Het privacybeleid op papier

Een onderzoek naar de gewenste wijze van gegevensverwerking binnen Payper

Auteur: Simone Audiffred

Afstudeerorganisatie: Payper

Breda, mei 2016

Het privacybeleid op papier

Een onderzoek naar de gewenste wijze van gegevensverwerking binnen Payper

Classificatie:	Intern
Auteur:	Simone Audiffred
Studentnummer:	2040439
Afstudeerorganisatie:	Payper
Afstudeermentor:	Dhr. mr. R.P.A Michielsen
Onderwijsinstelling:	Juridische Hogeschool Avans-Fontys te Tilburg
Opleiding:	HBO-Rechten
Afstudeerperiode:	februari 2016 – mei 2016
Eerste afstudeerdocent:	Mevr. mr. S.C.J Gruyters-de Greef
Tweede afstudeerdocent:	Dhr. mr. M.G.J Kooij

Breda, mei 2016

Voorwoord

In het kader van het afstuderen van de opleiding HBO-Rechten aan de Juridische Hogeschool, heb ik een afstudeerstage gelopen op de afdeling Legal bij Payper. Payper is een payrollbedrijf gevestigd in Breda. Gedurende deze stageperiode heb ik in opdracht van Payper een onderzoek gedaan naar de privacywetgeving en in het bijzonder naar de gewenste wijze van het verwerken van persoonsgegevens conform de eisen van de Wet bescherming persoonsgegevens.

Mijn onderzoek is mede mogelijk gemaakt door Rens Michielsen, Legal Counsel bij Payper. Ik wil hem bedanken dat ik mijn afstudeerstage bij Payper mocht vervullen en voor de goede begeleiding. Het was een ontzettend leuke en leerzame stage. Het onderwerp van mijn onderzoek was erg interessant. Omdat er binnen Payper nog weinig is uitgezocht met betrekking tot de privacywetgeving, vond ik het vooral heel leuk om hen op weg te helpen naar een goed privacybeleid. Graag wil ik tevens de rest van de collega's bedanken voor de gezellige sfeer binnen het bedrijf.

Het maken van dit onderzoek is mede mogelijk gemaakt door mijn eerste afstudeerdocent, Susanne Gruyters-de Greef. Ik wil haar heel erg bedanken voor de tijd die zij in mijn onderzoek heeft gestoken, de feedback en de inzichten die ze mij heeft gegeven.

Tot slot wil ik mijn directe omgeving bedanken. Mama en Michelle, bedankt voor de steun die jullie mij altijd geven! Daarnaast wil ik mijn goede (school)vriendinnetje Anne de Kinderen bedanken voor de leuke jaren die we samen hebben meegemaakt aan de JHS en voor haar steun en toeverlaat.

Zonder jullie was het maken van dit onderzoek niet mogelijk geweest!

Simone Audiffred

Tilburg, mei 2016

Inhoudsopgave

Lijst van afkortingen

Art.	Artikel
Awb	Algemene wet bestuursrecht
BSN	Burgerservicenummer
EHRM	Europees Hof voor de Rechten van de Mens
EU	Europese Unie
EVRM	Europees Verdrag van de Rechten van de Mens en de Fundamentele Vrijheden
FG	Functionaris voor de gegevensbescherming
GW	Grondwet
IVBPR	Internationaal Verdrag inzake Burgerrechten en Politieke rechten
IVECS	Internationaal Verdrag inzake economische culturele en sociale rechten
Meldplicht datalekken	Meldplicht datalekken en uitbreiding bestuurlijke Boetebevoegdheden Autoriteit Persoonsgegevens (Richtlijn 95/46/EG)
NAW	Naam, adres, woonplaats
UVRM	Universele verklaring van de Rechten van de Mens
UWV	Uitvoeringsinstituut Werknemersverzekeringen
VN	Verenigde Naties
Wabb	Wet algemene bepalingen Burgerservicenummer
Wbp	Wet bescherming persoonsgegevens
WPR	Wet persoonsregistratie
WVP	Wet Verbetering Poortwachter

Lijst van begrippen

Bestand – Elk gestructureerd geheel van persoonsgegevens, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.

Betrokkene - De betrokkene is de persoon op wie de betreffende gegevens betrekking hebben.

Bewerker – Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Medewerker – Indien er in het rapport over een medewerker wordt gesproken, worden de medewerkers bedoeld die feitelijk bij Payper werken.

Persoonsgegevens – Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

Verwerken – Elke handeling met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Verantwoordelijke – De verantwoordelijke is een organisatie of een natuurlijk persoon die verantwoordelijk is voor de gegevensverwerking en het aansturen hiervan.

Werknemer – Met werknemer wordt bedoeld degene die bij Payper op basis van een payrollconstructie in dienst is. Deze werknemer is feitelijk niet bij Payper werkzaam. Payper is slechts de juridische werkgever.

Samenvatting

De vraag die in dit rapport centraal staat is: “Op welke manier dient Payper persoonsgegevens te verwerken, zodat zij voldoet aan de eisen die de Wet bescherming persoonsgegevens hieraan stelt, mede gelet op de meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheden Autoriteit Persoonsgegevens?”

Payper is een payrollbedrijf en heeft te maken met vele werknemers (dataobjecten). Van al deze werknemers worden persoonsgegevens verwerkt. Payper heeft echter nog weinig aandacht besteed aan de wettelijke regels die rondom de gegevensverwerking gelden. Er is onvoldoende duidelijkheid of de huidige wijze van verwerken binnen Payper voldoet aan de wet. Een goed privacybeleid ontbreekt dan ook binnen de organisatie. De Wet bescherming persoonsgegevens bevat regels inzake de wijze waarop gegevens mogen worden verwerkt en op welke manier deze moeten worden beschermd. De wet is op 1 september 2001 in werking getreden. Op 1 januari 2016 is de wet gewijzigd. De wetswijziging ‘meldplicht datalekken en uitbreiding boetebevoegdheden Cbp’ heeft ervoor gezorgd dat er een aantal artikelen zijn aangepast en zijn toegevoegd aan de wet. In dit rapport wordt ingegaan op de wettelijke verplichtingen die voortvloeien uit de Wet bescherming persoonsgegevens alsmede uit de wetswijziging. De verwerking moet ten eerste kunnen worden gebaseerd op een gerechtvaardigd doel en op een van de gerechtvaardigde grondslagen die de wet noemt. De wet maakt een onderscheid in algemene persoonsgegevens en bijzondere persoonsgegevens. Beide gegevens moeten aan bepaalde verplichtingen voldoen mogen zij door een organisatie worden verwerkt. Daarnaast moet er sprake zijn van goede beveiliging en een redelijke bewaartermijn. De organisatie heeft bepaalde verplichtingen zoals de geheimhoudingsplicht en de informatieplicht. Tot slot heeft de betrokkene een aantal rechten die zij kan uitoefenen omtrent de gegevensverwerking.
De rechtmatigheid van de gegevensverwerking wordt gecontroleerd door de Autoriteit Persoonsgegevens. Dit is het bestuursorgaan dat zich bezighoudt met het adviseren en controleren van gegevensverwerkingen. De verwerking moet door degene die gegevens verwerkt aan de Autoriteit Persoonsgegevens worden gemeld. De Autoriteit Persoonsgegevens kan tevens een voorafgaand onderzoek instellen indien er specifieke risico’s aan de verwerkingen vastzitten. Daarnaast moet er een melding worden gemaakt indien er sprake is van een datalek. Wanneer er niet aan de wettelijke verplichtingen van gegevensverwerking wordt voldaan, is de Autoriteit Persoonsgegevens bevoegd tot het opleggen van een boete.
Voor een groot deel van de medewerkers van Payper is het onduidelijk welke regels er gelden omtrent het privacyrecht met betrekking tot gegevensverwerking. Dit leeft samen met het feit dat er binnen Payper nog weinig aandacht is besteed aan de privacy. Naar aanleiding van vragenlijsten die door verschillende medewerkers zijn ingevuld, is duidelijk geworden op welke wijze gegevens binnen Payper worden verwerkt. De belangrijkste conclusie die naar voren is gekomen, is dat Payper in haar huidige vorm niet voldoet aan de eisen van de wet. De kennis binnen de onderneming dient vergroot te worden. Dit kan Payper verwezenlijken middels het houden van een voorlichting, presentatie of informatiebijeenkomst. Het is belangrijk om de medewerkers op de hoogte te stellen van alle huidige wet- en regelgeving rondom dit onderwerp zodat er daadwerkelijk conform de wet wordt gewerkt. Payper dient na te denken over een goed omschreven doel die als basis dient voor het verzamelen van gegevens. Daarnaast is het van belang om de juiste beveiliging en bewaartermijnen te hanteren mede om datalekken zo veel mogelijk te voorkomen. Iedere medewerker die toegang heeft tot persoonsgegevens zal een geheimhoudingsverklaring moeten ondertekenen. Tot slot dient de onderneming een privacyreglement te implementeren zodat iedere medewerker binnen Payper op de hoogte is van alle regels die rondom de verwerking van persoonsgegevens gelden. Op die manier kan iedere medewerker zijn of haar functie optimaal uitoefenen zonder dat de wettelijke regels worden overtreden.

Hoofdstuk 1 Inleiding

In het eerste hoofdstuk worden de aanleiding en het probleem beschreven. Aan de hand daarvan zijn de centrale vraag, de doelstelling en een aantal deelvragen opgesteld. Tevens bevat dit hoofdstuk een korte omschrijving van de organisatie, de gebruikte onderzoeksstrategieën en een opbouw van het rapport.

§ 1.1 Afstudeerorganisatie

Payper B.V. (hierna: Payper) is een payrollbedrijf, kantoorhoudende te Breda. Payper biedt payrolloplossingen, HR-ondersteuning, advies aan bedrijven in retail, logistiek, zorg, beveiliging, horeca en uitzendbureaus. Payper biedt specifieke payrolloplossingen en neemt daarmee zorgen voor ondernemers weg. Op deze manier hebben ondernemingen meer tijd voor andere zaken en hoeven zij zich niet bezig te houden met de juridische aspecten zoals werkgeverrisico's. Het bedrijf telt +/- 45 werknemers, waaronder één Legal Counsel. Binnen het bedrijf is tevens een advocaat twee ochtenden in de week werkzaam.

De payrollconstructie is niet wettelijk geregeld. Payrolling houdt in dat een werknemer in dienst treedt bij een payrollbedrijf op basis van een arbeidsovereenkomst. De inlener werft en selecteert de werknemers. De werknemer treedt vervolgens in dienst bij een payrollbedrijf op basis van een arbeidsovereenkomst. Het payrollbedrijf is de juridische werkgever. Dit wil zeggen dat het payrollbedrijf de werkgeverrisico's draagt en voor de administratieve handelingen zorgt zoals de loonbelasting en de ontslagprocedure. De inlener is feitelijk werkgever. De werknemer verricht exclusief werk bij de inlener. Het payrollbedrijf en de inlener sluiten een inleenovereenkomst.

§ 1.2 Probleembeschrijving

De Wet bescherming persoonsgegevens (hierna: Wbp) is op 1 september 2001 in werking getreden en bevat regels inzake de wijze waarop persoonsgegevens verwerkt mogen worden. De Wbp is op dit moment de belangrijkste wetgeving omtrent het privacyrecht in Nederland. Privacybescherming wordt steeds belangrijker, vooral in het bedrijfsleven, en de wetgeving beweegt daarin mee.[1] Op 1 januari 2016 is de wetswijziging 'meldplicht datalekken en uitbreiding boetebevoegdheden Cbp' (hierna: meldplicht datalekken) in werking getreden. Dit houdt in dat een aantal artikelen van de Wbp zijn gewijzigd. Sinds de wetswijziging heeft het College bescherming persoonsgegevens, die vanaf 1 januari 2016 de Autoriteit Persoonsgegevens wordt genoemd, boetebevoegdheden gekregen die zij kunnen opleggen indien een organisatie de Wbp overtreedt. Daarnaast moeten ernstige datalekken aan de Autoriteit Persoonsgegevens worden gemeld.

De Wbp bevat bepalingen die de gegevensverwerking reguleert en de persoonsgegevens beschermt. De wet is op sommige stukken niet altijd even begrijpelijk en bepalingen kunnen op verschillende manieren worden geïnterpreteerd. Bedrijven hebben dan ook niet altijd besef van de geldende wet- en regelgeving met betrekking tot de gegevensverwerking. Daarbij zijn de regels rondom het verwerken van persoonsgegevens met de komst van de wetswijziging aangepast en aangescherpt. Dit roept bij Payper vragen op. Payper is een payrollbedrijf en heeft te maken met vele werknemers (dataobjecten). Zo heeft zij 7.000 actieve werknemers onder zich, waarvan zij persoonsgegevens verwerkt. Tevens heeft Payper te maken met verschillende opdrachtgevers en intermediairs. Payper wordt door de betreffende opdrachtgevers gevraagd om een werknemer op haar payroll te zetten. Hierbij krijgt Payper bepaalde persoonsgegevens van de werknemer die zij nodig heeft voor onder andere de salarisverwerking. Binnen Payper ontbreekt er echter een goed privacybeleid inzake de verwerking van persoonsgegevens. Er is bij Payper onvoldoende duidelijkheid

[1] 'Beveiliging van persoonsgegevens', Autoriteit Persoonsgegevens, Autoriteitpersoonsgegevens.nl (zoek op *Wbp*).

welke regels voor het verwerken van persoonsgegevens van toepassing zijn op de organisatie met name nu er sinds januari jl. een wetswijziging in werking is getreden.
Als gevolg van deze wetswijziging heeft de Autoriteit Persoonsgegevens de bevoegdheid om boetes tot 820.000,- euro op te leggen aan bedrijven die de Wbp overtreden. Payper loopt hiermee mogelijk een groot risico. Er is dan ook behoefte aan informatie omtrent de regels van de Wbp. De opdracht luidt om te onderzoeken welke huidige wet- en regelgeving en eventuele jurisprudentie er geldt voor het verwerken van persoonsgegevens, en op welke manier Payper dus persoonsgegevens mag en kan verwerken zodat zij voldoen aan de vereisten die de Wbp hieraan stelt. Een degelijk privacyreglement is voor Payper noodzakelijk zodat de gehele organisatie op de hoogte is van de gewenste wijze voor de verwerking van persoonsgegevens. Naar aanleiding van het onderzoek zal dan ook een dergelijk reglement voor Payper worden opgesteld.

§ 1.3 Doelstelling
Op 30 mei 2016 wordt een er een onderzoeksrapport met een privacyreglement aan Payper overhandigd die de Wet bescherming persoonsgegevens en de meldlicht datalekken en uitbreiding boetebevoegdheden Autoriteit Persoonsgegevens in kaart brengt, zodat Payper duidelijkheid heeft over de gewenste manier waarop persoonsgegevens binnen de organisatie verwerkt moeten worden.

§ 1.4 Onderzoeksvraag
Op welke manier dient Payper persoonsgegevens te verwerken, zodat zij voldoet aan de eisen die de Wet bescherming persoonsgegevens hieraan stelt, mede gelet op de meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheden Autoriteit Persoonsgegevens?

§ 1.5 Deelvragen
Om de centrale vraag te kunnen beantwoorden, is deze opgedeeld in de volgende deelvragen:

1. Welke eisen stelt de Wet bescherming persoonsgegevens aan het verwerken van persoonsgegevens?
2. Wat is de Autoriteit Persoonsgegevens?
3. Wat is de huidige wijze waarop persoonsgegevens binnen Payper worden verwerkt?

§ 1.6 Onderzoeksstrategieën
Om een antwoord te kunnen geven op de centrale vraag en de bijbehorende deelvragen dienen de juiste onderzoeksstrategieën te worden toegepast. De onderzoeksstrategie geeft aan welke middelen worden ingezet om het doel te bereiken. Bij iedere deelvraag is er een keuze gemaakt tussen een onderzoek naar het recht of een onderzoek naar de praktijk. Bij een onderzoek naar het recht kan er gebruik worden gemaakt van een literatuur- en rechtsbronnenonderzoek. De praktijk kan worden onderzocht door middel van een casestudy, een survey of een veldonderzoek.[2]

§ 1.7 Bronnen en methoden
Wanneer de onderzoeksstrategieën zijn bepaald, komen de betreffende bronnen en methoden aan de orde. De bronnen geven aan op welke manier informatie wordt verzameld en kennis wordt verworven. Veel geraadpleegde bronnen zijn voornamelijk rechtsbronnen, literatuur, documenten, personen en fysieke objecten. Voor het onderzoek naar het recht zal er voornamelijk gebruik worden gemaakt van wet- en regelgeving, jurisprudentie en literatuur. De bronnen bij het onderzoek naar de praktijk bestaan voornamelijk uit personen, documenten en fysieke objecten. Hierbij kan worden gedacht aan interviews met medewerkers die in dienst zijn van de organisatie.[3]

[2] Van Schaaijk 2011, p. 79.

[3] Van Schaaijk 2011, p. 83.

De methoden geven aan op welke wijze de relevante informatie in kaart kan worden gebracht. Bij het onderzoek naar het recht wordt er gebruik gemaakt van een inhoudsanalyse om de benodigde informatie te verzamelen. Het onderzoek naar de praktijk zal voornamelijk in kaart worden gebracht door middel van interviews en vragenlijsten.

De eerste deelvraag wordt beantwoord aan de hand van een onderzoek naar het recht. Relevante wet- en regelgeving, jurisprudentie en literatuur wordt geraadpleegd. De eerste deelvraag zal dan ook een beeld schetsen van de verplichtingen die voortvloeien uit de Wbp en de wijzigingen die sinds 1 januari 2016 van toepassing zijn. De tweede deelvraag is een combinatie van een onderzoek naar het recht en een onderzoek naar de praktijk. Voornamelijk wordt in kaart gebracht wat de Autoriteit Persoonsgegevens inhoudt, welke taken en bevoegdheden zij hebben en op welke manier zij te werk gaan. Tevens worden de richtlijnen die de Autoriteit Persoonsgegevens hanteert in kaart gebracht. De derde deelvraag is een onderzoek naar de praktijk waarbij de wijze van het verwerken van persoonsgegevens door Payper in kaart wordt gebracht. Tevens geeft deze deelvraag aan of Payper in haar huidige vorm voldoet aan alle relevante wet- en regelgeving omtrent het verwerken van persoonsgegevens.

Welke eisen stelt de Wet bescherming persoonsgegevens aan het verwerken van persoonsgegevens?
De eerste deelvraag wordt onderzocht aan de hand van een onderzoek naar het recht. Het in kaart brengen van de Wbp gebeurt aan de hand van een rechtsbronnen- en literatuuronderzoek. De belangrijkste rechtsbron is de Wbp en de wetswijziging Meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Autoriteit Persoonsgegevens. Daarnaast wordt relevante literatuur en jurisprudentie geraadpleegd. Hierbij zullen alle relevante regels omtrent de verwerking van persoonsgegevens naar voren komen. Op deze manier komt er duidelijkheid wat onder persoonsgegevens wordt verstaan, hoe de wet in elkaar steekt en wat de vereisten van de Wbp zijn. Tevens geeft deze deelvraag aan op welke wijze persoonsgegevens verwerkt mogen worden en waar een bedrijf aan moet voldoen wanneer zij conform de wet willen werken. Hierdoor is het voor Payper in een oogopslag duidelijk welke eisen de Wbp stelt omtrent het verwerken van persoonsgegevens.

Wat is de Autoriteit Persoonsgegevens?
De tweede deelvraag brengt de Autoriteit Persoonsgegevens in kaart. Hierbij wordt naast een onderzoek naar het recht tevens gebruik gemaakt van een onderzoek naar de praktijk. Vooral het onderzoek naar het recht zal voor veel relevante informatie zorgen. Dit gebeurt aan de hand van een rechtsbronnen- en literatuuronderzoek. Door middel van dit onderzoek zal duidelijk worden wat de Autoriteit Persoonsgegevens inhoudt, welke richtlijnen zij hanteren en wat de verschillende sancties zijn wanneer een organisatie de Wbp overtreedt. Net zoals bij de vorige deelvraag zal ook hier gebruik worden gemaakt van een inhoudsanalyse om de relevante informatie te kunnen verzamelen. Bij het onderzoek naar de praktijk wordt gebruik gemaakt van interviews. Verschillende personen die werkzaam zijn bij de Autoriteit Persoonsgegevens worden geïnterviewd om in kaart te brengen op welke manier de Autoriteit Persoonsgegevens te werk gaat.

Wat is de huidige wijze van verwerken van persoonsgegevens binnen Payper?
De derde deelvraag wordt beantwoord aan de hand van een onderzoek naar de praktijk. Payper heeft op dit moment geen privacyreglement of een duidelijke werkwijze omtrent de verwerking van persoonsgegevens. Er wordt onderzocht op welke manier de medewerkers van de organisatie omgaan met de persoonsgegevens, wat voor informatie zij hebben met betrekking tot dit onderwerp en op welke wijze de privacy binnen de organisatie is geregeld. Hierbij wordt gelet op de eisen van de Wbp en er zal in kaart worden gebracht of Payper aan deze eisen voldoet. Dit zal worden onderzocht aan de hand van een casestudy. Er wordt gebruik gemaakt van een interview met de Legal Counsel van Payper en een vragenlijst voor de medewerkers.

§ 1.8 Voorlopige hoofdstukindeling

Om een goed onderzoek te kunnen opleveren, en correct antwoord te kunnen geven op de centrale vraag zijn er deelvragen opgesteld die in de volgende hoofdstukken worden uitgewerkt.

Het eerste hoofdstuk beschrijft het juridische kader. Dit hoofdstuk is van belang om een juiste analyse van de geldende wet- en regelgeving in beeld te brengen. Aan de hand hiervan wordt duidelijk aan welke verplichtingen de gegevensverwerking dient te voldoen. Er wordt in kaart gebracht hoe het privacyrecht is geregeld op internationaal en op nationaal niveau. De wijzigingen die uit de meldplicht datalekken voortvloeien worden kort in kaart gebracht. Vervolgens wordt er op de Wbp ingegaan. De belangrijkste wettelijke bepalingen van de Wbp worden beschreven en uitgelegd. Enkele bepalingen bevatten relevante jurisprudentie. Tot slot wordt er een kleine conclusie van het hoofdstuk gegeven.
De tweede deelvraag is in hoofdstuk drie uitgewerkt. Dit hoofdstuk schetst een beeld van de Autoriteit Persoonsgegevens waarbij er wordt ingegaan op de verschillende taken en bevoegdheden van het bestuursorgaan. Vervolgens komen de verplichtingen die de verantwoordelijke ten aanzien van de Autoriteit Persoonsgegevens heeft aan bod. Dit is de melding, het voorafgaand onderzoek en de meldplicht datalekken. Hierbij worden verschillende beleidsregels die het bestuursorgaan hanteert besproken. Verder worden de sancties die de Autoriteit Persoonsgegevens aan een organisatie op kan leggen in beeld gebracht. Tot slot wordt er wederom een kleine conclusie van het betreffende hoofdstuk gegeven. Hoofdstuk 4 beschrijft de huidige manier van het verwerken van de persoonsgegevens. Door middel van vragenlijsten die aan de medewerkers zijn toegestuurd is in kaart gebracht op welke manier persoonsgegevens binnen Payper worden verwerkt en hoe met privacy wordt omgegaan binnen de organisatie. Op basis van de resultaten is beoordeeld in hoeverre de huidige verwerking voldoet aan de wettelijke verplichtingen die uit de Wbp voortvloeien. Om herhaling te voorkomen bevat het laatste hoofdstuk geen tussenconclusie zoals de andere hoofdstukken. De eindconclusie beantwoord de centrale vraag. Naar aanleiding van de conclusie worden er aanbevelingen aan Payper gedaan. De aanbevelingen bevatten aanpassingen van de wijze van verwerking om in de toekomst aan de Wbp te kunnen voldoen.

Op basis van het onderzoek is er een privacyreglement toegevoegd. Dit reglement zal Payper helpen om het privacyrecht binnen de organisatie op orde te krijgen en om werknemers op de hoogte te stellen van de eisen die de Wbp stelt omtrent gegevensverwerking.

1.9 Belangrijke begrippen

In het gehele rapport worden voornamelijk vier belangrijke begrippen veelvuldig gebruikt. Om extra duidelijkheid te creëren worden deze begrippen hieronder nogmaals benoemd. De begrippen worden zijn tevens opgenomen in de begrippenlijst.

Verantwoordelijke
De verantwoordelijke is een organisatie of een natuurlijk persoon die verantwoordelijk is voor de gegevensverwerking en het aansturen hiervan.

Betrokkene
De betrokkene is de persoon op wie de betreffende gegevens betrekking hebben.

Bovenstaande begrippen zijn tevens terug te vinden bij de definities in artikel 1 Wbp.

Om verwarring te voorkomen wordt er in dit rapport een onderscheid gemaakt tussen de begrippen ‘medewerker’ en ‘werkgever’.

Medewerker
Indien er in het rapport over een medewerker wordt gesproken, worden de medewerkers bedoeld die feitelijk bij Payper werken.

Werknemer
Met werknemer wordt bedoeld degene die bij Payper op basis van een payrollconstructie in dienst is. Deze werknemer is feitelijk niet bij Payper werkzaam. Payper is slechts de juridische werkgever.

Hoofdstuk 2 Wet bescherming persoonsgegevens

In dit hoofdstuk staat de Wet bescherming persoonsgegevens (Wbp) centraal. Allereerst wordt het privacyrecht op internationaal niveau in kaart gebracht. Verschillende internationale verklaringen en verdragen worden besproken. Daarna komt het juridisch kader op nationaal niveau aan bod. De Wbp wordt besproken en voornamelijk wordt er dieper ingegaan op verschillende artikelen uit de Wbp. De verplichtingen van degene die verantwoordelijk is voor de verwerkte persoonsgegevens, de rechten van de betrokkene en de rechtsbescherming worden besproken en tot slot wordt er een conclusie van het betreffende hoofdstuk gegeven.

§ 2.1 Juridisch kader op internationaal niveau

Op internationaal niveau bestaan er een aantal belangrijke verklaringen en verdragen die bepalingen bevatten over mensenrechten, waaronder het recht op bescherming van de privacy.

Op 10 december 1948 is de Universele Verklaring van de Rechten van de Mens (hierna: UVRM) aangenomen door de Verenigde Naties (hierna: VN). De verklaring diende om de basisrechten van de mensen hierin op te nemen. De UVRM is de eerste verklaring waarin fundamentele rechten en vrijheden zijn beschreven.[4] Het recht op privacy komt voort uit artikel 12 van de verklaring. Het artikel luidt: *"Niemand zal onderworpen worden aan willekeurige inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of goede naam. Tegen een dergelijke inmenging of aantasting heeft een ieder recht op bescherming door de wet."*[5]
De universele verklaring is niet bindend maar is zeker een inspiratiebron en uitgangspunt van vele wetten en verdragen omtrent mensenrechten. De UVRM is dan ook de basis voor twee bindende VN-verdragen voor de rechten van de mens. Dit zijn het Internationaal Verdrag inzake burgerrechten en politieke rechten (hierna: IVBPR) en het Internationaal Verdrag inzake economische culturele en sociale rechten (hierna: IVECS).[6] Artikel 17 IVBPR is nagenoeg hetzelfde artikel als artikel 12 uit de URVM. Het verschil tussen beide artikelen is dat artikel 17 IVBPR wél bindend is.[7]

In 1950 is het Europees verdrag voor de Rechten van de Mens en de Fundamentele Vrijheden (hierna: EVRM) tot stand gekomen, wat tevens op de UVRM is gebaseerd.[8] Het toezicht op dit verdrag ligt bij de Raad van Europa. In Nederland heeft het verdrag directe werking.[9] Dit wil zeggen dat de rechterlijke macht alle wetgeving aan het verdrag moet toetsen. Daarbij mogen Nederlandse burgers de rechten van het EVRM inroepen. In het EVRM is een belangrijk artikel opgenomen inzake de privacy. Dit artikel luidt:[10]
1. Een ieder heeft het recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.

[4] Art. 93 GW jo 2 IVBPR
[5] Art. 12 UVRM
[6] Amnesty.nl (zoek op *UVRM*).
[7] Art. 17 IVBPR
[8] Amnesty.nl (zoek op *UVRM*).
[9] Art. 93 GW
[10] Art. 8 lid 1 en 2 EVRM

§ 2.2 Juridisch kader op nationaal niveau

Binnen de nationale wetgeving wordt er in artikel 10 Grondwet (hierna: GW) ingegaan op het recht op bescherming van de privacy. Dit artikel geeft iedereen het recht op eerbiediging van zijn persoonlijke levenssfeer. Artikel 10 lid 1 GW werd bij herziening van de Grondwet in 1983 uitdrukkelijk als klassiek grondrecht geformuleerd.[11] Dit houdt in dat het recht is af te dwingen bij de rechter.[12] Het artikel sloot zich aan bij de gelijktijdig ontwikkelende jurisprudentie van het Europese Hof voor de Rechten van de Mens (hierna: EHRM) over de bescherming van de privacy zoals neergelegd in artikel 8 EVRM.[13] De Wet persoonsregistratie (hierna: WPR) die op 1 juli 1989 tot stand kwam, gaf uitvoering aan artikel 10 GW.

Op 23 november 1995 is door het Europees Parlement en de Raad van de Europese Unie een privacyrichtlijn opgesteld.[14] De Wbp is voor een groot deel een implementatie van deze richtlijn.[15] De Wbp is op 1 september 2001 in werking getreden. Informatie over personen wordt in het dagelijks leven steeds meer verzameld en gebruikt. Mede door nieuwe telecommunicatienetwerken kunnen persoonsgegevens gemakkelijker worden verspreid en verzameld. Hierdoor bestond er behoefte aan betere regels in Europa en in Nederland.[16] De Wbp bevat regels inzake het rechtmatig verwerken van persoonsgegevens. De wet is voor een groot deel gebaseerd op de Europese Richtlijn 95/46/EG.[17] Hierbij is mede gelet op artikel 10 van de grondwet. De Wbp vervangt de WPR.[18]

§ 2.3 Wetswijziging

Op 1 januari 2016 is de Wbp gewijzigd. Een aantal artikelen is aangepast en er zijn artikelen toegevoegd. Uit de wetswijziging meldplicht datalekken vloeien twee belangrijke wijzigingen voort. De eerste wijziging is de toevoeging van artikel 34a in de Wbp. Dit artikel bevat regels over de meldplicht van de verantwoordelijke in het geval van een datalek. In paragraaf 3.5 wordt hier dieper op ingegaan. De tweede wijziging gaat over de sanctieversterking van de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens is nu bevoegd tot het opleggen van bestuurlijke boeten aan verantwoordelijken.[19] Paragraaf 3.4.1 gaat hier dieper op in.

§ 2.4 De reikwijdte van de Wbp

Artikel 2 lid 1 Wbp geeft aan dat de wet van toepassing is op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Een onderscheid in het handmatig verwerken en het geautomatiseerd verwerken van gegevens is niet altijd in alle scherpte te maken. In de praktijk komt het regelmatig voor dat een gegeven deels handmatig en deels geautomatiseerd wordt verwerkt. Indien gegevens handmatig worden verwerkt moeten de gegevens in een bestand worden opgenomen zoals een dossiermap.

---

[11] Hooghiemstra & Nouwt 2007, p. 16.
[12] Overheid.nl (zoek op *Wbp*).
[13] Hooghiemstra & Nouwt 2007, p. 16.
[14] Richtlijn 95/46/EG.
[15] Kamerstukken II, 1997/98, 25892, 3 (MvT) p. 5.
[16] Hooghiemstra & Nouwt 2007, p. 9.
[17] Loonstra & Zondag 2015.
[18] Hooghiemstra & Nouwt 2007, p. 15.
[19] Kamerstukken I, 2014/15, 33662, A.

De reikwijdte van de Wbp wordt bepaald door het begrip ‘verwerken van persoonsgegevens’. Een omschrijving van de begrippen ‘verwerken’ en ‘persoonsgegevens’ is opgenomen in de begrippenlijst van de wet. Onder verwerken wordt verstaan: “elke handeling met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.”[20] Onder het begrip ‘persoonsgegevens’ wordt verstaan: “elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.”[21] Een naam, adres en woonplaats zijn veel voorkomende persoonsgegevens. Maar bijvoorbeeld ook telefoonnummers, faxnummers en gegevens van een partner zijn persoonsgegevens. Het verwerken van een persoonsgegevens is bijvoorbeeld het verzamelen van een naam, adres en BSN van een werknemer en deze vervolgens in het systeem zetten. Kort gezegd is gegevensverwerking elke handeling omtrent gegevens vanaf de verzameling tot aan de vernietiging.

Een aantal verwerkingen is uitgezonderd van de Wbp.[22] Zo is de Wbp niet van toepassing op het verwerken van persoonsgegevens:

- indien dit uitsluitend voor persoonlijke of huiselijk gebruik is;
- door of ten behoeve van de inlichtingen- en veiligheidsdiensten;
- ten behoeve van de uitvoering van de politietaak;
- door gemeenten in de gemeentelijke basisadministratie;
- ten behoeve van de uitvoering van de Wet justitiële en strafvorderlijke gegevens;
- ten behoeve van de uitvoering van de Kieswet;
- persoonsgegevens voor uitsluitend journalistieke, artistieke of literaire doeleinden.[23]

Deze uitzonderingen zijn niet van toepassing op Payper.

§ 2.5 De verwerking van persoonsgegevens

De Wbp bevat een aantal regels voor het verwerken van persoonsgegevens. De Wbp heeft in beginsel geen verbiedend karakter. Het verwerken van persoonsgegevens is toegestaan mits er wordt voldaan aan een aantal voorwaarden. De wet reguleert de wijze van gegevensverwerking. Als eerst stelt zij regels die betrekking hebben op de toelaatbaarheid en de kwaliteit van de gegevens die worden verwerkt.[24] Dit zijn de zogenaamde algemene beginselen van gegevensverwerking.[25] De beginselen vloeien voort uit de richtlijn. Daarnaast bevat de Wbp een aantal voorwaarden op grond waarvan de gegevensverwerking rechtmatig wordt geacht. Tot slot moet er worden gelet op de bewaartermijn en de wijze van beveiliging van de verwerkte persoonsgegevens.

§ 2.5.1 Algemene beginselen van gegevensverwerking

De gegevensverwerking moet aan alle algemene beginselen voldoen om rechtmatig te zijn. Tevens waarborgen de algemene beginselen de kwaliteit van de gegevens.

Het rechtmatigheidsbeginsel

Persoonsgegevens moeten in overeenstemming met de wet, behoorlijk en zorgvuldig worden verwerkt.[26] Het rechtmatigheidsbeginsel is het basisprincipe voor een rechtmatige

[20] Art. 1 sub b Wbp

[21] Art. 1 sub a Wbp

[22] Sauerwein & Linnemann 2001, p. 16.

[23] Art. 2 lid 2 jo 3 Wbp

[24] Kamerstukken II, 1997/98, 25892, 3 (MvT) p. 20.

[25] Hooghiemstra & Nouwt 2007, p. 20.

[26] Art. 6 Wbp

verwerking volgens de vereisten van de wet. Dit artikel is gebaseerd op artikel 6 van de richtlijn die voorschrijft dat gegevens op een eerlijke en rechtmatige manier moeten worden verwerkt.[27] De Nederlandse vertaling 'eerlijk en rechtmatig' is in de Wbp niet overgenomen. Dit komt doordat de begrippen 'eerlijk en rechtmatig' dubbelop zijn.[28] Indien gegevens op een oneerlijke manier worden verwerkt is er direct sprake van een onrechtmatige daad. Het begrip 'rechtmatig' heeft dan geen toegevoegde waarde meer. Daarnaast sluiten de begrippen 'behoorlijk' en 'zorgvuldig' beter aan bij de juridische begrippen van de Nederlandse wetgeving. Het begrip zorgvuldigheid sluit enerzijds aan bij de zorgvuldigheidsnorm van de onrechtmatige daad en anderzijds bij het zorgvuldigheidsbeginsel als algemeen beginsel van behoorlijk bestuur.[29] Uit jurisprudentie blijkt dat er wordt voldaan aan het rechtmatigheidsbeginsel indien alle vereisten van de wet worden nageleefd en de verantwoordelijke op een juiste manier met de gegevens omgaat.[30]

Het beginsel van doelbinding
De verantwoordelijke moet voorafgaand aan het verzamelen van persoonsgegevens een doel vaststellen. Dit doel moet welbepaald, uitdrukkelijk omschreven en gerechtvaardigd zijn.[31] Welbepalend wil zeggen dat het doel waarvoor de gegevens worden verzameld duidelijk van tevoren is bepaald. Het doel moet op een duidelijke manier worden omschreven zodat er geen twijfel mogelijk is over de reden waarom bepaalde gegevens worden verzameld. Tijdens het verwerkingsproces kan deze omschrijving niet meer worden aangepast. Er zal dus van tevoren goed over de omschrijving van het doel moeten worden nagedacht.[32] Uitdrukkelijk omschreven houdt in dat het doel moet worden vastgelegd. De verantwoordelijke kan het doel bijvoorbeeld omschrijven bij de melding aan de Autoriteit Persoonsgegevens.[33] Tot slot moet het doel gerechtvaardigd zijn. Op het moment dat er een doel is vastgesteld kunnen gegevens worden verzameld. Vervolgens worden deze gegevens verder verwerkt. In artikel 8 Wbp is een limitatieve opsomming gemaakt van gerechtvaardigde gronden voor die verwerking. De verwerking moet op tenminste een van die gronden kunnen steunen wil het doel gerechtvaardigd zijn. Artikel 8 wordt in paragraaf 2.5.2 verder uitgewerkt. Bij het inrichten van gegevensverwerking moet steeds worden nagegaan of de verwerking noodzakelijk is om het doel te bereiken.[34]

Iedere gegevensverwerking begint met het vaststellen van een specifiek doel. Dit is een van de belangrijkste aspecten omdat iedere verzameling van gegevens gebaseerd moet kunnen worden op dit doel. Aan de hand van dit doel kan worden bepaald welke gegevens vervolgens verzameld mogen worden om dit doel te bereiken. Op grond hiervan kan tevens worden bepaald:
- welke gegevens verwerkt mogen worden;
- wat er met die gegevens mag gebeuren;
- of de gegevens aan derden mogen worden verstrekt en zo ja, aan welke derden.

Het proportionaliteit- en subsidiariteitsbeginsel
Het proportionaliteit- en subsidiariteitsbeginsel speelt een belangrijke rol. Het proportionaliteitsbeginsel geldt rechtstreeks op grond van art. 8 EVRM. De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot het te dienen doel

[27] Art. 6 lid 1 sub a Richtlijn 95/46/EG.
[28] Kamerstukken II, 1997/98, 25892, 3 (MvT) p. 77-78.
[29] Hooghiemstra & Nouwt 2007, P.62.
[30] Rb 05 december 2003, *LJN* AO0044.
[31] Art. 7 Wbp
[32] Sauerwein & Linnemann 2001, p. 20.
[33] Hooghiemstra & Nouwt 2007, p.65.
[34] Sauerwein & Linnemann 2001, p. 20.

van de verwerking.[35] Dit wil zeggen dat de verantwoordelijke steeds een belangenafweging dient te maken tussen het eigen belang en het belang van de betrokkene, zo blijkt uit jurisprudentie. Zelfs wanneer een betrokkene toestemming geeft voor de verwerking dient de verantwoordelijke zelf te beoordelen of de verwerking noodzakelijk is.[36]
Het subsidiariteitsbeginsel houdt in dat het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid wordt bereikt en er geen andere, minder nadelige wijze voor de betrokkene bestaat om het doel te bereiken. Op de verantwoordelijke rust de plicht om binnen redelijke grenzen een inbreuk op de persoonlijke levenssfeer van anderen te vermijden dan wel zo beperkt mogelijk te houden.[37]
Een organisatie dient er dus voor te zorgen dat er alleen gegevens worden verwerkt indien dit noodzakelijk is om het doel te bereiken. Dit wordt op zodanige wijze volbracht dat de privacy van de betrokkene zo min mogelijk wordt geschonden.

Het beginsel van niet-onverenigbaarheid
Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.[38] In beginsel mogen gegevens worden verwerkt voor het doel waarvoor zij zijn verkregen. De gegevens mogen ook voor andere doeleinden dan waarvoor zij zijn verkregen worden verwerkt, mits deze doeleinden niet tegenstrijdig zijn met het oorspronkelijke doel.[39] Voor de beoordeling of het doel onverenigbaar is heeft de Wbp handvaten gegeven en een opsomming gemaakt waar de verantwoordelijke in zijn afweging in ieder geval rekening mee dient te houden.[40]

Het kwaliteitsbeginsel
De Wbp geeft aanvullende voorwaarden die vooral betrekking hebben op de inhoudelijke kwaliteit van de gegevens.[41] Persoonsgegevens worden slechts verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn.[42] Dit wil zeggen dat alleen relevante informatie, die nodig is om het doel te verwezenlijken, verwerkt mag worden. Onnodige gegevensverwerking is onrechtmatig.[43]

§ 2.5.2 Grondslagen rechtmatige verwerking
De voorwaarden voor rechtmatige verwerking zijn limitatief opgesomd in artikel 8 sub a t/m f Wbp. De gegevensverwerking moet gebaseerd kunnen worden op een van de grondslagen. Is dit niet het geval, dan is de verwerking niet gerechtvaardigd en dus niet toegestaan.[44]

Ondubbelzinnige toestemming
De eerste grondslag is de ondubbelzinnige toestemming van de betrokkene.[45] De Wbp omschrijft toestemming als elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat persoonsgegevens die hem betreffen worden verwerkt.[46] De toestemming moet aan een aantal criteria voldoen. Als eerst moet de toestemming in vrije wil zijn geuit. De betrokkene mag dus niet onder druk staan van de

[35] Kamerstukken II, 1997/98, 25892,3 (MvT) p. 12.
[36] HR 09 september 2011, *LJN* BQ8097.
[37] Hooghiemstra & Nouwt 2007, p. 17.
[38] Art. 9 Wbp
[39] Kamerstukken II, 1997/98, 25892, 3 (MvT) p. 20.
[40] Art. 9 lid 2 Wbp
[41] Kamerstukken II, 1997/98, 25892, 3 (MvT) p. 21.
[42] Art. 11 Wbp
[43] Art. 6:162 BW
[44] Sauerwein & Linnemann 2001, p.20.
[45] Art. 8 sub a Wbp
[46] Art. 1 sub i Wbp

verantwoordelijke. Daarnaast moet de toestemming zijn gericht op bepaalde gegevensverwerking. De betrokkene moet goed worden geïnformeerd en moet begrijpen waarvoor hij toestemming geeft. Tot slot moet de toestemming ondubbelzinnig zijn. Dit wil zeggen dat er geen twijfel kan ontstaan over de toestemming van de betrokkene. De toestemming moet uitgesproken en duidelijk zijn.[47] Zo zou een organisatie de betrokkene bij het tekenen van een overeenkomst bijvoorbeeld ook een verklaring kunnen laten tekenen waarin de betrokkene toestemming geeft voor de gegevensverwerking. Op die manier wordt de betrokkene enerzijds geïnformeerd over de gegevensverwerking en anderzijds wordt er direct toestemming verleend.

De verwerking is noodzakelijk voor de uitvoering van een overeenkomst
De tweede grondslag is de gegevensverwerking die noodzakelijk is voor de uitvoering van een overeenkomst 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.[48] De betrokkene moet hierbij een partij zijn. Dit wil zeggen dat op het moment dat er een overeenkomst is gesloten met de betrokkene, de gegevens van de betrokkene vervolgens verwerkt mogen worden indien zij noodzakelijk zijn voor de uitvoering van die overeenkomst. Daarbij mogen slechts de relevante gegevens worden verwerkt. Op basis van deze grondslag mogen er tevens gegevens worden verwerkt die nodig zijn in de fase voorafgaand aan het sluiten van een overeenkomst. Een voorwaarde hiervan is dat de betrokkene de handeling, die het verwerken van persoonsgegevens vereist, zelf verzoekt. De totstandkoming van de overeenkomst moet dus op initiatief zijn van de betrokkene, niet van de organisatie.

De verwerking is noodzakelijk om wettelijke verplichting na te komen
De derde grondslag waar het verwerken van gegevens op kan worden gebaseerd is de noodzakelijkheid van het verwerken van persoonsgegevens voor de uitvoering van een wettelijke plicht. Het moet niet (goed) mogelijk zijn om de wettelijke plicht te kunnen uitvoeren zonder het verwerken van persoonsgegevens. De plicht hoeft niet per se uit de wet te komen maar mag ook gelden op grond van bijvoorbeeld een gemeentelijke verordening.[49] Hierbij kan gedacht worden aan gemeentelijke basisregistratie voor persoonsgegevens of gegevens verstrekking aan de belastingdienst.

De verwerking is noodzakelijk ter vrijwaring van vitaal belang van de betrokkene
Persoonsgegevens mogen worden verwerkt op basis van de vierde grondslag, indien de gezondheid van de betrokkene in gevaar is en de persoonsgegevens nodig zijn om de betrokkene uit het gevaar te halen. Bijvoorbeeld wanneer de betrokkene bewusteloos in het ziekenhuis belandt en zijn medische gegevens nodig zijn.[50]

De verwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak
Dit wil zeggen dat een bestuursorgaan alleen gegevens mag verwerken indien dit noodzakelijk is voor zijn werk.[51] Deze grondslag geldt alleen voor overheidsorganen.

De verwerking is noodzakelijk voor behartiging van gerechtvaardigd belang
Indien activiteiten niet goed uitgevoerd kunnen worden zonder het verwerken van persoonsgegevens, kan er een beroep worden gedaan op de laatste grondslag. Deze grondslag is een zogenaamde restbepaling. De bepaling is algemener dan bovenstaande grondslagen. Hierbij wordt vereist dat er sprake is van een gerechtvaardigd belang van de

[47] Sauerwein & Linnemann 2001, p. 22.
[48] Art. 8 sub b Wbp
[49] Art. 8 sub c Wbp
[50] Art. 8 sub d Wbp
[51] Art. 8 sub e Wbp

verantwoordelijke of van een derde aan wie de gegevens worden verstrekt. Een gerechtvaardigd belang is aanwezig indien de verwerking voor de verantwoordelijke of de derde noodzakelijk is om diens normale bedrijfsactiviteiten uit te kunnen voeren. Er is geen sprake van een gerechtvaardigd belang indien er wordt geanticipeerd op bedrijfsactiviteiten waarvan de verantwoordelijke denkt persoonsgegevens nodig te hebben. Het verwerken moet gerechtvaardigd zijn ten aanzien van een individueel persoon. Daarnaast moet rekening worden gehouden met de hoeveelheid van de gegevens die worden verwerkt. Misschien kan hetzelfde resultaat worden behaald via een minder ingrijpende weg. De belangen of fundamentele rechten van de betrokkene mogen er in elk geval niet onder lijden en hebben voorrang.[52]

Voorbeeld van de algemene beginselen in de praktijk
Een organisatie stelt eerst een specifiek doel vast. Bijvoorbeeld het doel om werknemers te werven en in dienst te nemen. Op grond van dit doel mogen bepaalde gegevens worden verzameld. Er wordt vervolgens een arbeidsovereenkomst met de werknemer gesloten. De gegevens die voor deze handeling nodig zijn, zoals onder andere naam en geboortedatum, mogen dus door de werkgever worden verkregen. Dit sluit aan bij het doel en is dus gerechtvaardigd.

Wil de werkgever de gegevens vervolgens verwerken, zoals het verstrekken aan derden, het vastleggen of het gebruiken van de gegevens, dan moet deze verwerking kunnen worden gebaseerd op een van de gerechtvaardigde grondslagen die in artikel 8 Wbp zijn neergelegd. Iedere verwerking dient apart te worden beoordeeld aan een grondslag in de wet. Stel dat een werkgever het salaris van de werknemer wil uitkeren dan heeft de werkgever hier bepaalde gegevens voor nodig zoals een bankrekeningnummer. Het vastleggen van deze gegevens in het systeem sluit aan bij het doel van de organisatie en kan tevens worden gebaseerd op de grondslag uit artikel 8. Namelijk het uitvoering geven aan een overeenkomst.
Wil de verantwoordelijke gegevens verstrekken aan de belastingdienst dan moet deze verwerking wederom apart worden beoordeeld. Het verstrekken van gegevens aan de belastingdienst is een wettelijke verplichting. Deze verwerking kan wederom gebaseerd worden op een grondslag uit artikel 8. Namelijk de noodzakelijkheid van de verwerking voor een wettelijke verplichting.
Beide verwerkingen in dit voorbeeld zijn noodzakelijk om het doel te bereiken en zijn gerechtvaardigd op basis van de grondslagen.

§ 2.5.3 Overige eisen
De verantwoordelijke moet voldoen aan de vereisten van de Wbp inzake de bewaartermijn en de beveiliging van de persoonsgegevens.

Bewaartermijn
Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden verwerkt.[53] De Wbp bevat geen concrete bewaartermijn. In beginsel moet een organisatie de gegevens verwijderen wanneer deze gegevens niet meer relevant zijn voor het doel. De verantwoordelijke moet zelf overwegen of er voldoende redenen zijn om de gegevens langer te bewaren of dat de noodzakelijkheid is verlopen en de gegevens vernietigd moeten worden. Persoonsgegevens mogen in een archief worden bewaard indien dit nodig is voor wetenschappelijke, statistische of historische doeleinden. Zodra ze niet meer nodig zijn voor deze doeleinden moeten de gegevens alsnog worden vernietigd.[54]

[52] Art. 8 sub f Wbp
[53] Art. 10 Wbp
[54] Art. 10 lid 2 Wbp

Beveiliging
De verantwoordelijke dient zorg te dragen voor passende technische en organisatorische maatregelen om persoonsgegevens tegen verlies of enige vorm van onrechtmatige verwerking te beveiligen. Technische en organisatorische maatregelen dienen cumulatief te worden getroffen.[55] De maatregelen dienen een passend beveiligingsniveau te garanderen. Gelet moet worden op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen dienen mede gericht te zijn om onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.[56] Het begrip 'passend' houdt in dat de beveiliging in overeenstemming is met de stand van de techniek. De stand van de techniek is tijdsgebonden en de verantwoordelijke zal periodiek moeten bepalen wat een passend beveiligingsniveau is. Daarnaast duidt het begrip 'passend' mede aan op de proportionaliteit tussen de beveiligingsmaatregelen en de te beschermen gegevens. Er moeten strengere eisen worden gesteld naarmate het belang van de gegevens groter is. Daarnaast moeten de maatregelen die worden gesteld passend zijn voor de risico's die de verwerking met zich meebrengt. Het niveau van bescherming dient groter te zijn indien er meerdere mogelijkheden zijn om dat niveau te waarborgen.[57]
In 2013 heeft de Autoriteit Persoonsgegevens richtlijnen opgesteld die weergeven op welke wijze maatregelen dienen te worden toegepast door de verantwoordelijke.[58] Tevens brengen deze richtlijnen in kaart op welke wijze de Autoriteit Persoonsgegevens de beveiliging in individuele gevallen beoordeelt.

§ 2.6 De verwerking van bijzondere persoonsgegevens
De Wbp maakt een onderscheid in algemene en bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn alle gegevens betreffende iemands:
- godsdienst of levensovertuiging;
- ras;
- politieke gezindheid;
- gezondheid;
- seksuele leven;
- lidmaatschap van een vakvereniging en;
- strafrechtelijke persoonsgegevens.[59]

In beginsel is het verwerken van bijzondere persoonsgegevens verboden. Op dit verbod bestaan enkele algemene en specifieke uitzonderingen. Wanneer er een uitzondering uit de Wbp geldt, en een bijzonder persoonsgegevens toch verwerkt mag worden, dan zijn de algemene beginselen van gegevensverwerking onverminderd van toepassing.[60]

§ 2.6.1 Specifieke uitzonderingen
De artikelen 17 t/m 22 Wbp bevatten de specifieke uitzonderingen op het verbod.

Godsdienst of levensovertuiging
De verwerking van gegevens omtrent godsdienst of levensovertuiging kan slechts geschieden door kerkgenootschappen of genootschappen op geestelijke grondslag of andere instellingen op godsdienstige of levensbeschouwelijke grondslag, indien dit noodzakelijk is met het oog op de geestelijke verzorging van de betrokkene, tenzij deze daartegen schriftelijk bezwaar maakt.[61]

[55] Kamerstukken II, 1997/98, 25892, 3 (MvT) p. 99.
[56] Art. 13 Wbp
[57] Art. 13 Wbp
[58] Richtsnoeren beveiliging 2013.
[59] Art. 17 Wbp
[60] Hooghiemstra & Nouwt 2007, p. 22.
[61] Art. 17 Wbp

Ras
Het verwerken van persoonsgegevens van iemands ras is heel uitzonderlijk en slechts toegestaan indien de verwerking geschiedt met het oog op identificatie van de betrokkene en slechts voor zover dit doel onvermijdelijk is of in het kader van een voorkeursbeleid.[62]

Politieke gezindheid
Het verbod op de verwerking van dergelijke gegevens is niet van toepassing indien de verwerking geschiedt door instellingen met een politieke grondslag betreffende hun leden of werknemers, dan wel andere tot de instelling behorende personen. Deze gegevens mogen slechts worden verwerkt indien de verwerking geschiedt met het oog op de eisen die met betrekking tot iemands politieke gezindheid redelijkerwijs kunnen worden gesteld in verband met de vervulling van functies in bestuursorganen en adviescolleges.[63]

Lidmaatschap vakbond
De betreffende vakbond, of de vakcentrale waarvan die bond een onderdeel vormt, mag de gegevens betreffende iemands lidmaatschap verwerken voor zover dat gelet op de doelstelling van de vakbond noodzakelijk is. In ieder geval worden er geen gegevens aan derden verstrekt zonder toestemming van de betrokkene.[64]

Gezondheid
De Wbp noemt een aantal groepen van verantwoordelijken die, onder bepaalde voorwaarden, gegevens over iemands gezondheid mogen verwerken.[65] Onder deze doelgroepen vallen onder andere:
- ziekenhuizen;
- speciale scholen;
- verzekeraars;
- de raad voor de kinderbescherming.[66]

Dergelijke gegevens mogen alleen worden verwerkt door deze groepen indien dit geschiedt door een persoon die uit hoofde van ambt, beroep of wettelijk voorschrift dan wel krachtens een overeenkomst is gebonden aan een geheimhoudingsplicht.[67]

Strafrechtelijke persoonsgegevens
Organen die krachtens de wet zijn belast met de toepassing van het strafrecht, alsmede door verantwoordelijkheden die deze hebben verkregen krachtens de Wet politiegegevens of de Wet justitiële en strafvorderlijke gegevens, zijn bevoegd om strafrechtelijke gegevens te verwerken.[68]

§ 2.6.2 Algemene uitzonderingen
Naast specifieke uitzonderingen voor bijzondere persoonsgegevens geeft de Wbp tevens algemene uitzonderingen op het verbod voor het verwerken van bijzondere persoonsgegevens.[69] Dit is een restbepaling die enkel van toepassing is indien men het verwerken van bijzondere persoonsgegevens niet kan baseren op de uitzonderingen van artikel 17 t/m 22 Wbp.

[62] Art. 18 Wbp
[63] Art. 19 Wbp
[64] Art. 20 lid 1 en 2 Wbp
[65] Sauerwein & Linnemann 2001, p. 48.
[66] Art. 21 lid 1 Wbp
[67] Art. 21 lid 2 Wbp
[68] Art. 22 lid 1 Wbp
[69] Art. 23 Wbp

Uitdrukkelijke toestemming van de betrokkene
Indien de betrokkene uitdrukkelijk toestemming geeft geldt het verbod van bijzondere gegevensverwerking niet.[70] De betrokkene moet duidelijk kenbaar maken dat hij toestemming geeft voor de verwerking. Voor verdere voorwaarden zie paragraaf 2.5.2.

Gegevens zijn door de betrokkene duidelijk openbaar gemaakt
De intentie van de betrokkene om de gegevens openbaar te maken moet duidelijk zijn.[71]

Verwerking is noodzakelijk bij gerechtelijke procedure
In sommige omstandigheden kan iemand geen gerechtelijke procedure volgen indien er geen gegevens beschikbaar zijn over de wederpartij.[72] Het begrip 'noodzakelijk' geeft aan dat de gegevens niet zonder meer verwerkt mogen worden. Er zal een afweging moeten worden gemaakt tussen het recht op een eerlijk proces en het recht van de betrokkene op zijn privacy. Dit is gebleken uit een uitspraak van de Centrale Raad van Beroep uit 1995.[73]

Verwerking is noodzakelijk ter verdediging van de vitale belangen van de betrokkene
Dit is een grondslag voor verwerking maar hiermee wordt het verbod op verwerking bijzondere gegevens niet verbroken. De gegevens mogen slechts op dat moment indien het noodzakelijk is worden verwerkt.[74]

Verwerken is noodzakelijk ter voldoening aan een volkenrechtelijke verplichting
Voor deze uitzondering dient er een concrete rechtsgrondslag te bestaan. De grondslag voor het verwerken is niet formeel wettelijk maar het moet duidelijk zijn dat in de volkenrechtelijke regeling de verplichting slechts kan worden uitgevoerd indien bepaalde gegevens worden verwerkt. Hierbij moet sprake zijn van een zwaarwegend belang. Alleen dan is het verbod om bijzondere gegevens te verwerken niet van toepassing.[75]

Wet of ontheffing Autoriteit Persoonsgegevens
Indien een bijzondere wet aangeeft dat bijzondere gegevensverwerking is toegestaan, of de Autoriteit Persoonsgegevens een ontheffing verleent, is het verbod niet van toepassing.[76] Er moet hierbij aan twee voorwaarden worden voldaan: de verwerking dient noodzakelijk te zijn met het oog op een zwaarwegend algemeen belang en in het belang van de persoonlijke levenssfeer moeten er passende waarborgen worden gecreëerd.[77]

De gegevens worden verwerkt door de Autoriteit Persoonsgegevens of een ombudsman
Het verbod is niet van toepassing indien de Autoriteit Persoonsgegevens of een ombudsman de gegevens verwerkt op grond van artikel 9:17 Algemene wet bestuursrecht (hierna: Awb).[78] Bij deze regels geldt dat er sprake moet zijn van een zwaarwegend belang en er moeten passende waarborgen worden gecreëerd in het belang van de persoonlijke levenssfeer.[79]

[70] Art. 23 sub a Wbp
[71] Art. 23 sub b Wbp
[72] Art. 23 sub c Wbp
[73] CRvB 15 februari 1995, (JB 1995-64).
[74] Art. 23 sub d Wbp
[75] Art. 23 sub e Wbp
[76] Art. 23 sub f Wbp
[77] Kamerstukken II, 1997/98, 25892, 3 (MvT) p. 124.
[78] Art. 23 sub g Wbp
[79] Kamerstukken II, 1997/98, 25892, 3 (MvT) p. 10.

§ 2.6.3 Burger Service Nummer

De Wbp bepaalt dat een nummer dat ter identificatie bij wet is voorgeschreven, slechts verwerkt mag worden ter uitvoering van die betreffende wet, dan wel voor doeleinden bij die wet bepaald.[80] Het Burgerservicenummer (hierna: BSN) is zo'n identificatienummer. De Wet algemene bepalingen Burgerservicenummer (hierna: Wabb) bevat regels omtrent de gebruikers van dit nummer. Een overheidsorgaan of een ieder ander, voor zover deze werkzaamheden verricht waarbij het gebruik door hem of haar van het BSN bij of krachtens de wet is voorgeschreven, is bevoegd tot verwerking van het BSN.[81] In de eerste plaats is het BSN bedoeld voor contact tussen een burger en de overheid. Andere organisaties mogen slechts van het BSN gebruik maken indien dit wettelijk is bepaald.

§ 2.7 De verplichtingen van de verantwoordelijke

De verantwoordelijke dient aan een aantal verplichtingen te voldoen wanneer zij persoonsgegevens verwerken. Deze verplichtingen zien toe op de veiligheid en de bescherming van de persoonsgegevens. Daarnaast heeft de verantwoordelijke tevens de verplichting om informatie te verstrekken aan zowel de Autoriteit Persoonsgegevens als aan de betrokkene.

Geheimhoudingsplicht

De verantwoordelijke dient ervoor te zorgen dat iedere persoon die gegevens verwerkt een geheimhoudingsplicht heeft ten aanzien van de gegevens die zij verwerken.[82] Dit geldt slechts voor zover deze personen niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen.

Meldingsplicht en vooronderzoek

De verantwoordelijke dient een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens te melden bij de Autoriteit Persoonsgegevens.[83] Paragraaf 3.3 gaat hier nader op in.

Informatieplicht aan betrokkene

In de Wbp zijn de bepalingen omtrent informatieverstrekking in de artikelen 33 en 34 uitgewerkt. Deze bepalingen vormen een uitwerking van het transparantiebeginsel. De gegevensverwerking is in beginsel slechts 'behoorlijk' indien de betrokkene op de hoogte wordt gehouden van de verwerking. De Wbp geeft echter uitzonderingen op deze bepalingen.[84] Een belangrijk instrument om de gegevensverwerking transparant te maken is de verplichting van de verantwoordelijke om op eigen initiatief de betrokkene op de hoogte te stellen van de gegevensverwerking. De betrokkene dient in staat te zijn om de gegevensverwerking te volgen en om deze verwerking aan te vechten indien deze onrechtmatig is.[85] De verantwoordelijke dient hierbij de identiteit en de doeleinden van de verwerking te vermelden.[86]

Het onderscheid tussen artikel 33 en 34 Wbp bestaat voornamelijk uit het tijdstip waarop de betrokkene wordt geïnformeerd. Indien de persoonsgegevens bij de betrokkene zelf worden verkregen, dient de verantwoordelijke de betrokkene vóór het moment van verkrijging op de

[80] Art. 24 lid 1 Wbp
[81] Art. 1 sub d Wabb
[82] Art. 12 lid 2 jo 15 Wbp
[83] H4 Wbp
[84] Wbp-naslag art. 33.
[85] Art. 13 Wbp
[86] Art. 33 lid 2 jo 34 lid 2 Wbp

hoogte te stellen van de verkrijging, tenzij de betrokkene hiervan reeds op de hoogte is.[87] Worden de gegevens op een andere wijze verkregen, bijvoorbeeld via derden, dan wordt de betrokkene op de hoogte gesteld:

- op het moment van vastlegging van de betreffende gegevens, of;
- wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking.

Het uitgangspunt is dat de verantwoordelijke een informatieplicht heeft. Dit betekent echter niet dat de betrokkene geheel vrij is van verantwoordelijkheden. De betrokkene heeft een zekere onderzoeksplicht. In hoeverre de verantwoordelijke informatie moet verstrekken dan wel de betrokkene zelf op onderzoek uit moet gaan is niet wettelijk bepaald maar wordt bepaald door wat in het maatschappelijk verkeer redelijkerwijs verwacht mag worden. Factoren die hierbij een rol kunnen spelen zijn de soort gegevens, de verwerkingen die de verantwoordelijke wil verrichten, de eventuele derden aan wie de gegevens kunnen worden verstrekt, maar ook de maatschappelijke positie en onderlinge verhouding tussen de verantwoordelijke en de betrokkene, alsmede de wijze waarop zij met elkaar in contact zijn getreden.[88] Op de verantwoordelijke rust een extra verantwoordelijkheid tot informeren indien hij zelf de betrokkene benadert.[89] De betrokkene die de verantwoordelijke benadert, zal veelal op de hoogte zijn van diens identiteit en doeleinden.[90] Wanneer de betrokkene bijvoorbeeld elektronisch gegevens verstrekt dan is het voor de verantwoordelijke voor de hand liggend om langs dezelfde weg de betrokkene te informeren over de gegevensverwerking. Hierbij kan worden gedacht aan een privacybeleid waar de betrokkene naar wordt verwezen.

Op de informatieplicht bestaan een tweetal uitzonderingen. Er hoeft geen informatie aan de betrokkene te worden verstrekt indien:

- dit onmogelijk blijkt doordat de betrokkene bijvoorbeeld niet te achterhalen is of indien dit onevenredige inspanning kost. In dit geval mag de verantwoordelijke slechts de herkomst van de gegevens vaststellen.[91]
- indien de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval dient de verantwoordelijke de betrokkene op diens verzoek te informeren over het wettelijk voorschrift dat tot de vastlegging of verstrekking van de hem betreffende gegevens heeft geleid.[92]

Meldplicht bij datalek

De verantwoordelijke dient de Autoriteit Persoonsgegevens op de hoogte te stellen indien er sprake is van een datalek.[93] In paragraaf 3.5 wordt hier dieper op ingegaan.

§ 2.8 Rechten van de betrokkene

In beginsel moet iedereen in de gelegenheid zijn om na te kunnen gaan of zijn gegevens worden verwerkt. Dit is een belangrijk onderdeel van het transparantiebeginsel.[94] De betrokkene heeft het recht om de verantwoordelijke te verzoeken hem te informeren over de verwerkte persoonsgegevens. De verantwoordelijke dient schriftelijk binnen vier weken te

[87] Art. 33 lid 1 Wbp

[88] Kamerstukken II, 1997/98, 25892, 3 (MvT) p.36.

[89] Art. 33 lid 3 jo 34 lid 3 Wbp

[90] Kamerstukken II, 1997/98, 25892, 3 (MvT) p. 150-151.

[91] Art. 34 lid 4 Wbp

[92] Art. 34 lid 5 Wbp

[93] Art. 34a lid 1 Wbp

[94] Wbp-naslag art. 35 Wbp

antwoorden.[95] Indien dergelijke gegevens worden verwerkt, bevat de mededeling van de verantwoordelijke:

- een volledig overzicht van de gegevensverwerking in begrijpelijke taal;
- een omschrijving van het doel;
- de categorieën van gegevens waarop de verwerking betrekking heeft;
- de beschikbare informatie over de herkomst van de gegevens.[96]

De betrokkene kan de verantwoordelijke verzoeken om zijn persoonsgegevens aan te passen, te verwijderen of af te schermen wanneer deze feitelijk onjuist, onvolledig of niet ter zake dienden zijn voor het doel, dan wel in strijd zijn met een wettelijk voorschrift.[97] Een weigering van het verzoek dient met redenen te worden omkleed.[98] Geeft de verantwoordelijke gehoor aan het verzoek, dan dient hij er zorg voor te dragen dat dit zo spoedig mogelijk wordt uitgevoerd.[99] Tevens is de verantwoordelijke verplicht om derden, aan wie de gegevens al waren verstrekt, zo snel mogelijk van de correctie op de hoogte te brengen, tenzij dit onmogelijk blijkt of onevenredige inspanning kost.[100]

§ 2.9 Rechtsbescherming

De betrokkene heeft de mogelijkheden om verzet aan te tekenen, bezwaar te maken, schadevergoeding te eisen of bij de rechter een verbod tegen de verwerking te eisen.

Verzet

Indien gegevens op grond van artikel 8 sub e en f worden verwerkt, kan de betrokkene daartegen verzet aantekenen in verband met zijn persoonlijke omstandigheden.[101] Tevens kan de betrokkene verzet aantekenen indien gegevens worden verwerkt in verband met de totstandbrenging of instandhouding van een directe relatie tussen de verantwoordelijke of een derde met de betrokkene voor commerciële doeleinden.

Bezwaar

Een beslissing van een bestuursorgaan op het verzoek van een betrokkene is een besluit in de zin van de Awb. Het gaat hierbij slechts om een verzoek als in de artikelen 30 lid 3, 35, 36 en 38 lid 2 Wbp.[102] Dit betekent dat de betrokkene bezwaar kan aantekenen en in beroep kan gaan op grond van artikel 7:1 jo 8:1 Awb. De betrokkene kan een voorlopige voorziening aanvragen wanneer hij een dringend belang heeft bij het onmiddellijk staken van de verwerking.[103] In beginsel hebben de rechten die aan de betrokkene zijn toegekend ook alleen betrekking op de betrokkene zelf. Desondanks is het niet altijd te vermijden dat toelating van een verzoek ook inzicht kan geven in gegevens die op anderen betrekking hebben maar waar de betrokkene ook belang bij heeft.

Schadevergoeding

Indien de betrokkene schade lijdt doordat jegens hem in strijd is gehandeld met de bepalingen uit de Wbp, dan is de verantwoordelijke aansprakelijk voor die gelede schade. [104] De betrokkene kan zich tot de rechtbank wenden. Als de verantwoordelijke kan bewijzen dat

[95] Art. 35 lid 1 Wbp
[96] Art. 35 lid 2 Wbp
[97] Art. 36 lid 1 Wbp
[98] Art. 36 lid 2 Wbp
[99] Art. 36 lid 3 Wbp
[100] Art. 38 lid 1 Wbp
[101] Art. 40 lid 1 Wbp
[102] Art. 45 Wbp
[103] Art. 8:81 lid 1 Awb
[104] Art. 49 lid 1 jo 49 lid 3 Wbp

de schade hem niet kan worden toegerekend, kan hij geheel of gedeeltelijk ontheven worden van deze aansprakelijkheid.

Verbod
Wanneer de verantwoordelijke in strijd handelt met hetgeen dat in de Wbp is opgenomen, en een ander daar schade door lijdt of dreigt te lijden, kan de rechter hem zodanig gedrag verbieden en hem bevelen maatregelen te treffen om de gevolgen van dat gedrag te herstellen.[105]

§ 2.10 Conclusie
Het recht op bescherming van de privacy kan worden ontleend op zowel internationaal als op nationaal niveau. In Nederland is de Wbp de belangrijkste wetgeving voor de privacy. De Wbp bevat regels inzake de verwerking van persoonsgegevens. Sinds 1 januari 2016 is de Wbp gewijzigd. De meldingsplicht bij een datalek en de uitbreiding van bestuurlijke boetebevoegdheden van de Autoriteit Persoonsgegevens zijn de belangrijkste wijzigingen.

Er bestaan specifieke regels omtrent het verwerken van persoonsgegevens. Indien persoonsgegevens worden verwerkt, moet het verwerkingsproces voldoen aan een aantal eisen. Deze eisen worden weergegeven in de algemene beginselen van gegevensverwerking. De gegevens moeten conform de wet, op zorgvuldige en behoorlijke wijze worden verwerkt. Voorafgaand aan het verzamelen van gegevens moet de verantwoordelijke een doel omschrijven. Op basis van dit doet kan worden bepaald welke gegevens mogen worden verzameld. De verwerking van de gegevens moeten gebaseerd kunnen worden op dit doel. Er mogen niet meer gegevens worden verzameld dan noodzakelijk is om dit doel te bereiken. Daarnaast bevat de Wbp bepaalde grondslagen die de verwerking van persoonsgegevens rechtmatig maakt. De verantwoordelijke dient bij het verwerken van persoonsgegevens aandacht te geven aan de bewaartermijn en de manier waarop de gegevens zijn beveiligd.

Er bestaat een verschil tussen de algemene en de bijzondere persoonsgegevens. De algemene gegevens mogen worden verwerkt mits zij aan de regels van de Wbp voldoen. Bijzondere gegevens mogen niet worden verwerkt, tenzij zij aan bepaalde uitzonderingen van de Wbp voldoen. Het BSN is een apart geval. Wil een organisatie een BSN verwerken dan zal daar een directe grondslag uit een wet voor moeten zijn.

Degene die gegevens verwerkt heeft een aantal verantwoordelijkheden met betrekking tot het beschermen van de gegevens en het informeren van de Autoriteit Persoonsgegevens en de betrokkene. Zo moet hij zorgen voor een geheimhoudingsplicht van iedereen die de gegevens verwerkt en zal hij informatie aan zowel de Autoriteit Persoonsgegevens als aan de betrokkene moeten verstrekken. De betrokkene heeft ook rechten en kan indien nodig rechtsbescherming aanvragen.

[105] Art. 50 lid 1 Wbp

Hoofdstuk 3 Autoriteit Persoonsgegevens

Dit hoofdstuk gaat in op de Autoriteit Persoonsgegevens. Middels een interview met een medewerkster van de Autoriteit Persoonsgegevens kan er een beeld van het bestuursorgaan worden geschetst. Het interview is opgenomen in bijlage I. Er wordt in kaart gebracht welke taken en bevoegdheden de Autoriteit Persoonsgegevens heeft. Daarnaast wordt ingegaan op het toezicht van de Autoriteit Persoonsgegevens en de verschillende sancties die zij kan opleggen. Met de wetswijziging meldplicht datalekken die op 1 januari 2016 is ingegaan heeft de Autoriteit Persoonsgegevens boetebevoegdheden gekregen. Tevens worden de beleidsregels over de wetswijziging meldplicht datalekken in kaart gebracht. Tot slot is er een kleine conclusie.

§ 3.1 Het bestuursorgaan

Sinds 1 januari 2016 wordt het College bescherming persoonsgegevens de Autoriteit Persoonsgegevens genoemd.[106] De Autoriteit Persoonsgegevens is een onafhankelijk, zelfstandig bestuursorgaan. Binnen de organisatie zijn ongeveer 80 mensen werkzaam. De Autoriteit Persoonsgegevens bestaat uit een college, directeur, een afdeling communicatie, een afdeling juridische zaken en een afdeling bedrijfsvoering. Daarnaast bestaan er twee afdelingen die het college ondersteunen met het houden van toezicht op de publieke en de private sector.[107]

De Autoriteit Persoonsgegevens houdt zich bezig met het toezicht op de naleving van de wettelijke regels voor het verwerken van persoonsgegevens en adviseert over nieuwe regelgeving. Het grondrecht op bescherming van privacy is essentieel voor de werking van de rechtsstaat. De Autoriteit Persoonsgegevens beschermt dit recht.[108]

§ 3.2 Taken en bevoegdheden

Om het recht op privacy te waarborgen heeft de Autoriteit Persoonsgegevens een aantal taken en bevoegdheden. De taken en bevoegdheden van de Autoriteit Persoonsgegevens zijn vastgelegd in de Wbp.[109] Zo is de Autoriteit Persoonsgegevens belast met toezicht, advisering, voorlichting, informatieverstrekking en verantwoording en internationale taken.[110] De taken worden aan de Autoriteit Persoonsgegevens opgedragen via de wet. De Autoriteit Persoonsgegevens vervult taken in onafhankelijkheid.[111] In artikel 51 tot en met 61 Wbp worden de taken en bevoegdheden van de Autoriteit Persoonsgegevens opgesomd.

De Autoriteit Persoonsgegevens heeft onder andere de volgende taken en bevoegdheden:

- toezien op de verwerking van persoonsgegevens;
- adviseren over wetsvoorstellen;
- samenwerkingsprotocollen vaststellen;
- onderzoek naar gegevensverwerking uitvoeren;
- voorafgaand onderzoek uitvoeren;
- sancties aan verantwoordelijken opleggen.

[106] Art. 51 lid 4 Wbp

[107] Autoriteitpersoonsgegevens.nl.

[108] Autoriteitpersoonsgegevens.nl (zoek op *missie en visie*).

[109] Hoofdstuk 9 Wbp

[110] Bijlage I

[111] Art. 52 lid 1 en 2 Wbp

§ 3.2.1 De functionaris voor de gegevensbescherming

Een verantwoordelijke, of een organisatie waar verantwoordelijken bij zijn aangesloten, kan een eigen functionaris voor de gegevensbescherming (hierna: FG) benoemen.[112] De FG is een onafhankelijke toezichthouder binnen een organisatie.[113] De Wbp stelt een aantal eisen aan de FG. Als FG kan slechts een natuurlijk persoon worden benoemd. De FG kan dus niet bestaan uit een ondernemingsraad of een commissie. Daarnaast moet de FG over genoeg kennis beschikken om de taak te vervullen en hij moet voldoende betrouwbaar wordt geacht. De FG heeft dan ook een geheimhoudingsplicht. De FG voert zijn functie zelfstandig uit en krijgt geen aanwijzingen van de verantwoordelijke door wie hij is benoemd. De verantwoordelijke moet de FG bij de Autoriteit Persoonsgegevens aanmelden.[114] De FG levert een belangrijke bijdrage aan het correct verwerken van persoonsgegevens door de organisatie. Daarnaast draagt het Nederlands genootschap van Functionarissen voor de gegevensbescherming bij aan een goede taakvervulling van de FG.

De werkzaamheden van de FG zijn onder andere:

- toezicht houden op de verwerking van persoonsgegevens;
- de gegevensverwerking inventariseren;
- bijhouden van meldingen van gegevensverwerking;
- afhandelen van vragen en klachten;
- ontwikkelen van interne regelingen;
- adviseren over technologie en beveiliging;
- leveren van input bij het opstellen en aanpassen van een gedragscode;
- naleven van de gedragscode.[115]

De FG heeft geen formele sanctiebevoegdheden. De verantwoordelijke is wel verplicht om de FG controlebevoegdheden te geven. Een FG moet onder andere bevoegd zijn om ruimtes te betreden, zaken te onderzoeken en inlichtingen en inzage te verkrijgen.[116]

§ 3.3 Melding en voorafgaand onderzoek

Indien er sprake is van gegevensverwerking kan de verantwoordelijke verplicht zijn om hier voorafgaand aan de verwerking een melding van te doen. Tevens kan er een voorafgaand onderzoek nodig zijn.

§ 3.3.1 Melding

Een verantwoordelijke moet een geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens melden aan de Autoriteit Persoonsgegevens.[117] Indien een FG is aangesteld, dan kan de organisatie de verwerkingen bij de FG melden in plaats van bij de Autoriteit Persoonsgegevens, tenzij een voorafgaand onderzoek nodig is.[118] Deze melding dient te gebeuren voorafgaand aan de verwerking.[119] De Autoriteit Persoonsgegevens alsmede de FG stellen een openbaar register op van alle gegevensverwerkingen. Iedereen kan dit register kosteloos opvragen zodat men kan zien wie persoonsgegevens verwerkt en voor welk doel.[120]

[112] Art. 62 Wbp
[113] Ngfg.nl (zoek op *home*).
[114] Art. 63 Wbp
[115] Art. 64 Wbp
[116] Autoriteit Persoonsgegevens.nl (zoek op *FG*).
[117] Art. 27 Wbp
[118] Autoriteit Persoonsgegevens.nl (zoek op *FG*).
[119] Art. 27 lid 3 Wbp
[120] Bijlage I

In de melding dienen in ieder geval de volgende punten worden benoemd:
- naam en adres van de verantwoordelijke;
- het doel van de verwerking;
- een beschrijving van de categorie betrokkene en de gegevens;
- de ontvangers aan wie gegevens worden verstrekt;
- de voorgenomen doorgiften van gegevens naar landen buiten de EU;
- een algemene beschrijving over de gepastheid van de maatregelen.[121]

De verantwoordelijke dient zelf te beoordelen of de gegevensverwerking gemeld moet worden.[122] De Autoriteit Persoonsgegevens heeft een stappenplan opgesteld om een beoordeling te maken of de gegevensverwerking moet worden gemeld. De volgende stappen kunnen door de verantwoordelijke worden gevolgd:
- een inventarisatie maken van alle verwerkingen binnen de organisatie;
- iedere verwerking individueel beoordelen of dit voldoet aan de meldingsplicht;
- nagaan of verwerkingen zijn vrijgesteld;
- beoordelen of de gegevensverwerking specifieke risico's met zich meebrengt, in dat geval is er een voorafgaand onderzoek nodig en is melding verplicht.[123]

Organisaties kunnen zelf bepalen hoe zij het meldingsproces inrichten, voor zover zij zich daarbij aan de wettelijke regels houden. De FG kan een speciale versie van het Wbp-Meldingsprogramma van de Autoriteit Persoonsgegevens gebruiken. Vanaf het moment dat de verantwoordelijke een ontvangstbevestiging heeft ontvangen van de Autoriteit Persoonsgegevens is de melding geldig. Dit is echter geen bevestiging dat de gegevensverwerking op de juiste manier gebeurt. Via de Autoriteit Persoonsgegevens kan de verantwoordelijke de melding later nog wijzigen of intrekken.[124]

De gegevensverwerking waarbij de inbreuk op de fundamentele rechten en vrijheden van de betrokkene onwaarschijnlijk zijn, wordt vrijgesteld van de meldingsplicht.[125]

§ 3.3.2 Voorafgaand onderzoek

Sommige gegevensverwerkingen brengen specifieke risico's met zich mee. Indien dit het geval is, bepaalt de Wbp dat er een onderzoek plaatsvindt voorafgaand aan de verwerking. Het voorafgaand onderzoek wordt uitgevoerd door de Autoriteit Persoonsgegevens waarbij zij kijken of de verwerking aan de wettelijke eisen van de Wbp voldoet.[126]

De Autoriteit Persoonsgegevens stelt een voorafgaand onderzoek in, indien de verantwoordelijke:
- een persoonsnummer, zoals bijvoorbeeld het BSN, wil verwerken voor een ander doel dan waarvoor dit nummer bestemd is;
- gegevens wil vastleggen op grond van het gericht verzamelen van informatie door middel van een eigen onderzoek zonder dat de betrokkene hiervan op de hoogte wordt gesteld;
- strafrechtelijke gegevens ten behoeve van derden wil verwerken.[127]

De verantwoordelijke dient het voorafgaand onderzoek zelf aan te vragen en zal dus zelf moeten beoordelen of dit voorafgaand onderzoek is vereist. Indien een voorafgaand

[121] Art. 28 lid 1 Wbp
[122] Autoriteit Persoonsgegevens.nl (zoek op *gegevensverwerking*).
[123] Autoriteit Persoonsgegevens.nl (zoek op *gegevensverwerking*).
[124] Bijlage I
[125] Art. 29 Wbp
[126] Bijlage I
[127] Art. 31 Wbp

onderzoek is vereist moet de gegevensverwerking tevens aan de Autoriteit Persoonsgegevens worden gemeld.[128] Het onderzoek bestaat uit één of twee fases, het voorafgaand onderzoek en eventueel een nader onderzoek. Het voorbereidend onderzoek duurt maximaal 4 weken waarin de Autoriteit Persoonsgegevens een algemeen oordeel vormt over de verwerking. Op basis hiervan kan de Autoriteit Persoonsgegevens besluiten om een nader onderzoek in te stellen. Indien de Autoriteit Persoonsgegevens heeft besloten om de verwerking nader te onderzoeken dan begint fase 2. Het nader onderzoek duurt maximaal 20 weken. Het onderzoek bestaat uit een feitenonderzoek waarbij de rechtmatigheid van de verwerking wordt getoetst. In het bijzonder let de Autoriteit Persoonsgegevens op de risico's die de verwerking met zich meebrengt en of er voldoende maatregelen zijn getroffen om de gegevens te beschermen. De Autoriteit Persoonsgegevens neemt een ontwerpbesluit naar aanleiding van het onderzoek. Dit besluit wordt gepubliceerd waarna de verantwoordelijke en belanghebbende 6 weken de tijd hebben om een zienswijze te geven. Na dit termijn wordt er een definitief besluit genomen of de gegevensverwerking mag doorgaan of niet. Dit besluit wordt tevens gepubliceerd in de Staatscourant en op de website van de Autoriteit Persoonsgegevens. Indien de verantwoordelijke of een belanghebbende het niet met dit besluit eens is kan diegene beroep instellen tegen het besluit.[129]

§ 3.4 Sancties

De Autoriteit Persoonsgegevens heeft verschillende sanctiebevoegdheden. Zo is zij bevoegd om een last onder bestuursdwang[130] of een bestuurlijke boete[131] op te leggen ter handhaving van de bij de Wbp gestelde verplichtingen. Tevens bestaat er een mogelijkheid tot strafrechtelijke sancties.[132] De Boetebeleidsregels Autoriteit Persoonsgegevens 2016 (hierna: BAP) geven richtlijnen voor de bepaling van de hoogte van de bestuurlijke boete.

§ 3.4.1 Boetebevoegdheden

Op 1 januari 2016 is het wetsvoorstel Meldplicht datalekken in werking getreden.[133] Naar aanleiding hiervan zijn er belangrijke wijzigingen opgetreden in de Wbp. De Autoriteit heeft sterkere sanctiemogelijkheden om de naleving van de Wbp te bevorderen. Zo heeft zij de bevoegdheid gekregen om hoge bestuurlijke boetes op te leggen indien de wetgeving voor de privacy wordt overtreden. Vooral de preventieve werking van de boetebevoegdheden is voor de Autoriteit Persoonsgegevens van belang. De Autoriteit Persoonsgegevens hoopt hiermee bedrijven en overheden te stimuleren om eerder aandacht te schenken aan de bescherming van persoonsgegevens. Op deze manier zouden privacy overtredingen voorkomen kunnen worden. Indien de verantwoordelijke een overtreding van de Wbp heeft gepleegd, is de Autoriteit bevoegd om direct een boete op te leggen.

Uitgangspunt bij het bepalen van de hoogte van de boete is dat deze in verhouding staat met de begane overtreding. Op grond hiervan is er daarom gekozen voor een categorie-indeling en een bandbreedte-systematiek. De artikelen van de Wbp zijn ingedeeld in categorie 1, 2 of 3. Bij een overtreding wordt aan de hand van de categorie waar dat artikel staat gekeken wat de maximale hoogte van de boete is. In categorie 1 is de maximale boete € 820.000. In categorie 2 kan de boete oplopen tot € 450.000 en in categorie 3 is de maximale boete €20.500.[134] De precieze hoogte van de boete wordt bepaald door de ernst van de

[128] Art. 32 lid 1 Wbp
[129] Bijlage I
[130] Art. 65 Wbp
[131] Art. 66 Wbp
[132] Art. 75 Wbp
[133] Kamerstukken I, 2014/15, 33662, A.
[134] Bijlage 1,2 &3 BAP

overtreding.[135] Indien op grond van de overtreding aan de verantwoordelijke een boete van € 820.000 euro opgelegd kan worden, maar de Autoriteit Persoonsgegevens dit niet passend vindt, kan de Autoriteit Persoonsgegevens besluiten om een boete op te leggen ten hoogste 10% van de jaaromzet van de rechtspersoon.

De Autoriteit Persoonsgegevens kan later nog beslissen om de boete te verlagen of te verhogen. In artikel 9 en 10 van de Boetebeleidsregels Autoriteit Persoonsgegevens worden hier richtlijnen voor gegeven.

§ 3.5 Meldplicht datalekken

De verantwoordelijke stelt de Autoriteit Persoonsgegevens direct op de hoogte indien er sprake is van een inbreuk op de beveiliging en dit ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.[136] De verantwoordelijke moet tevens de betrokkene inlichten over de inbreuk. De melding omvat in ieder geval de aard van de inbreuk, de betrokkene en de aanbevolen maatregelen om de gevolgen te beperken.[137]

De verantwoordelijke dient zelf te bepalen of er sprake is van een datalek. Vervolgens moet de verantwoordelijke zelf een afweging maken of zij dit daadwerkelijk aan de Autoriteit Persoonsgegevens moet melden. De Autoriteit Persoonsgegevens heeft beleidsregels opgesteld omtrent de meldplicht datalekken.[138] Deze regels kunnen de verantwoordelijke helpen in de beoordeling of er sprake is van een datalek is en wanneer dit gemeld moet worden.

Er is een datalek indien er sprake is van een inbreuk op de beveiliging, waarbij persoonsgegevens verloren zijn gegaan, en er kan niet worden uitgesloten dat gegevensverwerking onrechtmatig worden verwerkt. Is er vervolgens sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, dan moet de datalek aan de Autoriteit Persoonsgegevens worden gemeld.[139]

Een datalek is een vernietiging, wijziging, het vrijkomen van of de toegang tot persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Niet alleen het vrijkomen of lekken van persoonsgegevens, maar ook het onrechtmatig verwerken van persoonsgegevens is een datalek. Indien persoonsgegevens worden blootgesteld aan verlief of onrechtmatige verwerking door een inbreuk op de beveiliging van deze gegevens dan wordt er dus gesproken van een datalek.

Voorbeelden van datalekken

- Een kwijtgeraakte usb-stick met persoonsgegevens.
- Een gestolen laptop.
- Een inbraak in een databestand, zoals het systeem waarin de gegevens worden opgeslagen.

Een datalek kan bij de Autoriteit Persoonsgegevens worden gemeld via het meldloket datalekken.

[135] Art. 5 jo 6 BAP

[136] Art. 34a lid 1 Wbp

[137] Art. 34a lid 3 Wbp

[138] Beleidsregels meldplicht datalekken 2015.

[139] Beleidsregels meldplicht datalekken 2015, p.5.

§ 3.6 Conclusie

Het College bescherming persoonsgegevens wordt sinds 1 januari 2016 de Autoriteit Persoonsgegevens genoemd. De taak van de Autoriteit Persoonsgegevens is het toezicht houden op de naleving van de wettelijke regels voor het verwerken van persoonsgegevens en het adviseren over nieuwe regelgeving. Daarnaast is de Autoriteit Persoonsgegevens belast met het geven van voorlichtingen, informatieverstrekking & verantwoording en internationale taken. Een verantwoordelijke kan een eigen functionaris voor de gegevensbescherming benoemen. Als FG kan slechts een natuurlijk persoon worden benoemd. De FG is een onafhankelijke toezichthouder binnen een organisatie.

De verantwoordelijke is verplicht voorafgaand aan de verwerking een melding te doen van de gegevensverwerking. Tevens kan er een voorafgaand onderzoek nodig zijn.

De Autoriteit Persoonsgegevens heeft verschillende sanctiebevoegdheden. Zo is zij bevoegd om een last onder bestuursdwang of een bestuurlijke boete op te leggen ter handhaving van de bij de Wbp gestelde verplichtingen. Tevens bestaat er een mogelijkheid tot strafrechtelijke sancties. Op 1 januari 2016 is het wetsvoorstel Meldplicht datalekken in werking getreden. Naar aanleiding hiervan zijn er belangrijke wijzigingen opgetreden in de Wbp. De Autoriteit heeft sterkere sanctiemogelijkheden om de naleving van de Wbp te bevorderen. Zo heeft zij de bevoegdheid gekregen om hoge bestuurlijke boetes op te leggen indien de wetgeving voor de privacy wordt overtreden. De verantwoordelijke stelt de Autoriteit Persoonsgegevens direct op de hoogte indien er sprake is van een inbreuk op de beveiliging en dit ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. De verantwoordelijke moet tevens de betrokkene inlichten over de inbreuk. De melding omvat in ieder geval de aard van de inbreuk, de betrokkene en de aanbevolen maatregelen om de gevolgen te beperken.

Hoofdstuk 4 Gegevensverwerking binnen Payper

In dit hoofdstuk wordt ingegaan op de verwerking van persoonsgegevens binnen Payper. Onder verschillende personen binnen de organisatie is een vragenlijst uitgezet om op deze manier in kaart te brengen op welke wijze gegevens door de medewerkers worden verwerkt. De vragenlijst bevat tevens een toelichting ter verduidelijking. De vragenlijsten zijn opgenomen in bijlage II. De bijbehorende toelichting is opgenomen in bijlage III. Daarnaast zijn er een aantal vragen gesteld aan de Legal Counsel die binnen Payper werkzaam is. Dit interview is opgenomen in bijlage IV.

Voor een groot deel van de medewerkers van Payper is het onduidelijk welke regels er gelden omtrent het privacyrecht met betrekking tot gegevensverwerking. Naar aanleiding van de vragenlijsten is duidelijk geworden welke gegevens worden verwerkt en op welke manier dit gebeurt. Om uiteindelijk te kunnen bepalen of de wijze van Payper omtrent gegevensverwerking voldoet aan de eisen die de Wbp hieraan stelt, is het belangrijk om te onderzoeken op welke wijze Payper persoonsgegevens verwerkt. Daarnaast is het belangrijk om de resultaten van dit praktijkonderzoek in beeld te brengen om uiteindelijk de juiste aanbevelingen aan Payper kunnen doen.

§ 4.1 Salesforce en Flexservice

Payper werkt met verschillende programma's om gegevens in te verwerken. De twee belangrijkste zijn Salesforce en Flexservice. Deze programma's worden onder andere gebruikt voor de dossieropbouw.

Payper heeft aangegeven dat zij nog niets hebben vastgelegd omtrent de verwerking van persoonsgegevens.[140] Er bestaat geen privacyreglement en de werknemers zijn niet ingelicht over specifieke regels omtrent de wijze waarop zij persoonsgegevens mogen verwerken. Er bestaan verschillende afdelingen binnen Payper zoals Operations, Sales, Verzuim, Finance en Legal. Verschillende overeenkomsten worden gesloten met werknemers, intermediairs en opdrachtgevers. Dit zorgt voor een brede verwerking van persoonsgegevens.

§ 4.2 Algemene gegevensverwerking

Middels de vragenlijst is er in kaart gebracht welke persoonsgegevens door Payper worden verwerkt en van wie deze gegevens zijn. De medewerkers hebben aangegeven dat er voornamelijk algemene gegevens worden verwerkt. Dit zijn:

- Naam, adres, woonplaats (hierna: NAW)
- Geboortedatum
- Telefoonnummer
- E-mailadres
- Leeftijd
- Geslacht
- Burgerservicenummer
- Rekeningnummer[141]

Een belangrijke vraag om inzicht te krijgen in de omvang van gegevensverwerking binnen Payper, is van wie en door wie de persoonsgegevens worden verwerkt. Binnen Payper werken ongeveer 45 mensen op verschillende afdelingen. De medewerkers hebben verschillende gegevens nodig van verschillende mensen om hun functie te kunnen uitoefenen. Uit de resultaten blijkt dat voornamelijk gegevens worden verwerkt van payrollwerknemers, opdrachtgevers, klanten, contactpersonen van bedrijven die benaderd

[140] Bijlage IV

[141] Bijlage II

worden en van intermediairs. Dit geeft aan dat de gegevensstroom binnen Payper zeer omvangrijk is.

§ 4.3 Algemene beginselen

Om te kunnen bepalen of de gegevens rechtmatig worden verzameld en verwerkt, worden de eisen die de Wbp stelt vergeleken met de wijze waarop Payper gegevens verwerkt. De verwerking dient ten eerste te voldoen aan de algemene beginselen van gegevensverwerking. Het is van belang dat er een specifiek doel door de organisatie is vastgesteld.[142] Dit doel moet aan een aantal voorwaarden voldoen. Op grond hiervan kan worden bepaald welke gegevens mogen worden verzameld. De verzamelde gegevens mogen vervolgens slechts worden verwerkt indien zij voldoen aan een van de gerechtvaardigde grondslagen.[143]

§ 4.3.1 Het doel van de verwerking

Payper verwerkt al langere tijd persoonsgegevens. Payper heeft vooralsnog geen doel omschreven of vastgelegd waarop de verzameling van gegevens kan worden gebaseerd. Het is belangrijk om een specifiek doel uitdrukkelijk te omschrijven.[144] Op basis van dit doel kan worden bepaald welke gegevens mogen worden verzameld. Tevens kan er middels een omschreven doel geen onduidelijkheid meer ontstaan over de rechtmatigheid van de gegevensverwerking.

Uit de vragenlijsten blijkt dat de medewerkers gegevens verzamelen op basis van specifieke doelen. Zij geven aan dat zij gegevens verkrijgen en verwerken ten behoeve van:

- het werven en selecteren van mensen;
- de dossieropbouw;
- salesactiviteiten (offerte uitbrengen);
- registreren en begeleiden van verzuim en salarisverwerking.[145]

Indien de gegevens noodzakelijk zijn om het doel te bereiken, mogen die gegevens worden verzameld. Er mogen niet meer gegevens worden verzameld dan noodzakelijk is. De ondervraagde medewerkers geven allemaal aan dat de gegevens die zij verwerken noodzakelijk zijn voor het uitoefenen van hun functie. Zo zijn NAW en geboortedatum bijvoorbeeld noodzakelijk voor het opstellen van overeenkomsten. Daarnaast geven zij aan dat zij de gegevens uitsluitend voor deze doelen verwerken.

Op basis van de resultaten uit de vragenlijsten kan worden gesteld dat de verzamelde gegevens rechtmatig zijn op grond van de gewenste doelen.[146]

§ 4.3.2 De grondslagen van de verwerking

Nadat de gegevens zijn verzameld, worden deze gegevens binnen Payper verwerkt. Elke wijze van verwerking, bijvoorbeeld het verstrekken aan derden, het vastleggen van gegevens of het vernietigen van gegevens moet vervolgens kunnen worden gebaseerd op een van de grondslagen uit artikel 8 Wbp.[147] Alleen dan is de verwerking gerechtvaardigd. De ondervraagde medewerkers hebben aangegeven dat zij onder andere gegevens opslaan in Salesforce en Flexservice. Opslaan is een vorm van verwerken. Deze verwerking moet kunnen steunen op een gerechtvaardigde grondslag.

[142] Art. 7 Wbp
[143] Art. 8 Wbp
[144] Bijlage IV
[145] Bijlage II
[146] Bijlage IV
[147] Art. 8 sub a t/m f Wbp

De medewerkers geven verschillende gronden aan voor de gegevensverwerking.[148] De drie gronden die worden genoemd zijn:

- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst;[149]
- De verwerking is noodzakelijk om wettelijke verplichting na te komen;[150]
- De verwerking is noodzakelijk voor behartiging van gerechtvaardigde belang van de verantwoordelijke.[151]

Veel van de gegevens die worden verwerkt zijn noodzakelijk voor de uitvoering van een overeenkomst. Indien Payper een arbeidsovereenkomst heeft met een werknemer, zal Payper tevens de salarisverwerking van deze werknemer verrichten. Voor het verwerken van het salaris heeft Payper gegevens van de werknemer nodig zoals onder andere een naam en een bankrekeningnummer.

De verwerking die noodzakelijk is om een wettelijke verplichting na te komen komt vooral voor bij de verzuimspecialiste. Zij verwerkt gegevens rondom de gezondheid van werknemers. Deze gegevens worden vaak doorgegeven aan het Uitvoeringsinstituut Werknemersverzekeringen (hierna: UWV) en de arbodienst. De wettelijke verplichtingen komen onder andere voort uit de ziektewet of de Wet Verbeterde Poortwachter.

Tot slot hebben een aantal van de medewerkers aangegeven gegevens te verwerken op basis van een gerechtvaardigd belang. Uit de resultaten van de vragenlijsten kan niet worden geconcludeerd of er in deze gevallen inderdaad sprake is van een gerechtvaardigd belang.

§ 4.3.3 Interne en externe uitwisseling

De gegevens worden intern uitgewisseld tussen collega's en verschillende afdelingen. Daarnaast worden de gegevens vastgelegd in Flexservice en/of Salesforce. Iedere medewerker die in het bezit is van inloggegevens heeft toegang tot deze programma's en heeft beschikking tot alle gegevens. Gegevens worden door een klein deel van de ondervraagde verstrekt aan derden. Door deze medewerkers is aangegeven dat de gegevens onder andere worden verstrekt aan het UWV, de arbodienst, intermediairs en opdrachtgevers.

Het verstrekken van gegevens is rechtmatig zolang dit overeenstemt met alle eisen die de Wbp stelt aan het verwerken van persoonsgegevens. Ook hier moet dus worden gelet op het gestelde doel van de organisatie en of de verwerking gebaseerd kan worden op een van de grondslagen.

Gegevens worden rechtmatig verstrekt aan het UWV, de arbodienst en aan de belastingdienst op grond van wettelijke verplichtingen.

Bijvoorbeeld

Een opdrachtgever/intermediair vraagt naar een naar de kopie van een ID kaart of paspoort van een werkgever voor zijn dossieropbouw. Dergelijke gegevens zijn door Payper niet verzameld om aan derden te verstrekken. Deze gegevens zijn verkregen om te voldoen aan de arbeidsovereenkomst en om het salaris van de betreffende medewerker te kunnen verwerken. Het sluit derhalve niet aan bij het doel van Payper om dergelijke gegevens aan derden te verstrekken. Daarnaast kan deze verwerking niet worden gebaseerd op een van de gerechtvaardigde grondslagen, tenzij de betrokkene ondubbelzinnig toestemming geeft

[148] Bijlage II
[149] Art. 8 Wbp
[150] Art. 8 Wbp
[151] Art. 8 Wbp

voor de verstrekking. In dit geval zou Payper deze gegevens dus niet aan een opdrachtgever of intermediair mogen verstrekken.

§ 4.4 Bijzondere persoonsgegevens

De helft van de medewerkers heeft aangegeven niet op de hoogte te zijn van het verschil tussen algemene en bijzondere persoonsgegevens. Het is dus mogelijk dat medewerkers bijzondere gegevens verwerken zonder dat zij kennis hebben van de speciale regels die hieraan zijn verbonden. In de Wbp staat opgesomd welke gegevens onder de bijzonder gegevens behoren. Het is van belang om bewust te zijn van het verschil tussen algemene en bijzondere gegevens omdat deze op andere manieren verwerkt moeten worden volgens de wet. Bijzondere gegevens mogen slechts op bepaalde gronden worden verwerkt. Verder moeten zij voldoen aan alle eisen van de algemene gegevens.

Binnen Payper is er een verzuimspecialiste werkzaam. De verzuimspecialiste heeft als enige werknemer aangegeven bijzondere persoonsgegevens te verwerken. Zij heeft te maken met de ziekmeldingen van werknemers en behandelt deze. Tevens spreekt zij bedrijfsartsen. Om de ziektemeldingen in te vullen wordt er gebruik gemaakt van gegevens die met de gezondheid te maken hebben. Als bijzondere persoonsgegevens worden binnen Payper dan ook alleen gegevens op basis van de gezondheid verwerkt. In de Wbp is bepaald dat dit alleen is toegestaan indien dit onder een bijzonder of specifieke uitzondering valt.

Gegevens over de gezondheid mogen door de verzuimspecialiste worden verwerkt op grond van een uitzondering in de Wbp.[152] Zij is gehouden aan een geheimhoudingsplicht en is de enige die deze gegevens mag inzien.[153]

De ziekmelding van de werknemer en zijn BSN worden verstrekt aan het UWV en aan de Arbodienst. Het BSN is een uniek kenmerk van de werknemer wat bij beide partijen nodig is voor de dossieropbouw. Het verstrekken van deze gegevens is toegestaan op basis van een wettelijke verplichting.

§ 4.5 Beveiliging

De beveiliging en bewaring van persoonsgegevens is van groot belang. In de vragenlijst zijn dan ook enkele vragen omtrent deze onderwerpen gesteld. Een fatsoenlijke beveiliging van de gegevens is een groot aspect voor het verantwoord omgaan met persoonsgegevens. In de praktijk blijkt echter dat er vaak tekort wordt geschoten ten aanzien van de beveiligingsmaatregelen. De Autoriteit Persoonsgegevens ontvangt hier dan ook regelmatig signalen over. De beveiliging die wordt getroffen ter bescherming van persoonsgegevens, is een van de hoofdpunten in het handhavingsbeleid van de Autoriteit Persoonsgegevens.[154]

Iedere medewerker heeft een computersysteem met een eigen gekozen wachtwoord. Dit is een standaardinstelling, die noodzakelijk is om Windows op te starten. Voor Salesforce en Flexservice zijn aparte inlogcodes vereist. De medewerkers dienen zich eerst in te loggen op het algemene netwerk, voordat zij zich kunnen inloggen in Flexservice of Salesforce.

Niet alle medewerkers vergrendelen hun computer wanneer ze tijdelijk niet bij hun werkplek aanwezig zijn. Wanneer deze medewerkers hun werkplaats verlaten en hun computer niet vergrendelen, kunnen onbevoegde mensen eenvoudig kennisnemen van de privacygevoelige informatie in. Om te voorkomen dat medewerkers vergeten hun computer te vergrendelen, is het mogelijk centraal een automatische vergrendeling in te stellen wanneer de computer een bepaalde tijd niet gebruikt wordt. Medewerkers kunnen ook zelf de automatische vergrendeling instellen. Door het vergrendelen dient de medewerker

[152] Art. 21 lid 1 sub f Wbp

[153] Art. 21 lid 2 Wbp

[154] Richtlijnen beveiliging 2013, p.2.

opnieuw zijn gebruikersnaam en wachtwoord in te voeren alvorens toegang te krijgen tot de computer. Voor Salesforce en Flexservice zijn aparte inlogcodes vereist. Medewerkers worden niet automatisch uitgelogd uit deze systemen. Medewerkers zullen dus ook rekening moeten houden met het correct afsluiten van deze programma's.

Er is geen sprake van autorisatie. De medewerkers gaven aan dat iedere collega met inloggegevens toegang heeft tot Salesforce en Flexservice. Dit betekent dat iedere medewerker toegang heeft tot alle verwerkte gegevens die in het systeem staan, ook tot gegevens die niet noodzakelijk zijn voor hun functie.

De gegevens worden in het systeem geplaatst en gebruikt. Wanneer de gegevens niet meer relevant zijn wordt er geen aandacht meer aan besteed. Er zullen dus veel verouderde, onjuiste en onvolledige gegevens in het systeem staan.

Payper is gevestigd op de vijfde verdieping van het kantoorgebouw. Het gebouw en de verdieping gaan beide apart op slot. Deze maatregelen zorgen voor een basisbeveiliging. Tot slot hanteer Payper een clean-desk methode. Dit betekent dat aan het eind van de dag geen belangrijke papieren of dossiers meer op het bureau liggen. In de praktijk is gebleken dat niet iedere medewerker zich aan deze methode houdt.

Medewerkers zijn zich onvoldoende bewust van de veiligheidsrisico's van dergelijk nalatig gedrag Doordat medewerkers de risico's van dergelijk gedrag onderschatten, ontstaat een direct gevaar voor de privacy van de betrokkenen. Daarom dient de organisatie zorg te dragen voor een optimaal beveiligingsniveau, dat minimaal voldoet aan art. 13 Wbp. Tevens mag van de medewerkers worden verwacht dat zij alles in het werk stellen om misbruik te voorkomen. Op basis van het goed werkgeverschap is Payper verplicht zorg te dragen voor een goede beveiliging van de persoonsgegevens. Op basis van het bovenstaande wordt vastgesteld dat Payper voor een groot deel niet aan de beveiligingsverplichting voldoet.

§ 4.6 Bewaartermijn
Binnen Payper is er geen enkele informatie verschaft over de bewaartermijn. Gegevens worden op dit moment oneindig bewaart.

In de vragenlijst is gevraagd op welke manier medewerkers gegevens verwerken. De wijze van verwerken die het meest voorkwamen zijn:

- Verzamelen
- Ordenen
- Opvragen
- Verspreiden
- Wijzigen
- Verstrekken aan derden
- Vastleggen
- Bijwerken
- Gebruiken
- Bewaren/archiveren
- Raadplegen
- Met elkaar in verband brengen

Hier valt op dat geen van de medewerkers heeft aangegeven gegevens te wissen, af te schermen of te vernietigen. Dit zou betekenen dat de gegevens voor altijd in het systeem blijven staan en dat niemand let op de bewaartermijn. Hierdoor kan Payper groot risico lopen. Het bewaren van gegevens die niet meer noodzakelijk zijn voor het doel moeten worden vernietigd. De bewaartermijn voldoet niet aan de eisen van de Wbp.

§ 4.7 De verplichtingen van de verantwoordelijke
Zoals in paragraaf 2.7 is aangegeven rusten er een aantal verplichtingen op de verantwoordelijke.

Geheimhoudingsplicht
De afdeling Legal beschikt over een geheimhoudingsplicht. De overige medewerkers geven aan dat zij niet geïnformeerd zijn over het geheimhouden van gegevens en niet beschikken over een geheimhoudingsverklaring.

Melding en voorafgaand onderzoek
Voorafgaand aan het verkrijgen van persoonsgegevens dient de verantwoordelijke dit te melden aan de Autoriteit Persoonsgegevens. Payper heeft vooralsnog geen melding gemaakt van de gegevensverwerking aan de Autoriteit Persoonsgegevens. Een melding is niet altijd verplicht. Payper moet zelf beoordelen of zij de gegevensverwerking aan de Autoriteit Persoonsgegevens moet melden. Aan de hand van een stappenplan die de Autoriteit Persoonsgegevens heeft opgesteld kan worden bepaald of een melding nodig is. Payper kan een melding doen via het meldingsformulier van de Autoriteit Persoonsgegevens die tevens in bijlage VI is toegevoegd. Alle verwerkingen dienen apart te worden gemeld. Payper heeft geen FG aanstelt en zal dus zelf de verwerking dienen te melden. De verstrekking van gegevens aan de belastingdienst en het UWV is vrijgesteld van de melding.
Payper dient zo snel mogelijk een melding te maken van de gegevensverwerking. Het niet nakomen van deze verplichting kan namelijk leiden tot een boete.

Indien de gegevensverwerking specifieke risico's met zich meebrengt wordt er een voorafgaand onderzoek ingesteld door de Autoriteit Persoonsgegevens. De specifieke risico's bestaan voornamelijk uit drie aspecten.

- Indien een BSN, voor een ander doel dan waarvoor dit is bestemd, wordt verwerkt dient er een voorafgaand onderzoek plaats te vinden. De medewerkers hebben aangegeven alleen het BSN te verwerken om te raadplegen en gegevens door te kunnen geven aan het UWV en de Arbodienst. Dit is in overeenstemming met het doel.
- Indien de verantwoordelijke gegevens wil vastleggen op grond van het gericht verzamelen van informatie door middel van een eigen onderzoek zonder dat de betrokkene hiervan op de hoogte wordt gesteld dient er een voorafgaand onderzoek plaats te vinden. Dit is niet van toepassing binnen Payper.
- Indien strafrechtelijke gegevens ten behoeve van derden worden verwerkt dient er een voorafgaand onderzoek plaats te vinden. Dit is op Payper niet van toepassing.

Uit de resultaten blijkt dat er bij Payper geen voorafgaand onderzoek nodig zal zijn.

Informatieplicht
De betrokkene dient op de hoogte te worden gebracht van de gegevensverwerking. De ondervraagde medewerkers gaven aan betrokkenen niet op de hoogte te houden van de gegevensverwerking. Slechts één medewerker gaf aan de betrokkene op de hoogte te stellen indien gegevens aan derden worden doorgegeven. Het moment waarop de betrokkene geïnformeerd dient te worden hangt samen met de vraag van wie de medewerker de gegevens heeft verkregen. De gegevens worden vaak verkregen van de betrokkene zelf. Voorafgaand aan deze verkrijging dient de verantwoordelijke de betrokkene op de hoogte te stellen. Gegevens worden tevens verkregen van intermediairs, opdrachtgevers en andere afdelingen binnen Payper. De verantwoordelijke zou bij deze verkrijging de betrokkene op de hoogte moeten stellen op het moment van vastlegging van de gegevens of wanneer de gegevens aan een derde worden verstrekt.
Uit de resultaten van de vragenlijsten blijkt dat er op dit punt niet wordt voldaan aan de informatieplicht en de wettelijke regels die hierbij horen.

Meldplicht datalekken
Payper heeft geen werkwijze opgesteld over de handelingen die moeten gebeuren indien er sprake is van een datalek. Het is belangrijk om een dergelijk regelement op te stellen zodat er op het moment van een datalek direct gehandeld kan worden om de schade zo ver mogelijk te beperken.

§ 4.8 De rechten van betrokkenen
De betrokkene heeft het recht om kennis te vernemen over de gegevensverwerking zodat hij hier een grip op kan houden of krijgen. De betrokkene is bevoegd om zijn verwerkte gegevens in te zien. Op grond hiervan kan hij verzoeken om de gegevens bijvoorbeeld te laten aanpassen of te laten verwijderen. Het is hiervoor wederom belangrijk dat de gegevens van de betrokkene volledig, correct en relevant zijn voor Payper. Medewerkers hebben weinig kennis van de rechten van betrokkenen.

§ 4.9 Het rechtmatigheidsbeginsel
Zoals in hoofdstuk 2 en artikel 6 Wbp is benoemd, dient de gehele gegevensverwerking te voldoen aan het rechtmatigheidsbeginsel. Payper voldoet hier niet aan. De gegevensverwerking binnen Payper gebeurt niet conform alle eisen die de Wbp hieraan stelt. Dit wil zeggen dat er niet op een behoorlijke en zorgvuldige manier met de gegevens wordt omgegaan. De gegevens worden op onrechtmatige wijze verwerkt. Er is nog geen doel vastgesteld door Payper en er wordt weinig aandacht besteed aan de gehele gegevensverwerking. Controle of de verwerking gerechtvaardigd is ontbreekt binnen het bedrijf. De gegevens worden niet op de juiste manier beveiligd waardoor Payper een groter risico loopt op datalekken. Daarnaast is er geen (duidelijke) bewaartermijn vastgelegd waardoor gegevens oneindig in de systemen blijven staan. Er wordt geen rekening gehouden met de informatieplicht en de rechten van de betrokkenen. Slechts een enkele medewerker heeft een geheimhoudingsverklaring ondertekend. Daarnaast hebben de meeste medewerkers geen besef van de privacywetgeving en de gevolgen die eraan vast zitten.

§ 4.10 Het belang van een privacyreglement
Aan de medewerkers is gevraagd of zij een privacyreglement binnen Payper noodzakelijk vinden. Alle medewerkers hebben geantwoord dat zij een dergelijk reglement van belang vinden voor henzelf of voor collega’s. Op basis van de resultaten van het onderzoek is er een reglement opgesteld. Dit kan Payper helpen bij het waarborgen van de privacy binnen de organisatie. Tevens stelt dit medewerkers op de hoogte van de wijze waarop zij gegevens mogen verwerken. Het privacyreglement is opgenomen in bijlage V.

Conclusie

Naar aanleiding van het onderzoek kunnen diverse conclusies worden getrokken. De conclusies zijn van belang voor het privacyreglement dat voor Payper wordt opgesteld. De conclusies komen voort uit een vergelijking tussen de eisen van de Wbp en het onderzoek naar de wijze waarop Payper gegevens verwerkt. Door middel van de ingevulde vragenlijsten is er veel duidelijkheid verkregen.

In de conclusie wordt antwoord gegeven op de centrale vraag: Op welke manier dient Payper persoonsgegevens te verwerken, zodat zij voldoet aan de eisen die de Wet bescherming persoonsgegevens hieraan stelt, mede gelet op de meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheden Autoriteit Persoonsgegevens?

De belangrijkste conclusie die naar voren is gekomen, is dat Payper in haar huidige vorm niet voldoet aan de eisen van de Wbp. De medewerkers hebben niet genoeg besef van de geldende wetgeving rondom de gegevensverwerking. Dit leeft samen met het feit dat er binnen Payper nog weinig aandacht is besteed aan de privacy.

Rechtmatigheidsbeginsel
Payper voldoet op allerlei vlakken niet aan de wetgeving die er rondom de gegevensverwerking is gesteld. Dit betekent dat er op onbehoorlijke en onzorgvuldige wijze met de gegevens wordt omgegaan. De huidige wijze van verwerking binnen Payper voldoet niet aan het rechtmatigheidsbeginsel en de gehele verwerking van persoonsgegevens kan op dit moment dan ook onrechtmatig worden genoemd.

Zoals in hoofdstuk 2 is beschreven bevat de Wbp bepalingen waaraan de gegevensverwerking moet voldoen. Een organisatie mag niet zomaar persoonsgegevens van personen of organisaties verwerken. Als eerst dient de verwerking te voldoen aan de algemene beginselen van gegevensverwerking. Vervolgens dient elke aparte verwerking gebaseerd te kunnen worden op een van de grondslagen die voortvloeien uit artikel 8 Wbp.

Doelbinding
Het uitgangspunt van elke verwerking is een welbepalend, uitdrukkelijk omschreven doel. Op grond van dit doel kan worden bepaald welke gegevens de verantwoordelijke mag verzamelen, wat er vervolgens met deze gegevens mag gebeuren en aan wie de gegevens mogen worden verstrekt. Iedere gegevensverwerking moet zijn grondslag kunnen vinden in dit vastgestelde doel.
Uit de vragenlijsten is gebleken dat het gewenste doel van Payper het gegevens verwerken ten behoeve van het werven en selecteren van mensen en salarisverwerking is. De gegevens moeten noodzakelijk zijn om het doel te behalen, mogen niet onverenigbaar zijn met het doel en dienen in verhouding te staan met de inbreuk op privacy van de betrokkene. Uit het onderzoek is gebleken dat de gegevens die Payper verkrijgt in overeenstemming zijn met het gestelde doel van de organisatie. Er wordt door Payper dus voldaan aan het algemene beginsel van doelbinding.

Gerechtvaardigde grondslagen
De verwerking van de gegevens dient vervolgens gebaseerd te kunnen worden op een van de grondslagen uit artikel 8 Wbp. Payper mag gegevens verwerken indien elke verwerking een gerechtvaardigde grondslag heeft. De medewerkers hebben drie grondslagen aangegeven waarop zij gegevens verwerken. Deze gronden zijn gerechtvaardigd conform artikel 8 Wbp. Payper moet erop blijven letten dat iedere verwerking op een van de gerechtvaardigde gronden kan worden gebaseerd.

Interne en externe verstrekking
De gegevensstromen binnen Payper heeft een grote omvang. Gegevens worden zowel intern als extern verkregen en verstrekt. De uitwisseling bestaat vooral tussen werknemers, opdrachtgevers, intermediairs en andere afdelingen binnen Payper. Gegevens verstrekken binnen de afdeling is toegestaan zolang iedere collega bevoegd is om kennis te nemen van de betreffende gegevens.
Naar aanleiding van het onderzoek kan worden geconcludeerd dat de gegevens verstrekt mogen worden aan externe instellingen zoals het UWV, de Arbodienst en de belastingdienst. Andere gegevensverstrekking aan derden zal per geval onderzocht moeten worden. Hierbij dient Payper wederom te controleren of de verwerking noodzakelijk is op grond van het doel en of de verwerking voldoet aan een gerechtvaardigde grondslag. De overige algemene beginselen van gegevensverwerking dienen tevens in acht te worden genomen.

Gezondheidsgegevens
De gegevens ten aanzien van de gezondheid van een medewerker mogen door de verzuimspecialist worden verwerkt. De verwerking vindt haar grondslag in het doel van Payper. Daarnaast is de verwerking gerechtvaardigd op grond van artikel 8 sub f Wbp. De verzuimspecialist heeft op dit moment nog geen geheimhoudingsverklaring ondertekend. Daarnaast zijn de gegevens die noodzakelijk zijn voor haar functie ook toegankelijk voor andere medewerkers die deze gegevens niet nodig hebben. Een vereiste voor de verwerking van gegevens omtrent de gezondheid van een werknemer is dat de verzuimspecialist zo snel mogelijk een geheimhoudingsverklaring ondertekend en dat de gegevens alleen voor haar beschikbaar zijn.

Beveiliging
Het waarborgen van de veiligheid van de persoonsgegevens is een groot aspect voor de verwezenlijking van de zorgvuldigheideis. De verantwoordelijke dient zorg te dragen voor passende technische en organisatorische maatregelen om persoonsgegevens tegen verlies of enige vorm van onrechtmatige verwerking te beveiligen. Op een aantal aspecten worden de gegevens binnen Payper beveiligd. Zo heeft iedere medewerker een eigen wachtwoord voor zijn computer en inlogcodes voor de systemen waarin gegevensverwerking plaatsvindt. De verdieping en het gebouw worden beide apart afgesloten en Payper hanteert een clean-desk methode. Daarentegen is er geen sprake van autorisatie van medewerkers voor specifieke gegevens. Iedere medewerker heeft beschikking tot de gegevens. Tevens worden er geen handelingen getroffen omtrent de verouderde gegevens. Computers worden niet (automatisch) vergrendeld en medewerkers besteden te weinig aandacht aan het vergrendelen van hun computer wanneer zij hun werkplek verlaten. Uit deze gegevens resulteert dat er op allerlei vlakken onvoldoende beschermingsmaatregelen zijn getroffen. De medewerkers zijn daarnaast onvoldoende op de hoogte van de mogelijke gevolgen. Payper is verantwoordelijk om zorg te dragen voor passende technische en organisatorische maatregelen om gegevens te beveiligen. Op dit moment voldoet Payper niet aan deze verplichting.

Bewaartermijn
Zoals hierboven ook al aangegeven wordt er niet omgekeken naar verouderde gegevens. Dit is niet alleen van belang voor de beveiliging, maar dit betekent ook dat er niet wordt voldaan aan de toegestane bewaartermijn van persoonsgegevens. De Wbp stelt dat gegevens mogen worden bewaard voor de tijd waarop de gegevens noodzakelijk zijn. Indien de gegeven niet meer nodig zijn om het doel te bereiken dienen de gegevens te worden vernietigd. Uit de vragenlijsten blijkt dat geen een medewerker op de hoogte is gebracht van een bewaartermijn. De gegevens worden niet vernietigd of uitgewist maar blijven oneindig in de systemen staan. Veel van deze gegevens zijn niet meer relevant voor het bedrijf en zouden dus vernietigd moeten worden. Op dit aspect voldoet Payper dus niet aan de eisen die de Wbp stelt.

Geheimhoudingsplicht
Op een enkeling na beschikken de medewerkers niet over een geheimhoudingsverklaring. Vooral bij sommige afdelingen, zoals de werknemers van de afdeling verzuim, is dit van groot belang.

Melding en voorafgaand onderzoek
Payper heeft reeds nog geen gegevensverwerking gemeld bij de Autorisatie Persoonsgegevens. Het is van belang om deze melding zo snel mogelijk te doen omdat Payper anders risico loopt op een boete vanuit de Autorisatie Persoonsgegevens. Een voorafgaand onderzoek is bij Payper niet nodig omdat de gegevensverwerking geen specifieke risico's met zich meebrengen.

Informatieplicht
Betrokkenen dienen op de hoogte te worden gehouden van de gegevensverwerking. De medewerkers van Payper hebben te weinig kennis over de rechten van betrokkenen. Betrokkenen worden dan ook niet op de hoogte gehouden van de gegevensverwerking binnen Payper. Slechts één medewerkers deelt aan betrokkene mede wanneer hun gegevens aan een derde worden verstrekt.

Naar aanleiding van de conclusies blijkt dat Payper nog een lange weg heeft te gaan om de gegevensverwerking op een juiste manier, conform de Wbp te laten verlopen. Intern dienen er nogal wat instructies te worden gegeven en Payper zal meer aandacht aan de privacywetgeving moeten besteden.

Aanbevelingen

Uit de conclusie is gebleken dat Payper op verschillende aspecten van de gegevensverwerking niet voldoet aan de wettelijke regels die uit de Wbp voortvloeien. Op basis van deze aspecten worden er aanbevelingen aan Payper gegeven hoe zij dit kunnen aanpassen tot een wijze die wel aan de wet voldoet.

Bewustwording
Uit het onderzoek is gebleken dat de medewerkers van Payper te weinig kennis hebben van de wettelijke regels omtrent gegevensverwerking. Slechts enkele medewerkers zijn op de hoogte van de wettelijke verplichtingen. De eerste aanbeveling aan Payper is dan ook het bewust maken van de medewerkers en de kennis rondom het privacyrecht te vergroten. Wanneer de medewerkers kennis over het onderwerp vergaren en de gevolgen kennen zullen zij ook veel oplettender worden. De bescherming van persoonsgegevens is voor iedereen van belang, welke functie hij ook uitoefent.

Medewerkers dienen voorgelicht te worden over het privacyrecht, over de wettelijke bepalingen waaraan de verwerking moet voldoen en over de gevolgen wanneer de wet niet wordt nageleefd. Hierbij kan gedacht worden aan een informatiebijeenkomst met een presentatie. Dit zou een taak kunnen zijn voor de Legal Counsel omdat hij het meeste kennis van de wettelijke bepalingen heeft en deze aan de andere medewerkers kan uitleggen. Daarnaast is het handig als de medewerkers een handleiding meekrijgen die zij later nog kunnen raadplegen. In de bijlage is een privacyreglement opgenomen die als basis voor de handleiding kan dienen.
Voor nieuwe medewerkers is het handig om de belangrijkste regels rondom gegevensverwerking toe te voegen in het introductieproces. Medewerkers dienen direct op de hoogte worden gebracht zodat ook zij de gewenste werkwijze kunnen hanteren. Tevens dienen zijn een handleiding te krijgen.

In de voorlichting dient in ieder geval aan de orde te komen:

- Aan welke voorwaarden de verzameling en de verwerking van gegevens moet voldoen. De medewerkers horen te weten wat het doel van de organisatie is en aan welke overige algemene beginselen de verwerking dient te voldoen. De medewerkers kunnen dan in de toekomst zelf oordelen of bepaalde gegevens mogen worden verzameld op grond van dit doel, en of deze gegevens relevant zijn. Daarnaast dienen zij geïnformeerd te worden over de gerechtvaardigde grondslagen en de verplichting dat de verwerking gebaseerd moet kunnen worden op een van deze grondslagen.
- De eisen die worden gesteld aan de beveiliging, de bewaartermijn en de informatieverplichting aan betrokkenen.

De informatie die aan de medewerkers wordt verschaft moet eenduidig zijn zodat iedere medewerker op dezelfde wijze handelt. Als er wordt geïnvesteerd in het vergroten van de kennis van de medewerkers zal dit in de toekomst veel voordeel opleveren. De medewerkers kunnen dan voortaan zelf afwegingen maken over onder andere bepaalde gegevensverwerkingen, het verstrekken van gegevens aan derden en het inlichten van betrokkenen.

Het doel voor de gegevensverwerking
Binnen Payper zal er goed moeten worden nagedacht over het doel wat zij willen omschrijven voor het verwerken van persoonsgegevens. Iedere verwerking dient zijn grondslag te kunnen vinden in dit doel. Wanneer het doel is vastgelegd kan dit niet meer worden veranderd. Het huidige doel van Payper is het verwerken van gegevens ten behoeve van het werven en selecteren van mensen en salarisverwerking. Dit doel is erg eenduidig en dient misschien uitgebreider te worden. Payper kan een overzicht maken van de gegevens

die noodzakelijk zijn voor Payper en welke gegevens de medewerkers nodig hebben om hun functie te kunnen uitoefenen. Op basis hiervan kan Payper een goed doel formuleren waar iedere verwerking op gebaseerd kan worden.

Beveiliging
De rechtmatigheid en zorgvuldigheid van gegevensverwerking valt of staat met de mate waarop de gegevens zijn beveiligd. Gebleken is dat Payper niet geheel aan de beveiligingsverplichting voldoet. De Autoriteit Persoonsgegevens heeft richtlijnen opgesteld omtrent de beveiliging van persoonsgegevens. Op basis van die richtlijnen is het Payper aan te bevelen om een 'plan-do-check-act' cyclus op te stellen en te hanteren. Met deze cyclus is Payper in staat om tot een blijvend, passend beveiligingsniveau te komen.

De plan-do-act-check cyclus
1. Betrouwbaarheidseisen onderzoeken

De betrouwbaarheidseisen zijn onder te verdelen in drie aspecten van beveiliging. Dit zijn de beschikbaarheid, integriteit en de vertrouwelijkheid. Deze aspecten betreffen het waarborgen van de gegevens door middel van juistheid en volledigheid van de gegevens en het toezicht op de toegankelijkheid van informatie voor degene die hiertoe zijn geautoriseerd. Kortom, de gegevens dienen volledig en correct te zijn en alleen medewerkers die bevoegd zijn tot de gegevens dienen hier toegang tot te krijgen.

2. Passende maatregelen treffen

- Een risicoanalyse

Middels een risicoanalyse kan Payper onderzoeken welke risico's de verwerking met zich meebrengt. De risicoanalyse kan Payper zelf uitvoeren. De dreigingen die kunnen leiden tot een beveiligingsincident dienen te worden geïnventariseerd. Bij verwerking via het internet is hacken bijvoorbeeld een dreiging waar rekening mee moet worden gehouden. Hiernaast bestaat de kans op diefstal van bijvoorbeeld draagbare laptops of geheugenmedia. Vervolgens dient Payper te onderzoeken welke gevolgen dit incident kan hebben en hoe groot de kans is dat deze gevolgen zich daadwerkelijk voordoen. Indien er persoonsgegevens van een werknemer worden gestolen zou dit bijvoorbeeld kunnen leiden tot identiteitsfraude. Al deze bedreigingen en gevolgen worden in de risicoanalyse opgenomen.
Naar aanleiding van de risicoanalyse kunnen verschillende maatregelen worden getroffen.

- Preventieve maatregelen: het voorkomen van een beveiligingsincident door de juiste maatregelen te treffen zoals hieronder bij 'toepassen beveiligingsmaatregelen' is beschreven.
- Detectieve maatregelen: indien een beveiligingsincident heeft plaatsgevonden dient Payper hier zo snel mogelijk van op de hoogte te zijn zodat zij de gevolgen op tijd kunnen beperken.
- Repressieve maatregelen: het beperken van de negatieve gevolgen van het beveiligingsincident.
- Herstelmaatregelen: het verhelpen van de negatieve gevolgen zoals een schadevergoeding vaststellen voor betrokkenen.
- Correctieve maatregelen: het repareren van de gebleken tekortkomingen. De beveiligingsmaatregelen dienen dus te worden aangepast.

- Toepassen beveiligingsmaatregelen

- De beveiliging dient technisch in orde te zijn. Hierbij valt te denken aan firewalls. Daarnaast kan Payper instellen dat iedereen eens in de 3 maanden een melding krijgt om zijn wachtwoord te wijzigen.
- Medewerkers dienen hun computer te vergrendelen wanneer zij hun werkplek verlaten. Tevens kan ingesteld worden dat de computer automatisch na enkele minuten wordt vergrendeld.
- Medewerkers moeten worden gewezen op het belang van de clean-desk methode.

- Het risico op datalekken moet zo veel mogelijk worden beperkt. Er kan bijvoorbeeld worden afgesproken dat privé laptops niet zijn toegestaan, er geen USB-sticks worden gebruikt en er geen belangrijke gegevens via privé-mailadressen worden verzonden.
- Iedere medewerker dient zijn computer en de programma's op juiste manier af te sluiten.

3. Controleren

Payper dient te controleren of de beveiligingsmaatregelen daadwerkelijk zijn getroffen en of ze correct werken. Dit kan een taak zijn die de ICT-afdeling op zich neemt. Zij kunnen bijvoorbeeld beoordelen of de firewalls op de juiste manier werken en of alle technische maatregelen zijn getroffen. Daarnaast is het van belang dat de medewerkers zelf blijven letten op de beveiligingsmaatregelen zoals het vergrendelen van computers en het tijdig wijzigen van wachtwoorden.

4. Evalueren en eventueel aanpassen

Vervolgens is het belangrijk om ieder halfjaar te evalueren of de beveiliging nog optimaal werkt. Houdt hierbij rekening met de stand van de techniek. Zo kunnen er waar nodig beveiligingsmaatregelen worden aangepast of aangescherpt en zijn de maatregelen altijd up-to-date. Binnen Payper kan er een of meerdere personen worden aanwijzen die dit in de gaten houden. Indien Payper dit nodig vindt zouden zij eventueel een deskundige kunnen inschakelen.

Tot slot is het aan te bevelen dat degene die verantwoordelijk is voor de beveiliging binnen Payper, de richtlijnen van de Autoriteit Persoonsgegevens doorleest zodat diegene op de hoogte is van de wijze waarop de Autoriteit Persoonsgegevens de beveiliging binnen een organisatie controleert. Indien de richtlijnen van de Autoriteit Persoonsgegevens worden gevolgd zorgt dit voor een optimale beveiliging.

Autorisatie

Zoals hierboven is aangegeven is het belangrijk om personen te autoriseren voor de toegang van bepaalde gegevens. Niet iedere medewerker verwerkt persoonsgegevens. Het is voor hen dan ook niet noodzakelijk om toegang te hebben tot deze gegevens. De medewerkers binnen Payper vervullen verschillende functies waar zij verschillende persoonsgegevens voor nodig hebben. Iemand van de afdeling sales zal andere gegeven nodig hebben dan iemand van de afdeling finance. Ook hier is het van belang dat medewerkers alleen bevoegd zijn tot toegang van de gegevens die voor het uitoefenen van hun functie noodzakelijk is. Tot slot zijn er bijzondere gegevensverwerkingen zoals de verwerking op basis van gezondheid. Hierbij moet extra aandacht worden besteed aan de autorisatie van de betreffende personen omdat op deze gegevens speciale voorwaarden van toepassing zijn. Het belang van de autorisatie is zodat er in de toekomst geen onduidelijkheden kunnen ontstaan over de relevantie van gegevens en bevoegdheden. Om de autorisatie te verwezenlijken zal Payper moeten onderzoeken of bepaalde rechten ook daadwerkelijk noodzakelijk zijn voor de uitoefening van de functie van deze medewerker en welke gegevens noodzakelijk zijn voor die medewerker.

Bewaartermijn

Zoals in de conclusie is beschreven wordt er binnen Payper geen aandacht besteedt aan de bewaartermijn. Verouderde gegevens moeten worden aangepast. Gegevens die niet meer noodzakelijk of relevant zijn dienen uit de systemen te worden gewist. De wettelijke verplichtingen omtrent het verwerken van gegevens dient Payper hierbij in aanmerking te nemen. Het vernietigen of uitwissen van gegevens valt onder het verwerken van gegevens. Payper dient hier aandacht aan te besteden en de verouderde gegevens uit de systemen te verwijderen.

Geheimhoudingsplicht
Geadviseerd wordt om alle huidige medewerkers binnen Payper die persoonsgegevens verwerken een geheimhoudingsverklaring te laten ondertekenen. Bij nieuwe medewerkers kan dit geschieden op het moment dat zij hun arbeidsovereenkomst ondertekenen.

Melding maken van de gegevensverwerking
Payper heeft nog geen enkele gegevensverwerking aangemeld bij de Autoriteit Persoonsgegevens. Dit kan leiden tot financiële gevolgen voor de organisatie. Hierdoor wordt Payper aanbevolen om op zeer korte termijn de informatie te verzamelen die nodig is voor de melding, het meldingsformulier in te vullen en op te sturen aan de Autoriteit Persoonsgegevens. Het meldformulier is te vinden in bijlage VI.

De FG
Payper kan overwegen om een FG binnen de organisatie aan te stellen. Gezien de omvang van de organisatie is dit echter niet noodzakelijk. Indien de organisatie uitbreidt kan er wellicht alsnog worden besloten om een FG aan te stellen. Payper zal hierbij zelf het beste kunnen beoordelen wanneer het voor hen voordeliger is om een FG aan te stellen.

Werkwijze datalekken opstellen
De Autoriteit Persoonsgegevens dient direct op de hoogte te worden gesteld indien er sprake is van een ernstig datalek binnen de organisatie. Dit houdt in dat Payper direct op de hoogte moet zijn indien er sprake is van een dergelijk incident. Een datalek hoeft niet altijd aan de Autoriteit Persoonsgegevens te worden gemeld. Payper wordt geadviseerd om een werkwijze op te stellen indien er sprake is van een datalek. Aan de hand van de werkwijze is het direct duidelijk hoe er moet worden gehandeld en wat er moet worden gemeld aan de Autoriteit Persoonsgegevens.

Privacyreglement implementeren
In de bijlage is een privacyreglement voor Payper opgesteld. Het reglement draagt bij aan de bewustwording en de kennis van de medewerkers. Daarnaast stelt het medewerkers binnen Payper op de hoogte van wat er van hun wordt verwacht met betrekking tot het verwerken van gegevens. Het reglement dient te worden geïntroduceerd aan iedere medewerker. Daarnaast is het belangrijk dat iedere medewerker het privacyreglement bij de hand heeft zodat zij hier altijd op terug kunnen vallen. Het reglement zal voor iedere medewerker binnen Payper toegankelijk moeten zijn bijvoorbeeld door het reglement in het systeem te plaatsen. Vervolgens dient Payper toezicht te houden op de naleving van het reglement. Payper dient ervoor te zorgen dat medewerkers niet terugvallen in hun oude gedrag.

Op grond van artikel 25 Wbp kan Payper de Autoriteit Persoonsgegevens verzoeken om te verklaren dat het reglement een juiste uitwerking vormt van de Wbp. Dit geeft Payper zekerheid en het verkleint de risico's op een sanctie enorm.

Controle
Tot slot is het belangrijk om de wijze van verwerking door medewerkers te blijven controleren. Payper wordt geadviseerd om elk halfjaar de huidige wijze van gegevensverwerking te evalueren. De evaluatie kan bijvoorbeeld geschieden door iedere medewerker elektronisch een vragenlijst te laten beantwoorden. Hierin kunnen onder andere de volgende vragen worden gesteld:

- Welke gegevens worden verwerkt;
- Door wie deze gegevens worden verwerkt
- Op grond van welk doel de gegevens worden verwerkt;
- Of elk gegeven relevant is voor het vervullen van zijn of haar functie;
- Welke gegevens aan derden worden verstrekt;
- Of betrokkenen worden geïnformeerd en op welke manier;
- En of medewerkers zich houden aan de juiste bewaartermijn van de gegevens.

Op basis van de evaluatie kan er een overzicht worden gemaakt. Hieruit zal blijken of de medewerkers de juiste kennis hebben en of zij gegevens op de juiste manier verwerken. Er kan dan eventueel nog een extra informatiebijeenkomst worden gehouden om de medewerkers op de hoogte te blijven houden van de wettelijke verplichtingen.

Literatuurlijst

Boeken

Hooghiemstra & Nouwt 2007
T.F.M. Hooghiemstra & J. Nouwt, *Tekst en toelichting Wet bescherming persoonsgegevens,* Den Haag: Sdu 2007.

Janssen 2012
L. Janssen, *Staats- en bestuursrecht bronnenboek,* Den Haag: Boom Juridische Uitgevers 2012.

Loonstra & Zondag 2015
C.J. Loonstra & W.A. Zondag, *Arbeidsrechtelijke themata,* Den Haag: Boom Juridische Uitgevers 2015.

Elektronische bronnen

'Beleidsregels, www.autoriteitpersoonsgegevens.nl (zoek op *zelf doen* > *beleidsregels*).

'Beveiliging van persoonsgegevens', www.autoriteitpersoonsgegevens.nl (zoek op *Wbp*).

'Gedragscodes, www.autoriteitpersoonsgegevens.nl (zoek op *zelf doen* > *gedragscodes*).

'Het werk van de Autoriteit Persoonsgegevens', www.autoriteitpersoonsgegevens.nl (zoek op *Over privacy*).

'Melden verwerken persoonsgegevens', www.autoriteitpersoonsgegevens.nl (zoek op *melden> verwerken persoonsgegevens*).

'Meldingsprogramma', www.autoriteitpersoonsgegevens.nl (zoek op *melden> meldingsprogramma*).

'Meldplicht datalekken', www.autoriteitpersoonsgegevens.nl (zoek op *melden*).

'Missie, visie, kernwaarden', www.autoriteitpersoonsgegevens.nl (zoek op *missie, visie, kernwaarden).*

'Naslag Wet bescherming persoonsgegevens' www.autoriteitpersoonsgegevens.nl (zoek op *wetten).*

'Persoonsgegevens, www.rijksoverheid.nl (zoek op *onderwerpen* > *persoonsgegevens*).

'Voorafgaand onderzoek', www.autoriteitpersoonsgegevens.nl (zoek op *melden* > *voorafgaand onderzoek*).

'Wat is Payroll?' www.payper.nl (zoek op *payroll*).

'Wet basisregistratie personen', www.autoriteitpersoonsgegevens.nl (zoek op *wetten).*

www.amnesty.nl (zoek op *UVRM*).

www.ngfg.nl (zoek op *home*).

Handleidingen en rapporten

Autoriteit Persoonsgegevens 2015
Autoriteit Persoonsgegevens, 'De meldplicht datalekker in de Wbp', Den Haag: 2015.

Sauerwein & Linnemann 2002
L.B. Sauerwein en J.J. Linnemann, 'Handleiding voor verwerkers van persoonsgegevens', (Ministerie van Justitie), Den Haag: 2002.

Autoriteit Persoonsgegevens 2016
Wbp-naslag (Autoriteit Persoonsgegevens.nl)

Beleidsregels meldplicht datalekken 2015
Autoriteit Persoonsgegevens

Richtsnoeren beveiliging 2013
Autoriteit Persoonsgegevens

Jurisprudentie

Rechtbank Maastricht 05 december 2003, ECLI:NL:RBMAA:2003:AO0044.
Hoge Raad 09 september 2011, ECLI:NL:HR:2011:BQ8097.
Centrale Raad van Beroep 15 februari 1995, ECLI: NL:CRVB:1995:ZB1348.
.

Parlementaire stukken

Kamerstukken I, 2014/15, 33662, nr. A (wetswijziging meldplicht datalekken)

kamerstukken II, 1997/98, 25892, 3 (MvT)

Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens

Tijdschriften

Verhey, *RegelMaat* 2015/30
L.F.M. Verhey, 'Verwerking persoonsgegevens', RegelMaat 2015.

Verhey en Raijmakers, *RegelMaat* 2013
L.F.M. Verhey & M.W. Raijmakers, 'Artikel 8 EVRM: proportionaliteit en verwerking van persoonsgegevens', RegelMaat 2013.

Rechtsbronnen

Algemene wet bestuursrecht
Boetebeleidsregels Autoriteit Persoonsgegevens 2016
Europees Verdrag van de Rechten van de Mens en de Fundamentele Vrijheden
Grondwet
Internationaal Verdrag inzake Burgerrechten en Politieke rechten
Internationaal Verdrag inzake economische culturele en sociale rechten
Universele verklaring van de Rechten van de Mens
Wet algemene bepalingen Burgerservicenummer
Wet bescherming persoonsgegevens

Wet persoonsregistratie
Wet verbetering poortwachter
Ziektewet