

Checklist basisprincipes privacyregelgeving

1. Inleiding

Hieronder volgt een overzicht met de basisprincipes van de Wet bescherming persoonsgegevens (Wbp), de belangrijkste privacywet in Nederland. Dit is geen volledig overzicht van alle vereisten, maar een toelichting op de belangrijkste principes die voor iedere verwerking van persoonsgegevens gelden. Een belangrijk uitgangspunt is dat de gevraagde en verwerkte persoonsgegevens **noodzakelijk** moeten zijn om het doel van de verwerking te kunnen bereiken. Dat zal vóór de verwerking van de persoonsgegevens altijd moeten worden afgewogen. Vanaf 25 mei 2018 zal de Wet bescherming persoonsgegevens worden vervangen door de Algemene Verordening Gegevensbescherming (AVG), maar deze basisprincipes blijven gelden.

2. Begrippen

Een persoonsgegeven is ieder gegeven dat herleidbaar is tot een individu (de betrokkene). Daaronder vallen niet alleen adresgegevens, telefoonnummer en e-mailadres, maar ook inloggegevens, kenteken en IP-adres.

Verwerking van persoonsgegevens is iedere handeling die betrekking heeft op persoonsgegevens, zoals opslaan, raadplegen, opvragen en zelfs vernietigen.

Verantwoordelijke is degene die het doel en de middelen bepaalt voor de verwerking van persoonsgegevens. De Wbp gaat uit van het principe dat de daarin opgenomen vereisten gelden voor de verantwoordelijke, ook indien deze bepaalde verwerkingen door een derde (bewerker) laat verrichten.

De hierna opgenomen basisprincipes (wettelijke vereisten) rusten op de verantwoordelijke.

3. Basisprincipes Wbp:

1) Er dient een vooraf welbepaald en duidelijk omschreven **doel** te zijn

- Iedere verwerking dient een doel te hebben en dat doel moet zijn omschreven, bijvoorbeeld in een privacybeleid.
- Voorbeelden van verwerkingsdoelen: uitvoering van de overeenkomst met betrokkene, personeelsbeheer, betaling van salarissen.

2) De persoonsgegevens mogen **niet** worden verwerkt of gebruikt **in strijd met of buiten het bepaalde doel**

- Het doel bepaalt de ruimte van verwerking. Als een persoonsgegeven is verwerkt voor een bepaald doel mag dat persoonsgegeven naderhand niet worden verwerkt buiten dat doel. Het is daarom belangrijk de doelen ruim te omschrijven.
- Zo is Mediamarkt op de vingers getikt voor het gebruik van camerabeelden van beveiligingscamera's voor het aanspreken van haar personeel op hun

functioneren. Omdat de persoonsgegevens waren verzameld voor de beveiliging van de eigendommen van Mediamarkt, mochten deze gegevens niet voor de beoordeling van werknemers worden gebruikt.

3) Er is een **wettelijke grondslag** nodig om persoonsgegevens voor het bepaalde doel te mogen verwerken (art. 8 Wbp), zoals:

- de verwerking is **noodzakelijk** voor de **uitvoering van een overeenkomst**;
 - Bijvoorbeeld de verwerking van adres- en betaalgegevens voor de uitvoering van een huurovereenkomst.
- De verwerking is **noodzakelijk** voor de nakoming van een **wettelijke verplichting**.
 - Bijvoorbeeld het beschikbaar stellen van persoonsgegevens aan de fiscus.
- De verwerking is **noodzakelijk** voor de behartiging van het **gerechtvaardigd belang** van de verantwoordelijke.
 - Een gerechtvaardigd belang wordt aanwezig geacht in het geval dat de verwerking noodzakelijk is om de reguliere bedrijfsactiviteiten uit te voeren of te ondersteunen. Daarnaast dient het belang bij het bereiken van het doel van de gegevensverwerking te worden afgewogen tegen het privacybelang van de betrokkene.
- De betrokkene heeft zijn **ondubbelzinnige toestemming** gegeven voor de verwerking.
 - Dit lijkt vaak aan goede grondslag, maar is risicovol. Toestemming kan worden geweigerd of ten allen tijde worden ingetrokken en daar is verantwoordelijke aan gebonden. Bovendien is het voor arbeidsverhoudingen geen gewenste grondslag, omdat toestemming daar als ongeldig zou kunnen worden beschouwd vanwege op de ongelijke machtsverhouding tussen werkgever en werknemer.

4) De verwerking moet **proportioneel** zijn en voldoen aan de **subsidiariteits-eis**

- Er mogen niet meer persoonsgegevens worden verwerkt dan **noodzakelijk** is voor het bereiken van het doel van de verwerking. Als het doel ook kan worden bereikt door een geringere inbreuk op de privacy van de betrokkene dan zal de weg van de minste inbreuk moeten worden gekozen.

5) Verbod op verwerking van **bijzondere persoonsgegevens**

- Bijzondere persoonsgegevens zijn: gegevens inzake godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap vakbond en strafrechtelijke gegevens. Deze gegevens mogen niet worden verwerkt, tenzij dit in overeenstemming met artikelen 16-23 Wbp geschiedt.

- Voorbeeld: gegevens over iemands gezondheid mogen op grond van art. 21 Wbp alleen worden verwerkt door hulpverleners of instellingen of voorzieningen voor gezondheidszorg voor zover dat met het oog op een goede behandeling of verzorging noodzakelijk is.

6) Informatieplicht:

- Verantwoordelijke dient betrokkenen van wie zij persoonsgegevens verwerkt op een duidelijke en makkelijk raadpleegbare wijze te informeren over welke persoonsgegevens voor welk doel worden verwerkt, hoe de gegevens worden gebruikt en of deze gegevens worden verstrekt aan derden.
- Dit kan bijvoorbeeld via een privacyverklaring op de website of in een folder. Voor werknemers zou dit via een privacyprotocol op intranet kunnen.

7) De persoonsgegevens moeten **accuraat** worden gehouden en verantwoordelijke dient **passende organisatorische en technische veiligheidsmaatregelen** te nemen om de persoonsgegevens te beschermen tegen onrechtmatige verwerking, corruptie of verlies.

- Een adequate beveiliging van persoonsgegevens is een vereiste uit de wet dat een steeds grotere rol speelt bij de handhaving door de Autoriteit Persoonsgegevens (AP en tevens het College Bescherming Persoonsgegevens, CBP, genaamd). De AP (het CBP) heeft [richtsnoeren beveiliging persoonsgegevens](#) opgesteld waarin dit vereiste nader wordt uitgelegd. Verantwoordelijke zal moeten kunnen aantonen dat voldoende veiligheidsmaatregelen zijn getroffen en geborgd om de persoonsgegevens van de betrokkenen te beschermen. Per 1 januari 2016 is bovendien de Meldplicht datalekken in werking getreden waarbij in geval van een datalek de verplichting kan bestaan het lek aan de AP en eventueel aan de betrokkenen te melden. Daarnaast heeft de AP hoge boetemogelijkheden gekregen bij schending van de Wbp, waaronder de schending van de beveiligingsplicht, die kan oplopen tot € 820.000,- of zelfs 10% van de jaaromzet.

8) Inzagerecht:

- Indien een betrokkene daarom verzoekt dient deze binnen 4 weken van verantwoordelijke een overzicht te krijgen met zijn of haar gegevensverwerkingen. Iedere betrokkene heeft het recht op inzage en verbetering en eventueel verwijdering of afscherming van zijn/haar gegevens. Dat wil niet zeggen dat er kopieën van alle stukken moeten worden gegeven als daarom wordt gevraagd. Interne notities *mogen* bijvoorbeeld verwijderd worden en eventuele verwijzingen naar andere personen *moeten* in principe verwijderd worden.

9) Meldingsplicht:

- Er geldt momenteel nog een meldingsplicht van digitale gegevensverwerkingen bij de AP. Voor gangbare gegevensverwerkingen, zoals het voeren van administraties bestaan vrijstellingen.
- De meldingsplicht **vervalt** echter onder de komende Algemene Verordening Gegevensbescherming die per 25 mei 2018 van toepassing wordt. In de plaats daarvan zal iedere verantwoordelijke en bewerker een verwerkingsregister moeten bijhouden. Ook wel [documentatieplicht](#) genaamd.

10) **Bewerkersovereenkomst:**

- Bij het inschakelen van een derde (bewerker) voor de verwerking van persoonsgegevens, zoals een salarisadministrateur of een clouddienstverlener, blijft verantwoordelijke als verantwoordelijke van de persoonsgegevens verplicht de rechtmatige verwerking van deze persoonsgegevens te controleren en te waarborgen.
- Op verantwoordelijke rust daarbij de wettelijke plicht om een bewerkersovereenkomst te sluiten met haar bewerkers.
 - In de bewerkersovereenkomst moet in ieder geval zijn geregeld wat het doel is van de verwerking, welke gegevens worden verwerkt, de verplichting voor de bewerker om de gegevens niet voor eigen doeleinden of zonder opdracht van de verantwoordelijke te verwerken, de beveiligingsmaatregelen die de bewerker moet treffen en de wijze van uitvoeren van de meldplicht datalekken.

4. Tot slot

In de komende AVG wordt, veel meer dan in de Wbp, de wijze waarop voldaan moet worden aan de privacyregels opgelegd. Zoals de verplichting tot het bijhouden van een verwerkingsregister. Bovendien wordt de boete die de Autoriteit Persoonsgegevens kan opleggen verhoogd tot een maximum van 20 miljoen of 4 % van de wereldwijde jaaromzet.

Naast de vereisten uit de Wbp gelden andere wettelijke vereisten met betrekking tot specifieke verwerkingen van persoonsgegevens. Zo kent de Telecommunicatiewet verplichtingen met betrekking tot SPAM en cookies en bestaan er specifieke wetgeving, zoals de Kieswet en de Wet openbaarheid bestuur voor overheden en de Wet geneeskundige behandelingsovereenkomst met betrekking tot medische gegevens.

Heeft u vragen over de vereisten van de privacy regelgeving of over de specifieke wetgeving, dan adviseer ik u uiteraard graag nader.

Monique Hennekens
Najaar 2016

Hekkelman Advocaten N.V.
T 024 - 382 83 29
M 06 - 281 393 87
m.hennekens@hekkelman.nl