

Onderstaand vindt u per vraag van de Quickscan een korte toelichting op de antwoordmogelijkheden. Via deze toelichting kunt u nagaan welke betekenis het door u gegeven antwoord heeft voor uw organisatie. Tevens kunt u bepalen welke vervolgstappen nuttig zijn.

De vragenlijst is beknopt en gaat niet in op alle aspecten van de bescherming van persoonsgegevens, zoals geregeld in de Wet bescherming persoonsgegevens (WBP). Dit geldt ook voor de toelichting op de antwoordmogelijkheden. Voor een aantal vragen is bij het antwoord 'nee', ter verduidelijking, een voorbeeld opgenomen van een situatie die niet in overeenstemming is met de WBP. In deze toelichting worden de termen privacybescherming en bescherming van persoonsgegevens door elkaar gebruikt. Ze zijn te beschouwen als synoniemen.

Als u naar aanleiding van het invullen van de Quickscan of de toelichting op de antwoorden nog vragen heeft, kunt u contact opnemen met een adviseur van het College bescherming persoonsgegevens (CBP), telefonisch bereikbaar op werkdagen van 09.00 – 12.30 uur, 070 – 3811300.

Toelichting op de antwoordmogelijkheden

Privacybewustzijn in de organisatie

De eerste drie vragen van de Quickscan gaan over het bewustzijn van privacy in de organisatie. Wil een organisatie de privacy van haar personeelsleden en klanten waarborgen dan is het belangrijk dat alle medewerkers zich bewust zijn van zowel de risico's die de privacy kunnen aantasten als de noodzakelijke maatregelen die de privacy moeten waarborgen. Het creëren van privacybewustzijn binnen de organisatie is een eerste stap op weg naar een goede bescherming van de privacy.

1. Is in uw bedrijf voorlichting gegeven over de nieuwe privacywet (WBP)?

- Ja** Dit is een goed teken. De nieuwe privacywetgeving (WBP) kent verschillen ten opzichte van de oude wet. Het is belangrijk dat werknemers op de hoogte zijn van de wettelijke regeling en bekend zijn met de verschillen tussen de oude (WPR) en nieuwe (WBP) wet.
- Nee** Het is aan te bevelen om bij de leiding / directie van de organisatie na te vragen of men bekend is met de nieuwe privacywetgeving en of de organisatie plannen heeft om de gevolgen van deze nieuwe wet voor de eigen organisatie te beoordelen. De WBP kent beperkte overgangstermijnen. Het is goed mogelijk dat er aanvullende of nieuwe maatregelen getroffen moeten worden om aan de eisen van de WBP te voldoen. Daarnaast regelt de WBP dat verwerkingen van persoonsgegevens opnieuw moeten worden aangemeld bij het CBP. U kunt de leiding / directie van uw organisatie attent maken op de "Handleiding voor verwerkers van persoonsgegevens", zoals die door het ministerie van Justitie is opgesteld (www.minjust.nl).

2. Heeft de directie of leiding uitgesproken dat de organisatie de privacy van personen moet respecteren?

- Ja** De leiding of directie is verantwoordelijk voor de bescherming van persoonsgegevens in de organisatie. Het is daarom goed dat de leiding of directie zich expliciet uitspreekt over de bescherming van persoonsgegevens door de organisatie. Een voorbeeldfunctie van leiding of directie werkt positief naar de medewerkers.
- Nee** Het is uiteraard niet verplicht dat de leiding of directie van een organisatie zich expliciet uitspreekt over de bescherming van persoonsgegevens door de organisatie. Een dergelijke uitspraak maakt echter wel duidelijk dat de leiding of directie niet akkoord gaat als de privacy van personen geschonden wordt. U kunt navraag doen binnen uw organisatie hoe men aankijkt / omgaat met de bescherming van persoonsgegevens.

3. Wordt er op uitvoerend niveau binnen uw organisatie aandacht besteed aan privacybescherming?

- Ja** Het is goed dat uw organisatie ook op uitvoerend niveau de privacybescherming onder de aandacht brengt. Het zijn de medewerkers in de organisatie die direct betrokken zijn bij het verwerken van persoonsgegevens die de privacybescherming realiseren / waarborgen.
- Nee** Het realiseren van een goede privacybescherming kan niet door de leiding of directie alleen gebeuren. Alle medewerkers die betrokken zijn bij het verwerken van persoonsgegevens dienen op de hoogte te zijn van wat wel en niet mag volgens de WBP en welke verplichtingen de WBP aan de organisatie oplegt. U kunt bij de leiding of directie van uw organisatie aandringen op speciale aandacht voor privacybescherming op uitvoerend niveau, bijvoorbeeld via voorlichting.

Uitvoering wettelijke bepalingen

De wet legt aan organisaties die persoonsgegevens verwerken bepaalde eisen en verplichtingen op. Tevens kent de wet aan personen van wie persoonsgegevens worden verwerkt bepaalde rechten toe. De naleving van de belangrijkste eisen, verplichtingen en rechten staat centraal in de vragen 4 tot en met 9.

4. Beperkt uw organisatie het verwerken van persoonsgegevens tot de doelstelling(en) waarvoor ze verzameld zijn en doelstellingen die daarmee verenigbaar zijn?

- Ja** De organisatie voldoet hiermee aan de wettelijke eis. Het is overigens goed om van tijd tot tijd voor de verwerkingen te controleren of deze nog plaatsvinden binnen de vooraf gedefinieerde doelstelling(en) of daarmee verenigbare doelstelling(en).
- Nee** Als uw organisatie zich niet houdt aan de oorspronkelijke doelstelling(en) van verwerking of doelstellingen die daarmee verenigbaar zijn dan handelt de organisatie in strijd met de wet. De wetgever wil voorkomen dat persoonsgegevens te pas en te onpas worden gebruikt door organisaties. Het gebruik van persoonsgegevens voor andere doelstellingen dan waarvoor een persoon ze verstrekt heeft, kan bij de verstrekker onvrede oproepen. Als de verstrekker had geweten dat de persoonsgegevens voor een andere doelstelling worden gebruikt, had die ze mogelijk in het geheel niet verstrekt. Het spreekt voor zich dat voor de uitvoering van wettelijke regelingen de noodzakelijke persoonsgegevens altijd verstrekt moeten worden (denk aan het invullen van uw aangiftebiljet voor de belastingdienst of uw aanvraag voor huursubsidie).

5. Vindt het verwerken van persoonsgegevens binnen uw organisatie plaats in overeenstemming met de WBP?

- Ja** De organisatie voldoet hiermee aan de wettelijke bepalingen. Ook nu is regelmatige toetsing van de grondslag zinvol.
- Nee** Indien er voor de verwerkingen van persoonsgegevens binnen uw organisatie geen rechtmatige grondslag is, bent u in overtreding met de wet. De wet benoemt de grondslagen voor het verwerken van persoonsgegevens limitatief. Verwerking mag slechts plaatsvinden als de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend, of de gegevensverwerking noodzakelijk is om een van de volgende redenen:
- voor de uitvoering van een overeenkomst waarbij de betrokkenen partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;
 - om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;
 - ter vrijwaring van een vitaal belang van betrokkene;

- voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt;
 - voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.
- Interpretatie van de hiervoor genoemde redenen is niet altijd even duidelijk. Het kan gewenst zijn om bij twijfel over de rechtmatigheid van de grondslag juridische ondersteuning te vragen.

6. Zijn er regels vastgesteld voor het verwerken van persoonsgegevens binnen uw organisatie?

Ja Zonder regelgeving is het moeilijk om de zorgvuldigheid van het verwerken van persoonsgegevens te waarborgen. Dat er in uw organisatie regelgeving is, is een goede zaak maar dat betekent nog niet dat de verwerking ook zorgvuldig geschiedt. Vastgesteld moet worden of de regels toereikend zijn en of de regels intern ook worden nageleefd (zie vraag 13). De regels zouden het gehele traject van verwerking moeten omvatten.

Nee Als regels voor het verwerken van persoonsgegevens ontbreken kan de organisatie de zorgvuldigheid van het verwerken niet zonder meer waarborgen. Het is belangrijk dat er voor de medewerkers die belast zijn met het verwerken van persoonsgegevens duidelijke werkinstructies zijn. Als regels ontbreken betekent dat niet dat de verwerking niet zorgvuldig gebeurt. De kans op fouten is echter groter dan in het geval er wel duidelijke regels zijn opgesteld en vastgelegd.

7. Zijn er specifieke regels vastgesteld voor het verwerken van bijzondere persoonsgegevens binnen uw organisatie?

Ja Door specifieke regels voor het verwerken van bijzondere persoonsgegevens op te stellen, voorkomt uw organisatie dat de bijzondere persoonsgegevens onrechtmatig worden verwerkt. Uiteraard is het belangrijk ook voor deze regels de naleving regelmatig te controleren.

Nee Het verwerken van bijzondere persoonsgegevens is in de WBP omgeven met strengere eisen. Bijzondere gegevens mogen alleen in een beperkt aantal situaties, zoals in de wet beschreven, verwerkt worden. Om te voorkomen dat bijzondere persoonsgegevens worden verzameld, vastgelegd, verwerkt en verstrekt, zou de organisatie hiervoor duidelijke regels moeten opstellen. Nu deze regels er niet zijn, loopt uw organisatie hier een groter risico om de wettelijke bepalingen te overtreden.

8. Controleert uw organisatie persoonsgegevens op juistheid en volledigheid?

Ja Door persoonsgegevens te controleren op juistheid en volledigheid komt u tegemoet aan de eis van zorgvuldigheid die de wet stelt aan het verwerken van persoonsgegevens. Het is belangrijk om te bepalen of de controle ook effectief is en alle persoonsgegevens afdekt.

Nee Het ontbreken van controle op de juistheid en volledigheid van persoonsgegevens in uw organisatie schept een risico dat persoonsgegevens niet correct zijn. Personen van wie gegevens niet correct verwerkt zijn, kunnen hierover bij uw organisatie klagen en herstel eisen. Door persoonsgegevens te controleren, voorkomt u onnodig administratieve werkzaamheden om persoonsgegevens achteraf te corrigeren.

9. Leeft uw organisatie de informatieplicht naar betrokkenen na?

Ja De organisatie voldoet hiermee aan de wettelijke bepalingen.

Nee De organisatie handelt in strijd met de wet. Betrokkenen hebben er recht op dat u hen, conform de bepalingen van de WBP, informeert voordat u persoonsgegevens verkrijgt, of indien u de persoonsgegevens van derden ontvangt, voordat u deze vastlegt of verstrekt aan anderen. Het is verstandig de leiding of directie te wijzen op deze tekortkoming.

10. Komt uw organisatie de rechten van betrokkenen na?

Ja De organisatie voldoet hiermee aan de wettelijke bepalingen.

Nee Betrokkenen hebben recht op inzage, wijziging en verzet tegen het verwerken van hun persoonsgegevens. De organisatie handelt in strijd met de wet. Het niet naleven van wettelijke bepalingen kan consequenties hebben voor de organisatie. Het is verstandig om de leiding of directie hierop te wijzen.

Beveiliging

De wet stelt expliciet dat de organisatie die persoonsgegevens verwerkt passende technische en organisatorische maatregelen moet treffen om de verwerking van persoonsgegevens te beveiligen tegen onrechtmatige verwerking of verlies.

11. Heeft uw organisatie bevoegdheden aan medewerkers toegekend zodat uitsluitend geautoriseerde medewerkers toegang hebben tot persoonsgegevens?

Ja De organisatie voorkomt dat ongeautoriseerde medewerkers persoonsgegevens kunnen raadplegen of verwerken. Het is overigens wel belangrijk dat de organisatie regelmatig de maatregelen beoordeelt op toereikendheid.

Nee Het risico bestaat dat onbevoegde medewerkers persoonsgegevens raadplegen of verwerken en daarmee schade toebrengen aan de vastgelegde persoonsgegevens of deze onrechtmatig verstrekken.

12. Heeft uw organisatie maatregelen getroffen die verlies en onrechtmatige verwerking van persoonsgegevens tegengaan?

Ja Via deze maatregelen draagt de organisatie bij aan de veiligheid van verwerking van persoonsgegevens.

Nee Naast een goede toegangsbeveiliging tot het geautomatiseerde systeem (zie vraag 11) dienen ook andere maatregelen getroffen te worden om onrechtmatige verwerking of verlies van persoonsgegevens te voorkomen. Voor een overzicht van een adequaat stelsel van maatregelen wordt verwezen naar het document Beveiligen verwerking persoonsgegevens dat elders op deze website is te vinden.

Controle

De goede werking van maatregelen is mede afhankelijk van controle op de naleving / toepassing van de maatregelen.

13. Wordt de naleving van de maatregelen voor privacybescherming binnen uw organisatie van tijd tot tijd gecontroleerd?

Ja Door de getroffen maatregelen ook daadwerkelijk van tijd tot tijd te controleren of ze worden nageleefd, zorgt de organisatie voor een goede bescherming van de persoonsgegevens.

Nee De organisatie kan hele goede maatregelen hebben getroffen maar als deze door de medewerkers in de organisatie niet altijd worden uitgevoerd dan zijn de maatregelen niet zinvol. Het is verstandig om van tijd tot tijd de naleving intern te controleren.