
Overheid	42	15	7
Markt	25	1	



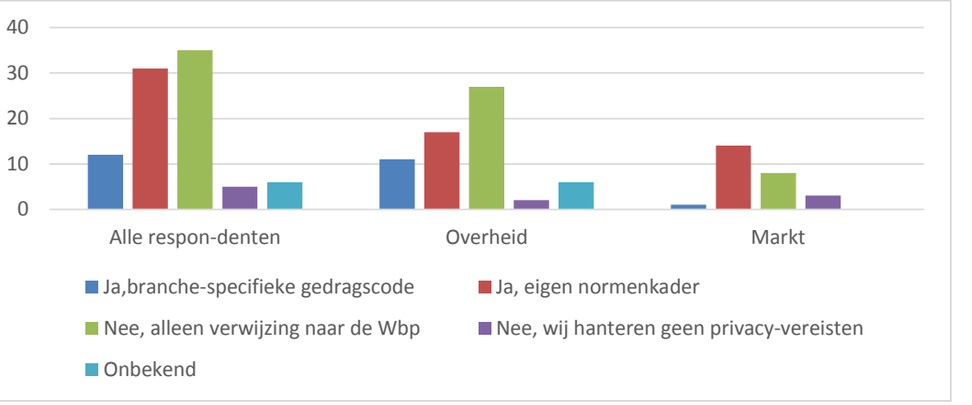
Heeft uw organisatie een plan opgesteld waarin het privacybeleid wordt geconcretiseerd in te nemen maatregelen, met tijdspad, benodigde middelen, etc?

	Ja	Nee	Onbekend
Alle respondenten	47	36	7
Overheid	28	30	6
Markt	19	6	1



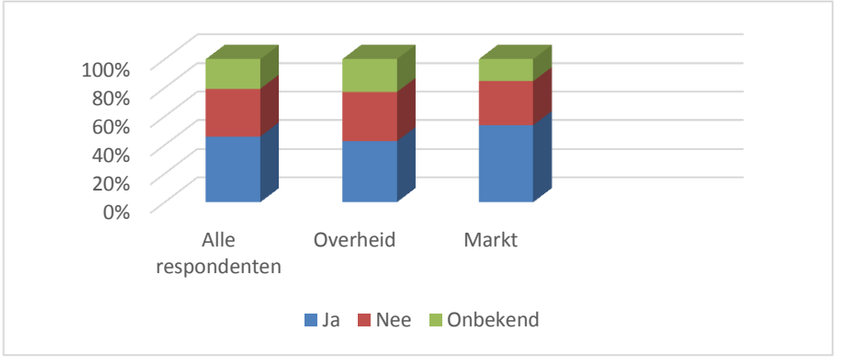
Hanteert uw organisatie een normenkader of gedragscode, waarin de Wet bescherming persoonsgegevens nader is gespecificeerd voor uw branche of organisatie?

	Alle respon-denten	Overheid	Markt
Ja,branche-specifieke gedragscode	12	11	1
Ja, eigen normenkader	31	17	14
Nee, alleen verwijzing naar de Wbp	35	27	8
Nee, wij hanteren geen privacy-vereisten	5	2	3
Onbekend	6	6	



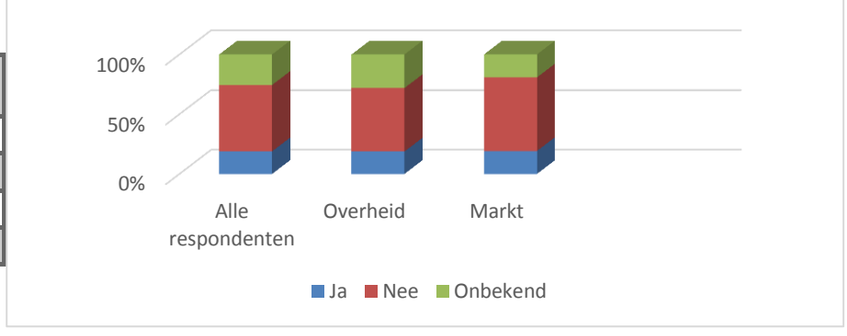
Is privacy expliciet belegd in een van de bestuursportefeuilles?

	Ja	Nee	Onbekend
Alle respondenten	40	29	18
Overheid	26	21	14
Markt	14	8	4



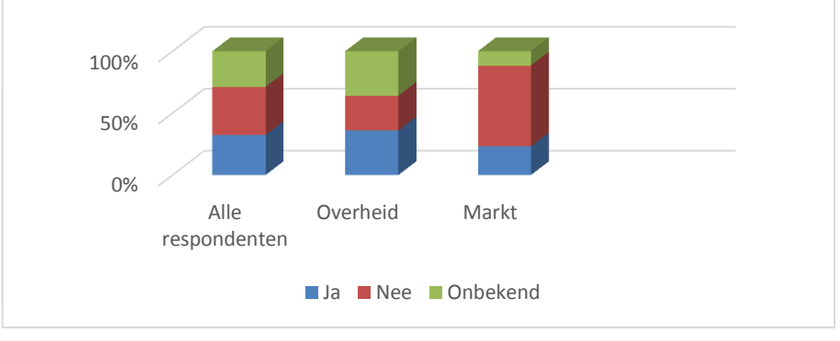
Heeft uw organisatie in het jaarverslag een paragraaf aangaande privacy opgenomen?

	Ja	Nee	Onbekend
Alle respondenten	17	50	23
Overheid	12	34	18
Markt	5	16	5



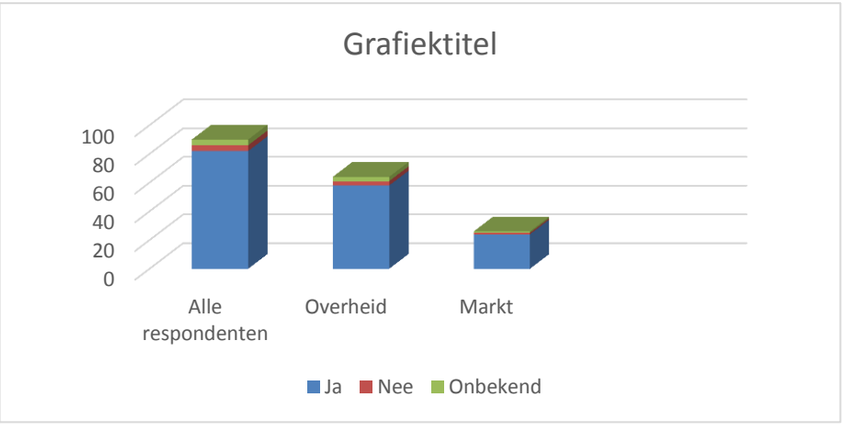
Komt privacy als thema aan de orde in de afstemming met het departement of toezichthouder ?

	Ja	Nee	Onbekend
Alle respondenten	29	35	26
Overheid	23	18	23
Markt	6	17	3



Worden de (juridische) ontwikkelingen op het gebied van privacy gevolgd (zoals de Meldplicht Datalekken en de Europese Algemene Verordening Gegevensbescherming) en wordt hier op geanticipeerd?

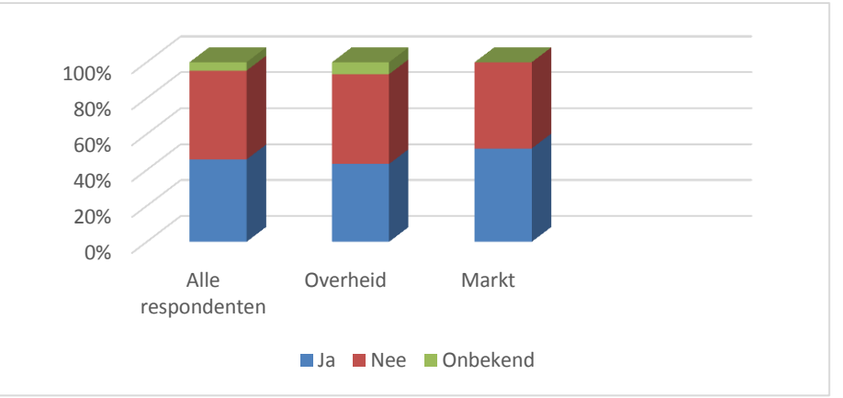
	Ja	Nee	Onbekend
Alle respondenten	82	4	4
Overheid	58	3	3
Markt	24	1	1



PRIVACY ORGANISATIE

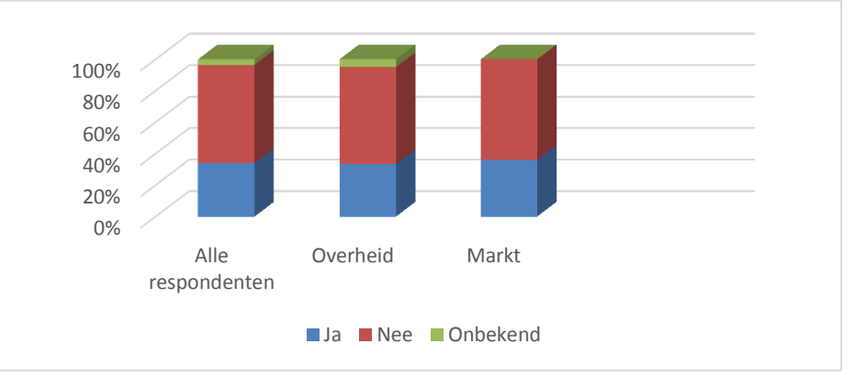
Heeft uw organisatie een privacy-organisatie ingericht, waarbinnen de verantwoordelijkheden voor privacy vastliggen?

	Ja	Nee	Onbekend
Alle respondenten	39	42	4
Overheid	26	30	4
Markt	13	12	0



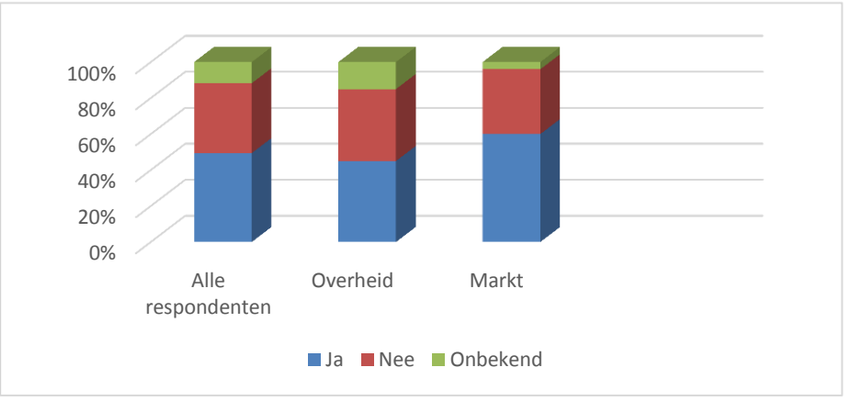
Heeft uw organisatie een Functionaris Gegevensbescherming aangesteld?

	Ja	Nee	Onbekend
Alle respondenten	29	53	3
Overheid	20	37	3
Markt	9	16	0



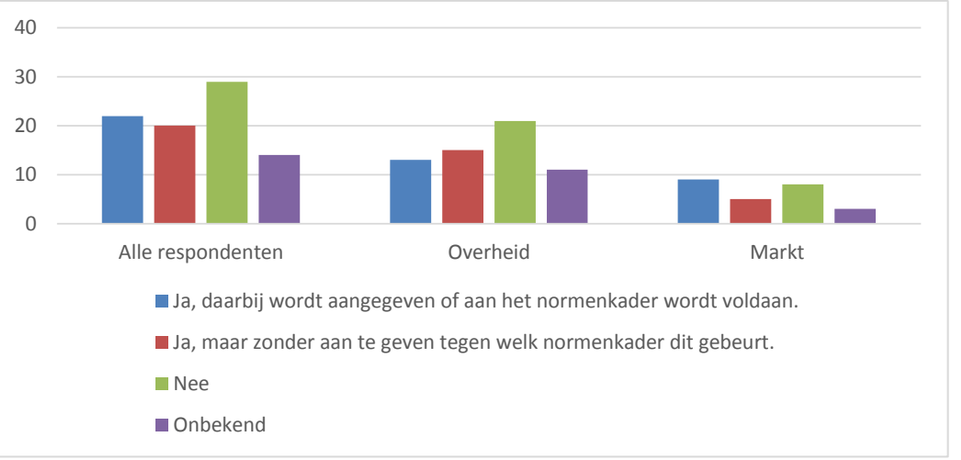
Heeft uw organisatie vastgelegd hoe moet worden omgegaan met privacyvraagstukken bij het ontwerp van de gegevensverwerking?

	Ja	Nee	Onbekend
Alle respondenten	42	33	10
Overheid	27	24	9
Markt	15	9	1



Rapporteren de verantwoordelijken voor de verwerking van persoonsgegevens over hoe persoonsgegevens (conform een normenkader) verwerkt worden?

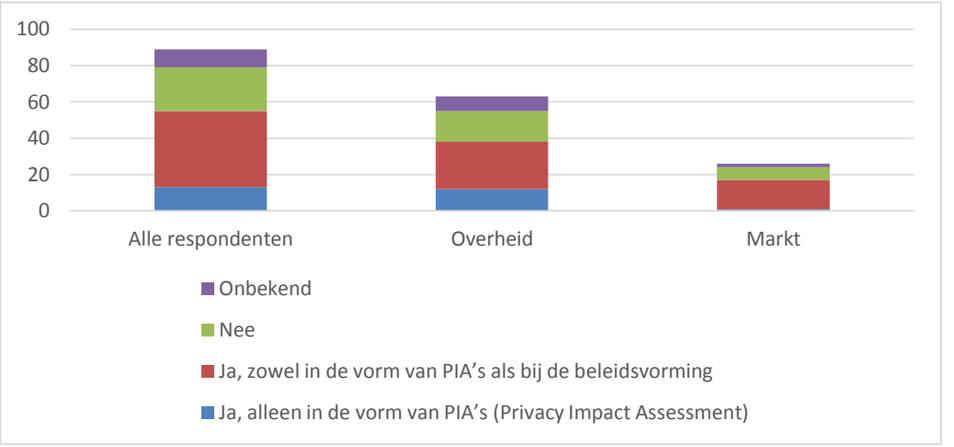
	Alle respondenten	Overheid	Markt
Ja, daarbij wordt aangegeven of aan het normenkader wordt voldaan.	22	13	9
Ja, maar zonder aan te geven tegen welk normenkader dit gebeurt.	20	15	5
Nee	29	21	8
Onbekend	14	11	3



RISICOMANAGEMENT, INCIDENT- EN CRISISBEHEERSING

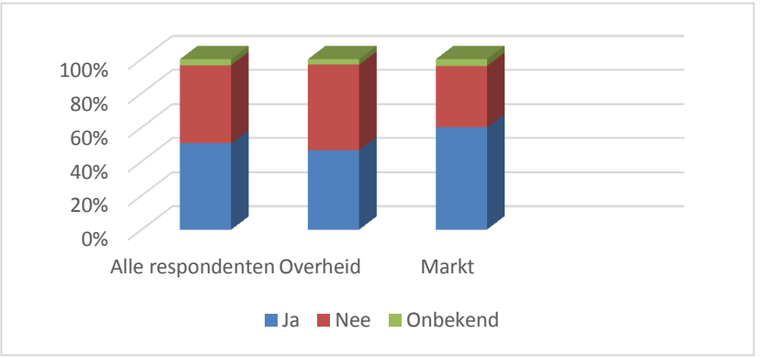
Baseert uw organisatie zich bij de bescherming van privacy op bewuste risicoafwe-gingen?

	Alle respondenten	Overheid	Markt
Ja, alleen in de vorm van PIA's (Privacy Impact Assessment)	13	12	1
Ja, zowel in de vorm van PIA's als bij de beleidsvorming	42	26	16
Nee	24	17	7
Onbekend	10	8	2



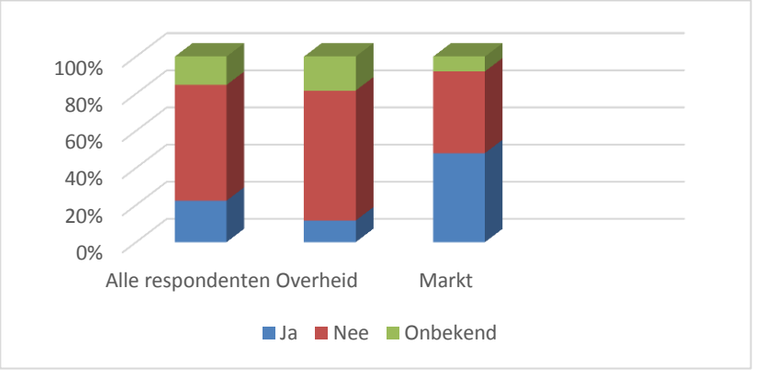
Heeft uw organisatie een crisisplan ingericht om calamiteiten op het gebied van privacy (zoals datalekken) het hoofd te kunnen bieden?

	Ja	Nee	Onbekend
Alle respondenten	43	39	3
Overheid	28	30	2
Markt	15	9	1



Worden crisisplannen op het gebied van privacy periodiek getoetst en geoefend?

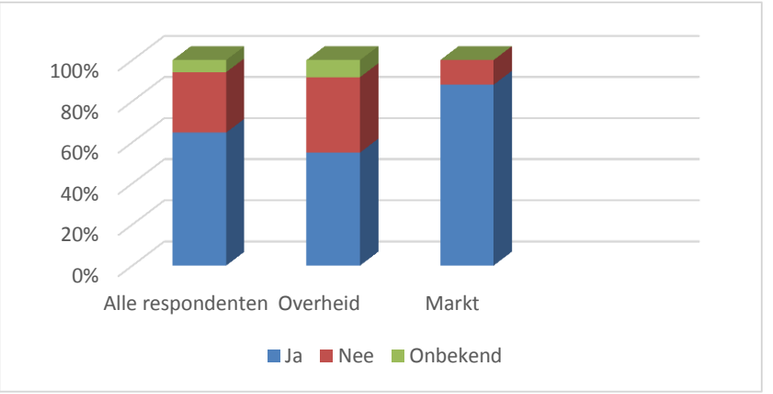
	Ja	Nee	Onbekend
Alle respondenten	19	53	13
Overheid	7	42	11
Markt	12	11	2



LEREN EN ONTWIKKELEN

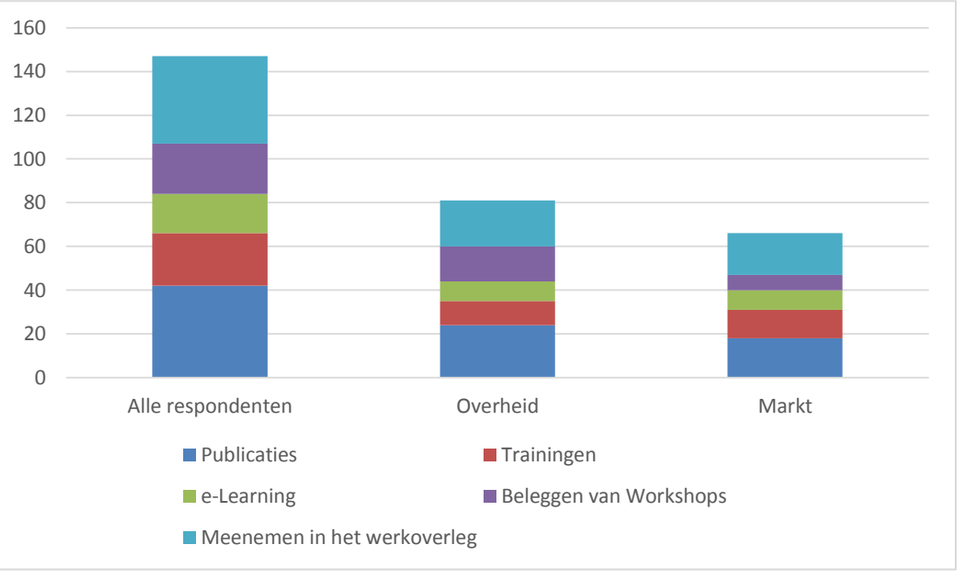
Zet uw organisatie in op blijvend 'privacy-bewustzijn' bij haar medewerkers door middel van leren en ontwikkelen?

	Ja	Nee	Onbekend
Alle respondenten	55	25	5
Overheid	33	22	5
Markt	22	3	0



Onder de middelen die organisaties hierbij inzetten, zijn publicaties en werkoverleggen duidelijk favoriet:

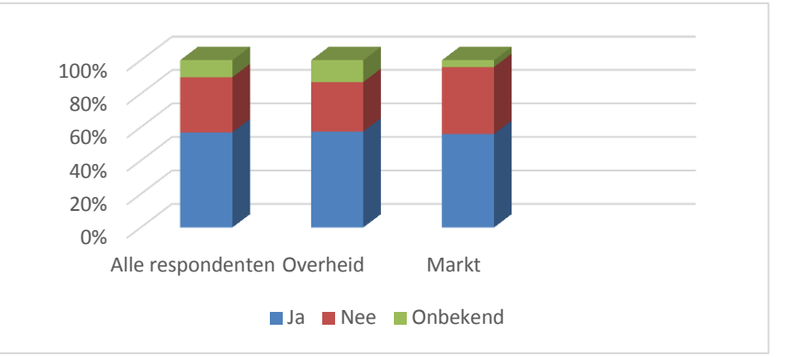
	Alle respondenten	Overheid	Markt
Publicaties	42	24	18
Trainingen	24	11	13
e-Learning	18	9	9
Beleggen van Workshops	23	16	7
Meenemen in het werkoverleg	40	21	19



INHOUDELIJKE ONDERSTEUNING

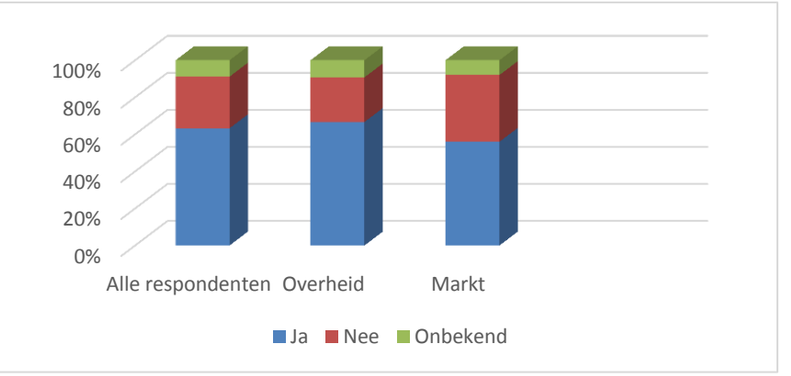
Heeft uw organisatie behoefte aan een normenkader, waarbij de Wet bescherming persoonsgegevens eenvoudiger toegankelijk is?

	Ja	Nee	Onbekend
Alle respondenten	45	26	8
Overheid	31	16	7
Markt	14	10	1



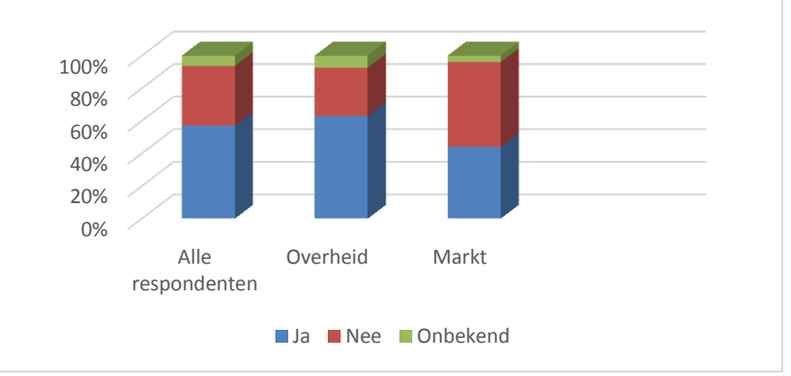
Heeft uw organisatie behoefte aan een handreiking Privacy by Design (om privacy mee te nemen bij de ontwikkeling van gegevensverwerkingen)?

	Ja	Nee	Onbekend
Alle respondenten	50	22	7
Overheid	36	13	5
Markt	14	9	2



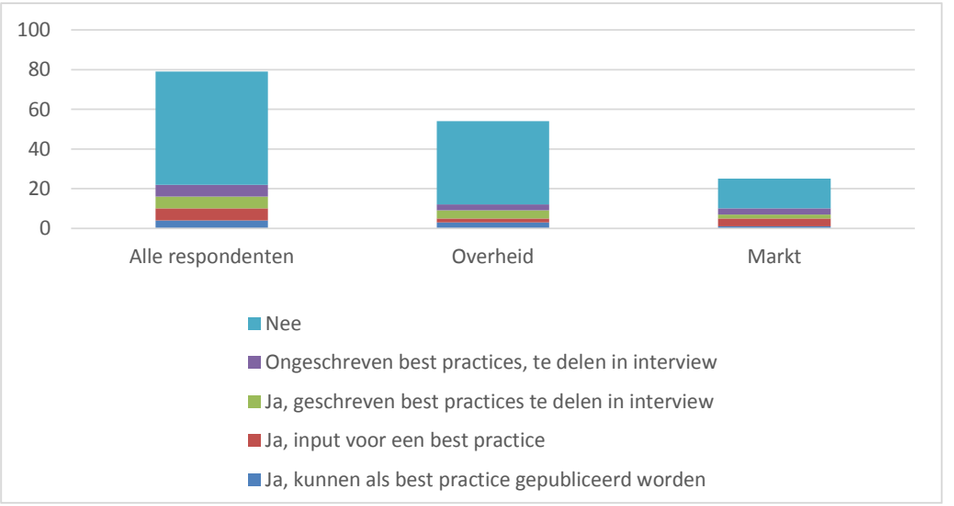
Heeft uw organisatie behoefte aan een handreiking om de governance op privacy binnen de organisatie in te richten?

	Ja	Nee	Onbekend
Alle respondenten	45	29	5
Overheid	34	16	4
Markt	11	13	1



Hanteert u binnen uw organisatie best practices (bijv. op het gebied van privacybeleid, normenkaders, organisatorische maatregelen) die u wilt delen met anderen in de CIP gemeenschap?

	Alle respondenten	Overheid	Markt
Ja, kunnen als best practice gepubliceerd worden	4	3	1
Ja, input voor een best practice	6	2	4
Ja, geschreven best practices te delen in interview	6	4	2
Ongeschreven best practices, te delen in interview	6	3	3
Nee	57	42	15



Het CIP neemt zich voor een vraagbaakfunctie in te richten waar CIP-deelnemers terecht kunnen met vragen op het gebied van privacy. De opzet die ons voor ogen staat is de volgende. Iedereen in het CIP-netwerk kan vragen stellen; wij zorgen ervoor dat de vragen beantwoord worden door gebruikmaking van kennis die in datzelfde netwerk voorhanden is.

	Alle respondenten	Overheid	Markt
Geen behoefte aan	12	8	5
Welkome functie; niet zelf bijdragen	36	20	16
Welkome functie; wij kunnen ook zelf bijdragen	30	16	14