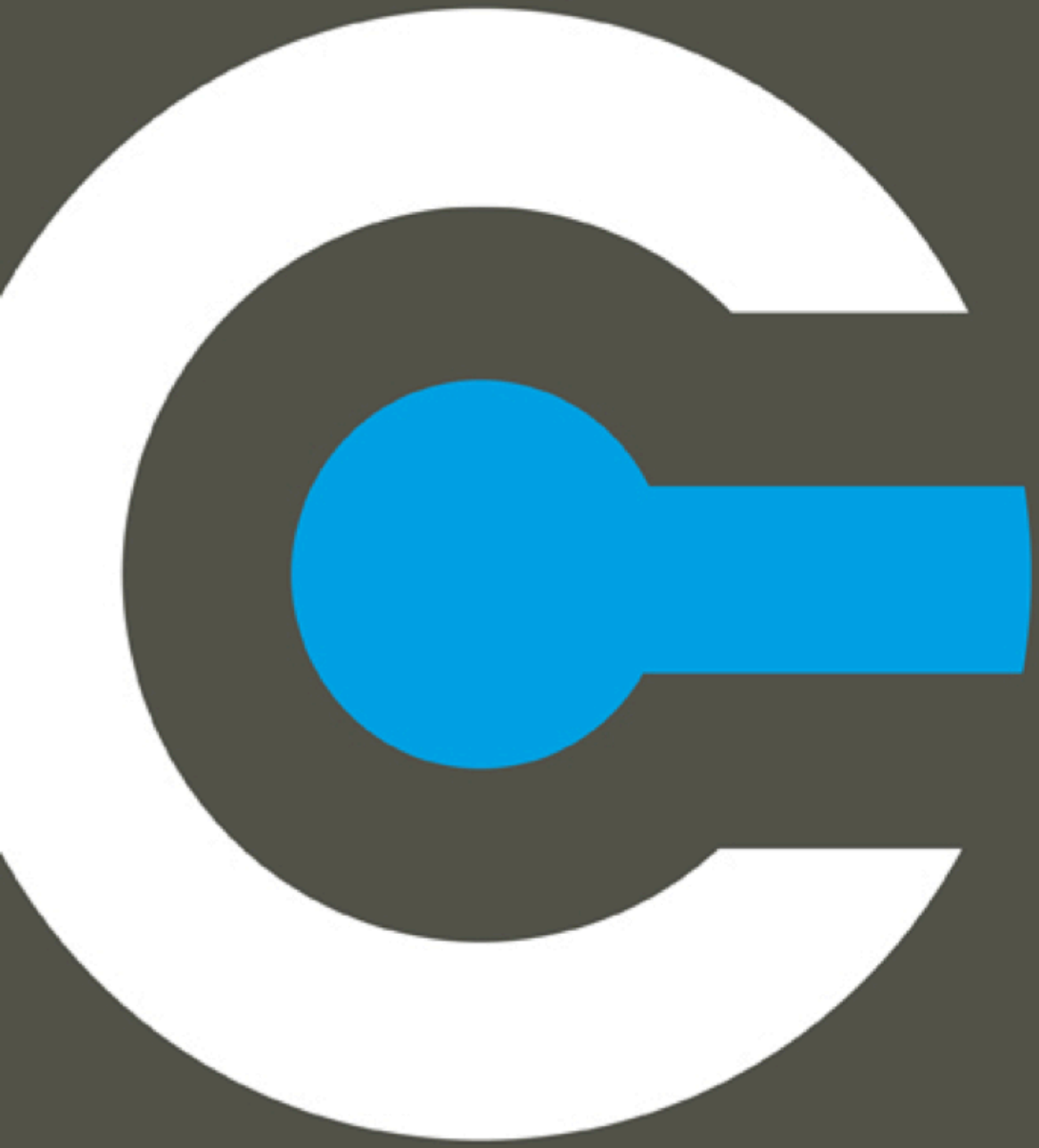
Privacy Governance Handreiking Veiligheidshuizen



Considerati
www.considerati.com

mr. dr. B.W. Schermer
mr. drs. M. Wubben CIPP/E
mr. N. Falot

Mei 2014

Voorwoord

In mei 2013 is door adviesbureau Considerati en de Rijkuniversiteit Leiden in opdracht van het Ministerie van Veiligheid en Justitie een impactanalyse uitgevoerd op het gebruik van het Generiek Casusoverleg Ondersteunend Systeem (GCOS) bij het casusoverleg in de Veiligheidshuizen. Deze analyse leverde op dat zowel in de inrichting van de werkprocessen binnen de Veiligheidshuizen als in de applicatie GCOS aanpassingen nodig waren om legitieme verwerking van persoonsgegevens te bevorderen. Vanuit de Veiligheidshuizen zelf en door de daarin samenwerkende ketenpartners werd eveneens aangedrongen op ondersteuning bij het beantwoorden van privacyvraagstukken en op meer eenduidigheid in de manier waarop in en rond casusoverleggen persoonsgegevens worden verwerkt. Ook ontstond onzekerheid over het gebruik van GCOS bij die overleggen.

Voor het Ministerie waren deze signalen aanleiding voor twee acties.

In samenspraak met het gebruikersveld is in kaart gebracht welke aanpassingen in GCOS nodig zijn, om goede verwerking van persoonsgegevens beter te faciliteren. Deze aanpassingen hebben betrekking op autorisaties, op de aard van de gegevens die in GCOS worden verwerkt en opgeslagen en op het afsluiten van casussen. Ook is vastgesteld hoe GCOS dient te worden ingericht om beter geïntegreerd casusoverleg - het zogenaamde 'casusoverleg op maat' zoals gedefinieerd in het Landelijk Kader voor de Veiligheidshuizen- te kunnen ondersteunen. Deze aanpassingen worden in de komende periode met gebruikersorganisaties, beheerder Justid en VenJ als eigenaar van GCOS, onder regie van het Bureau Regie en Beheer, uitgewerkt en gerealiseerd.

Voor de ondersteuning van Veiligheidshuizen heeft VenJ aan Considerati gevraagd een Handreiking privacy governance voor de Veiligheidshuizen te maken. Deze Handreiking is een hulpmiddel dat Veiligheidshuizen kunnen gebruiken om de werkprocessen, de organisatieinrichting en de beveiligingspraktijk te verbeteren zodat casusoverleg effectief blijft én de daarvoor benodigde gegevens binnen de grenzen van wet en regelgeving worden verwerkt. Ook biedt het een handvat om met nieuwe typen casusoverleg te organiseren, al dan niet in opdracht van gemeenten. Voor de totstandkoming van deze handreiking is met een aantal Veiligheidshuizen geanalyseerd hoe zij hun privacybeleid en –praktijk nu ingericht hebben. Ook is met ketenpartners in kaart gebracht welke eisen en wensen zij hebben ten aanzien van verwerking van persoonsgegeven in de samenwerking met andere partijen.

Het resultaat ligt voor u: de Handreiking privacy governance Veiligheidshuizen. Met de Vereniging van Managers van Veiligheidshuizen en de samenwerkende ketenpartners worden nadere afspraken gemaakt worden over hoe de Handreiking maximale waarde voor de inrichting van de werkprocessen in de Veiligheidshuizen kan hebben. Ik heb er vertrouwen in dat de Handreiking een nuttig instrument is voor de doorontwikkeling van Veiligheidshuizen waarbij de verwerking van persoonsgegevens rechtmatige is én de aanpak effectief blijft.

Drs. Mr. R.R. ter Kuile,
Directeur Justitieel Jeugdbeleid,
Ministerie van Veiligheid en Justitie
April 2014

Inhoudsopgave

Inleiding

Het delen van persoonsgegevens in en rondom het veiligheidshuis is vaak noodzakelijk om oplossingen te vinden in gevallen waarin sprake is van 'ketenoverstijgende complexe multi-problematiek'. [1] In de praktijk betekent dit dat het noodzakelijk is dat partijen uit verschillende domeinen, zoals de strafrechtketen en de zorgketen, gezamenlijk optreden om tot een oplossing te komen. Daarnaast heeft een aantal veiligheidshuizen de taak om casusoverleggen te faciliteren die niet aan de criteria voor complexe multi-problematiek voldoen, maar waarbij het delen van gegevens met andere partijen toch noodzakelijk is om tot een oplossing te komen. Een voorbeeld hiervan is het kader Huiselijk Geweld.

Het verwerken[2] van persoonsgegevens staat vaak op gespannen voet met het recht op privacy van degene wiens gegevens worden verwerkt. Het is daarom van belang dat voldoende aandacht wordt geschonken aan de privacyaspecten van gegevensverwerkingen in en rondom het veiligheidshuis.

Deze handreiking dient als praktisch hulpmiddel bij (het organiseren van) een zorgvuldige omgang met persoonsgegevens in en rondom het veiligheidshuis. Hierbij zal het begrip 'privacy governance' centraal staan. Privacy governance komt kort gezegd neer op 'goed huisvaderschap' bij het verwerken van persoonsgegevens. De privacywetgeving stelt een aantal eisen aan degene die persoonsgegevens verwerkt. Bijvoorbeeld het waarborgen van de kwaliteit van gegevens, het zorg dragen voor de beveiliging en het informeren van degene wiens gegevens worden verwerkt. Wanneer deze eisen niet goed worden ingevuld is er geen sprake van goed huisvaderschap van gegevens. Deze handreiking geeft concrete handvatten voor het invullen van het goed huisvaderschap door middel van privacy governance.

In deze handreiking wordt slechts beperkt ingegaan op 'wat wel en niet mag'. De reden hiervoor is dat de rechtmatigheid van een verwerking volledig afhankelijk is van de specifieke context waarin zij plaatsvindt. De privacywetgeving geeft dan ook geen pasklaar antwoord op de vraag wat wel en niet mag met persoonsgegevens. De wet biedt wel een kader voor het maken van de juiste afweging omtrent rechtmatigheid. Deze handreiking geeft toelichting op dit kader en biedt daarnaast praktisch advies over hoe zorgvuldig om te gaan met persoonsgegevens.

Gebruik van deze Handreiking

Deze privacy governance handreiking is geschreven voor diegene die verantwoordelijk is voor het organiseren van een zorgvuldige omgang met privacy en gegevens in het veiligheidshuis. Dit is uiteindelijk het management van het veiligheidshuis en iets breder

[1] Zie voor de criteria van ketenoverstijgende complexe multi-problematiek het Landelijk Kader Veiligheidshuizen, p.17. Te raadplegen via: http://www.veiligheidshuizen.nl/doc/VHH-Landelijk-Kader-definitief.pdf

[2] Het delen van (gevoelige) persoonsgegevens wordt evenals het verzamelen, opslaan, delen, bewerken en verwijderen juridisch aangeduid met de term 'verwerken' (artikel 1, sub b, Wbp). In deze handleiding verstaan we dus onder het verwerken van persoonsgegevens alle handelingen die met persoonsgegevens kunnen worden verricht, waaronder het delen van de gegevens met ketenpartners.

gezien het management van de betrokken partijen binnen het samenwerkingsverband. Hier ligt ook een taak voor de gemeente, als verantwoordelijke instantie voor de samenwerking binnen de veiligheidshuizen. De concrete handreikingen die worden gedaan kunnen worden ingevuld door een 'privacy officer', maar ook de manager of ieder ander die deze taak is toebedeeld.

Een groot deel van de elementen uit deze handreiking kan door de aangewezen verantwoordelijke zelf worden ingevuld. Voor een aantal van de elementen wordt echter aangeraden gespecialiseerd juridisch advies in te winnen, omdat dit technische juridische vraagstukken betreft die van grote invloed kunnen zijn op de compliance van het veiligheidshuis. Dit advies kan zowel worden ingewonnen bij externe privacy professionals als bij een intern privacy jurist.

Leeswijzer

Deze handreiking bestaat uit twee delen.

Deel 1 gaat dieper in op wat 'privacy governance' is, waarom dit belangrijk is in en rondom het veiligheidshuis, het wettelijke kader voor de gegevensverwerking en hoe een privacy governance programma wordt opgestart.

Deel 2 bevat een gedetailleerde uitwerking van de verschillende onderdelen van privacy governance voor het veiligheidshuis. Een veiligheidshuis dat privacy en gegevens-bescherming in en rondom de organisatie wil borgen, moet er naar streven al deze onderdelen op te pakken.

Deel 1: Privacy Governance

1 Privacy in het veiligheidshuis

1.1 Het belang van privacy voor het veiligheidshuis

Persoonsgegevens worden verwerkt om bepaalde doelen te bereiken. In het geval van het veiligheidshuis is het doel om casusoverleg voor ketenoverstijgende complexe multi-problematiek en eventuele andere, aan het veiligheidshuis opgedragen casuïstiek mogelijk te maken. Tegenover dit belang staat veelal het privacybelang van het casussubject zelf en/of dat van de familie en omgeving.

Het beschermen van de privacybelangen van de betrokkene, diens familie of omgeving zal in eerste instantie vaak als een drempel of hindernis worden gezien voor de verwerking van persoonsgegevens. Voorgenomen verwerkingen kunnen worden vertraagd of tegen-gehouden omdat moet worden onderzocht of deze voldoen aan de privacywetgeving. Privacy hoeft echter geen obstakel te zijn: een verantwoorde en zorgvuldige omgang met persoonsgegevens heeft ook voordelen voor het veiligheidshuis.

Naast privacybescherming voor de betrokkene kan een verantwoorde en zorgvuldige omgang met persoonsgegevens de volgende voordelen voor het veiligheidshuis bieden:

1) Het verkleint het risico op non-compliance en daarmee handhaving door de toezichthouder en negatieve aandacht voor het veiligheidshuis vanuit politiek en media. De continuïteit van het veiligheidshuis wordt met een verantwoorde en zorgvuldige omgang met persoonsgegevens gewaarborgd.
2) Het geeft ketenpartners meer vertrouwen waardoor de bereidheid om gegevens te delen groeit.
3) Het stimuleert het vertrouwen in het veiligheidshuis bij betrokkenen, waardoor de kans op medewerking van cliënten groeit.

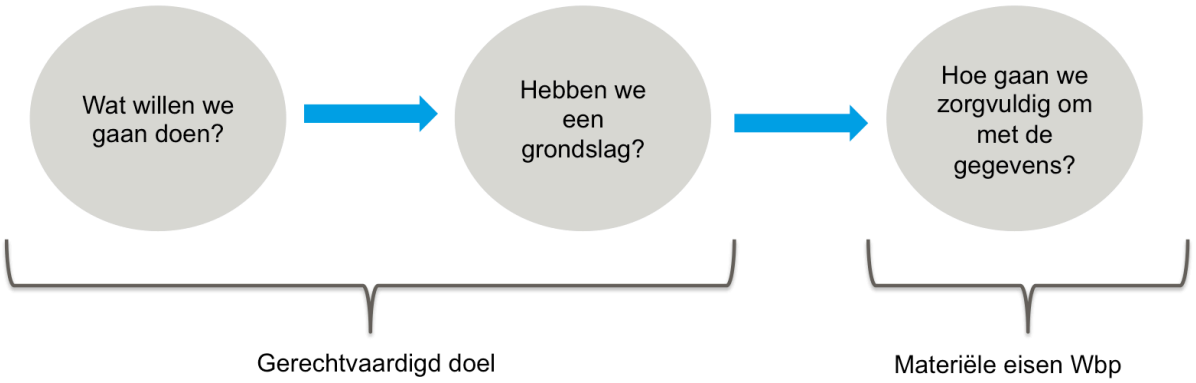
1.2 De Wet bescherming persoonsgegevens

Een groot deel van verantwoordelijke en zorgvuldige omgang met persoonsgegevens heeft te maken met het voldoen aan toepasselijke wet- en regelgeving. De Wet bescherming persoonsgegevens (Wbp) bevat de belangrijkste regels voor de bescherming van privacy wanneer het gaat om het verwerken van persoonsgegevens.[3]

De Wet bescherming persoonsgegevens beschermt de informationele privacy van burgers en biedt daarmee een kader dat de verwerking van persoonsgegevens onder condities toestaat. In tegenstelling tot wat vaak gedacht wordt, verbiedt de Wbp dus niet het delen van gegevens, maar geeft de Wbp aan onder welke omstandigheden dit mag (legitimiteit) en hoe er vervolgens met de gegevens moet worden omgegaan (zorgvuldigheid).

[3] Artikel 1, sub a, Wbp.

De Wbp hanteert een bepaalde systematiek om te bepalen of een voorgenomen verwerking is toegestaan. Door de volgende vragen voor ogen te houden kan worden bepaald of de voorgenomen verwerking in lijn is met de Wbp:



De bovenstaande vragen vertalen zich in de volgende drie eisen voor de verwerking van persoonsgegevens:

- Ad 1: Wat willen we gaan doen?
  Voor de verwerking van persoonsgegevens moeten welbepaalde en nadrukkelijk omschreven doelen zijn vastgesteld.
- Ad 2: Hebben we een grondslag?
  Deze doelen moeten gerechtvaardigd zijn. Of het doel gerechtvaardigd is, is ten eerste afhankelijk of de verwerking gebaseerd kan worden op één van de grondslagen uit de Wbp.[4] Daarnaast moet worden nagegaan of de aanpak effectief, proportioneel en is en of de gestelde doelen niet op een andere manier te bereiken zijn (subsidiariteit).
- Ad 3: Hoe gaan we zorgvuldig om met de gegevens?
  In de Wbp worden een aantal materiële eisen gesteld (zoals beveiliging of transparantie) waarmee invulling wordt gegeven aan een zorgvuldige omgang met persoonsgegevens.

Deze eisen zullen verder worden uitgewerkt in Deel II.

De regels uit de Wbp zijn open geformuleerde normen die vaak moeilijk direct toepasbaar zijn in concrete gevallen. De Wbp heeft daardoor niet voor iedere specifieke situatie een duidelijk antwoord. Met name door de complexiteit van de verwerkingen in en rondom het veiligheidshuis, waarbij verschillende partijen betrokken zijn, kan het lastig zijn om in een specifiek geval concreet invulling te geven aan de open geformuleerde normen uit de Wbp. Met behulp van het in deze handreiking uiteengezette privacy governance programma wordt praktische invulling van de open geformuleerde normen uit de Wbp vergemakkelijkt.

[4] Omdat elke situatie anders is worden geen concrete adviezen gegeven over de te gebruiken grondslagen voor de gegevensverwerking. Wel worden de mogelijke grondslagen benoemd en kort toegelicht. Zie paragraaf 3.2.1.

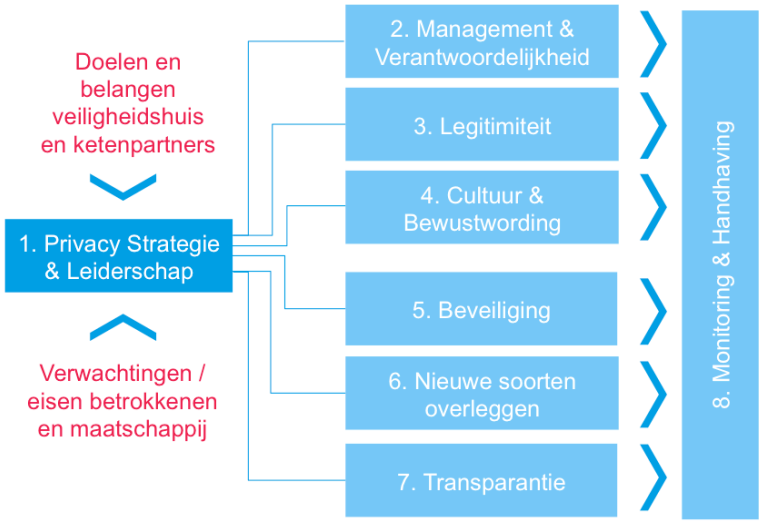
1.3 Waarom Privacy Governance?

Privacy governance stuurt en controleert alle processen in en rondom het veiligheidshuis waarbij persoonsgegevens worden verwerkt. Privacy governance is een programmatische aanpak op het gebied van privacy en de bescherming van persoonsgegevens die invulling geeft aan het 'goed huisvaderschap' van gegevens. Door middel van privacy governance wordt een verantwoorde wijze van verwerking van persoonsgegevens in en rondom het veiligheidshuis gerealiseerd. Op verantwoorde wijze persoonsgegevens verwerken gaat verder dan naleving van wet- en regelgeving; om op zorgvuldige wijze met persoonsgegevens om te gaan moet ook worden nagegaan hoe het belang van privacy binnen het veiligheidshuis wordt ingevuld (privacy ethiek) en hoe over privacy naar de buitenwereld wordt gecommuniceerd (transparantie). Deze elementen zullen daarom worden meegenomen in het opstellen van een privacy governance plan voor het veiligheidshuis.

De winst van het uitvoeren van een privacy governance programma is dat het gehele proces van gegevensverwerking duidelijk en controleerbaar wordt. Voor diegenen die de werkzaamheden van het veiligheidshuis uitvoeren schept een privacy governance programma zekerheid over de manier waarop invulling moet worden gegeven aan het privacybelang van de betrokkenen. Hierdoor worden fouten (die leiden tot onrechtmatige verwerkingen) beperkt of voorkomen en lopen het veiligheidshuis en de ketenpartners minder risico op reputatieschade en handhaving door de toezichthouder. Ook helpt een privacy governance programma bij de transparantie van het veiligheidshuis; de gegevensverwerking wordt zodanig ingericht dat te allen tijde inzichtelijk kan worden gemaakt hoe de gegevensverwerking is gegaan, welke keuzes daarbij zijn gemaakt en waarom. Hiermee kan optimaal verantwoording worden afgelegd over de verwerking van persoonsgegevens aan betrokkenen, ketenpartners, de toezichthouder en de politiek.

1.4 Een privacy governance programma starten: acht onderdelen

Een privacy governance programma bestaat uit een achttal onderdelen. Deze onderdelen worden hieronder afzonderlijk kort toegelicht. In het volgende deel worden de onderdelen uitgebreider toegelicht en worden de acties die per onderdeel kunnen worden ondernomen benoemd en uitgewerkt.



1. Privacy Strategie & Leiderschap

Strategie en Leiderschap omvat het maken van keuzes over de verwerking van persoonsgegevens (de zogenaamde privacy ethiek). Daarnaast moet het management keuzes maken over hoe de eisen van de wet praktisch worden vormgegeven binnen de organisatie (compliance). Dit omvat onder andere het richting geven aan het privacy governance programma en het stellen van prioriteiten binnen de uitvoering.

Zorgvuldige omgang met persoonsgegevens draagt bij aan het vertrouwen dat ketenpartners en cliënten hebben in het veiligheidshuis. Wanneer het management privacy hoog op de bestuurlijke agenda plaatst en goed huisvaderschap zowel intern (bij het personeel) als extern (bij de ketenpartners) stimuleert, groeit het vertrouwen in het veiligheidshuis. Dit betekent dat ketenpartners eerder geneigd zullen zijn om gegevens te delen en cliënten minder weerstand hebben tegen de verwerking van hun persoonsgegevens. Daarnaast helpt het bepalen van een duidelijke strategie medewerkers in de zorgvuldige omgang met persoonsgegevens.

2. Management en verantwoordelijkheid

De verantwoordelijkheid voor het uitvoeren van het privacy governance plan in de dagelijkse praktijk moet binnen het veiligheidshuis zijn belegd (bijvoorbeeld bij een privacy officer). Ook moeten voldoende middelen beschikbaar zijn voor de uitvoering van het plan. Het veiligheidshuis moet procedures inrichten om rekenschap af te kunnen leggen over het verzamelen en gebruiken van gegevens aan de betrokkene, de ketenpartners, de toezichthouder en andere partijen zoals belangenverenigingen en politiek. Ook moet de samenwerking duidelijk worden vormgegeven. Door de verantwoordelijkheid voor de verwerking van persoonsgegevens duidelijk te beleggen en hier voldoende middelen voor vrij te maken, wordt naleving van de vastgestelde privacystrategie gewaarborgd.

3. Legitimiteit van verwerkingen

Persoonsgegevens mogen alleen worden verwerkt op basis van een legitieme grondslag. Het veiligheidshuis moet daarom zicht hebben op alle verwerkingen en kunnen aantonen waarom deze legitiem zijn. Zoals eerder in dit hoofdstuk is besproken, bepaalt de systematiek van de Wbp dat legitimiteit wordt afgeleid uit het doel en de grondslag van de gegevensverwerking en het antwoord op de vraag of goed invulling is gegeven aan de materiële eisen van de Wbp. In Deel 2 zal hier nader op worden ingegaan met aandacht voor de specifieke problematiek die van toepassing is op de gegevensverwerking in en rondom het veiligheidshuis.

4. Privacycultuur en bewustzijn

Een goed privacybeleid werkt alleen als alle medewerkers op de hoogte zijn van het belang van privacy en duidelijke instructies krijgen over hoe zij om moeten gaan met persoonsgegevens. Door middel van specifieke trainingen, permanente scholing en hulpmiddelen die zorgvuldige omgang met privacy en persoonsgegevens stimuleren, kan de privacycultuur binnen het veiligheidshuis en de ketenpartners worden verbeterd.

5. Veiligheid van gegevens

Veiligheid van gegevens is een belangrijke eis uit de Wbp. Het veiligheidshuis moet een risico-inventarisatie maken en op basis daarvan een duidelijk plan voor informatiebeveiliging opstellen (een beveiligingsbeleid). Hierbij moet rekening worden gehouden met de aard en gevoeligheid van de gegevens, en het risico van verlies of onrechtmatige verwerking daarvan voor de betrokkene. Bij de beveiliging moet rekening worden gehouden met de fysieke beveiliging, de opslag van gegevens en de beveiliging van dataverkeer. Uitgangspunt voor de beveiliging moeten relevante standaarden zijn zoals bijvoorbeeld ISO 27001. Binnen de overheid kan worden aangesloten bij standaarden als de VIR en VIR-BI.

6. Nieuw soort casusoverleg

Privacybescherming is een continue ontwikkeling. Het kan voorkomen dat het veiligheidshuis vanuit de gemeente de opdracht krijgt een nieuw soort casusoverleg te faciliteren. De vraag die hierbij rijst is of reeds in het kader van een andersoortig casusoverleg verzamelde gegevens in dit nieuwe soort casusoverleg mogen worden gebruikt. In principe mogen gegevens alleen worden verwerkt voor zover dit in lijn is met het oorspronkelijke doel waarvoor zij zijn verzameld (doelbinding).[5] Wil het veiligheidshuis en/of de ketenpartners een nieuwe verwerking gaan doen met gegevens die reeds verwerkt worden, dan moet gekeken worden of dit in lijn is met de doelbinding, zie paragraaf 3.2 en Hoofdstuk 6. Het is aan het veiligheidshuis om dit te toetsen, alsmede na te gaan wat de impact op de privacy is voor de betrokkene wiens gegevens worden (her)gebruikt.

7. Transparantie

Het veiligheidshuis moet openheid van zaken geven over de manier waarop persoonsgegevens worden verwerkt en voor welke doelen. Openheid en transparantie omvat het doen van meldingen bij het College bescherming persoonsgegevens, het plaatsen van privacy notificaties op de website en voorlichting via bijvoorbeeld folders en informatiebladen aan de betrokkene die wordt besproken in het veiligheidshuis.

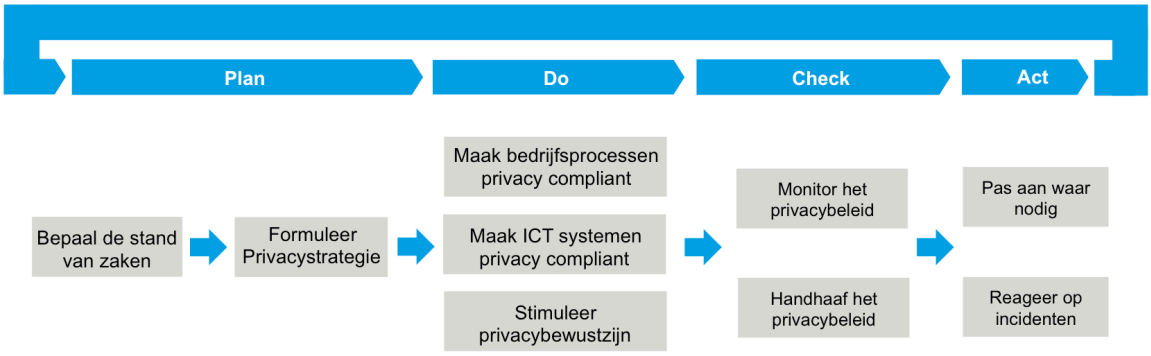
8. Handhaving en monitoring

Sluitstuk van een goed privacy programma is monitoring en handhaving. Door het monitoren van het privacy programma kan het programma waar nodig worden bijgestuurd. Handhaving zorgt ervoor dat het belang van privacy wordt onderstreept en medewerkers worden afgerekend op onzorgvuldig handelen.

1.5 Privacy governance als cyclisch proces

Privacy is constant in beweging. Niet alleen kan wet- en regelgeving omtrent privacy en gegevensbescherming veranderen, ook interne ontwikkelingen kunnen tot nieuwe inzichten, beleid en procedures leiden. Om privacybescherming in en rondom het veiligheidshuis op een optimaal niveau te krijgen en te houden, is het belangrijk dat met deze veranderingen rekening wordt gehouden. Een privacy governance plan uitvoeren is daarom niet een eenmalige actie, maar zal periodiek op onderdelen moeten worden nagekeken, bijgesteld of herhaald. Dit kan door middel van het doorlopen van een plan-do-check-act cyclus.

[5] Artikel 9 Wbp.


Plan
Do
Check
Act
Bepaal de stand van zaken
Formuleer Privacystrategie
Maak bedrijfsprocessen privacy compliant
Maak ICT systemen privacy compliant
Stimuleer privacybewustzijn
Monitor het privacybeleid
Handhaaf het privacybeleid
Pas aan waar nodig
Reageer op incidenten

Deel 2: Aan de slag met een eigen privacy governance plan

In dit deel worden de acht elementen van privacy governance in specifieke acties uiteengezet.

1 Strategie & Leiderschap

1.1 Definieer privacy als strategische waarde

Wil privacybeleid succesvol zijn, dan moet de hele organisatie hiervan doordrongen zijn. Dit begint bij het management. Wanneer de leiding van de organisatie privacy niet als strategische waarde beschouwt, dan is de kans dat het privacybeleid succesvol is en medewerkers zich er aan houden gering. Het management van het veiligheidshuis moet privacy en bescherming van persoonsgegevens daarom (hoog) op de interne agenda plaatsen. Ook binnen ketensamenwerkingen moet men het belang van privacy onderkennen.

Ook moet het management de te bereiken doelstellingen op het gebied van privacybescherming voor de organisatie bepalen.

Vragen die het management zich kan stellen bij het achterhalen van de strategische waarde van privacy voor het veiligheidshuis zijn:

- Welke risico's brengt het verzamelen en delen van gegevens met zich mee voor de privacy van de betrokkenen?
- Welke risico's brengt het verwerken van persoonsgegevens met zich mee voor het veiligheidshuis en/of de ketenpartners?
- Waar liggen de prioriteiten in het versterken van het privacybeleid?
- Hoe worden middelen aangewend om privacy compliance te stimuleren?
- Hoe wordt intern en extern gecommuniceerd over het belang van privacy?

1.2 Bepaal de positie van het veiligheidshuis

Wil effectief invulling worden gegeven aan het privacybeleid dan moet het veiligheidshuis haar positie binnen de ketensamenwerking(en) bepalen. Het Landelijk Kader Veiligheidshuizen biedt hier houvast.[6] In het Landelijk Kader Veiligheidshuizen wordt de positionering, functie, doelstelling, scope en organisatie van een veiligheidshuis in het algemeen uiteengezet. Dit Landelijk Kader kan als uitgangspunt dienen bij het bepalen van de eigen positie als veiligheidshuis.

De hoofdvraag bij het bepalen van de positie van het veiligheidshuis vanuit privacyperspectief is welk *doel* het veiligheidshuis heeft. Het doel van het veiligheidshuis is bepaald bij de oprichting ervan en kan worden afgeleid uit het mandaat waaronder het veiligheidshuis werkzaam is. Een leidende vraag hierbij is: 'waarom is het veiligheidshuis opgericht?' De verwerking van persoonsgegevens moet passen binnen het doel van het veiligheidshuis.

---

[6] Ministerie van Veiligheid en Justitie, 'Landelijk kader Veiligheidshuizen. Vóór en dóór partners', pagina 17, via http://www.veiligheidshuizen.nl/doc/VHH-Landelijk-Kader-definitief.pdf.

Ook moet worden vastgesteld welke *rol* het veiligheidshuis speelt in het verwezenlijken van haar doelstellingen. Mag het veiligheidshuis alleen naar aanleiding van een melding samenwerking tussen ketenpartners faciliteren, of mag het veiligheidshuis (bijvoorbeeld in opdracht van de gemeente) hierin ook zelf het initiatief nemen?

Pas wanneer het veiligheidshuis goed voor ogen heeft wat haar eigen rol en positie is, kan samenwerking met andere partijen optimaal worden vormgegeven en kunnen casus efficiënt worden opgelost.

1.3 Bepaal de huidige stand van zaken

Na de positionering van het veiligheidshuis op het gebied van privacy is het vervolgens zaak om te bepalen wat de huidige stand van zaken is met betrekking tot privacy governance binnen het veiligheidshuis. Het bepalen van de huidige stand van zaken wordt ook wel een nulmeting genoemd.

Het veiligheidshuis en/of het samenwerkingsverband moet eerst weten hoe zij 'scoren' op alle acht de elementen van privacy governance. Dit betekent dat men zicht moet krijgen op onder andere de volgende concrete vragen:

1) Welke gegevens worden verwerkt? (Zie paragraaf 3.1)
2) Voor welke doeleinden worden deze gegevens verwerkt? (Zie paragraaf 3.2)
3) Zijn deze gegevens noodzakelijk voor het doel? (Zie paragraaf 3.2)
4) Is er een legitieme grondslag voor het verwerken van deze gegevens? (Zie paragraaf 3.3)
5) Welke afspraken zijn gemaakt met ketenpartners? (Zie paragraaf 2.4 en 3.4 en 3.5)
6) Is invulling gegeven aan beveiligingseisen? (Zie hoofdstuk 5)
7) Zijn maatregelen genomen om invulling te geven aan de rechten van de betrokkene? (Zie paragraaf 3.9)

Alvorens invulling te geven aan de onderdelen van deze handreiking kan ieder onderdeel worden nagelopen om na te gaan in hoeverre dit onderdeel al in het eigen veiligheidshuis is belegd. Hierdoor wordt inzicht verkregen in het huidige niveau van compliance en krijgen veiligheidshuis en ketenpartners zicht op de noodzakelijke verbeterstappen. Een inventarisatie van de huidige stand van zaken kan worden uitgevoerd door een interne privacy deskundige of door een extern privacy adviesbureau.

1.4 Stel een strategisch privacy plan vast

Op basis van de positionering en de nulmeting wordt een strategisch privacy plan geformuleerd. Bij een strategisch privacy plan wordt bepaald:

- welke onderdelen van het privacybeleid (directe) aandacht behoeven;
- welke onderdelen in een later stadium worden opgepakt;
- wie voor de uitvoering van het privacybeleid verantwoordelijk is;
- welke middelen worden vrijgemaakt voor de invulling van het privacybeleid;
- wat de doorlooptijd is van de voorgenomen acties; en
- hoe wordt gerapporteerd over de resultaten (Key Performance Indicators).

Een strategisch privacy plan helpt om privacy op de lange termijn goed binnen het veiligheidshuis te beleggen. Ook worden door middel van een strategisch privacy plan de

verschillende onderdelen van privacy governance op een zo effectief mogelijke wijze ingevuld.

1.5 Intern privacy beleid

Het strategische privacy plan wordt door het opstellen van een intern privacy beleid vertaald naar een praktisch kader voor het dagelijkse werk binnen het veiligheidshuis. Een intern privacy beleid geeft invulling aan de doelstellingen die zijn vastgelegd in het strategisch privacy plan en is de 'houvast' voor medewerkers.

In een intern privacy beleid komen minimaal de volgende zaken aan de orde:

Algemeen deel van het privacy beleid:

- Voor wie het beleid geldt (voor welke medewerkers).
- De wettelijke kaders die gelden voor de verwerking van persoonsgegevens.
- De doelstellingen op het gebied van privacybescherming voor het veiligheidshuis.

Inhoudelijke aspecten:

- Uitleg van veel voorkomende begrippen zoals (bijzonder) persoonsgegeven, betrokkene, verantwoordelijke et cetera.;
- De mogelijke doelen en grondslagen voor de verwerking van persoonsgegevens en hoe deze kunnen worden vastgesteld;
- De mogelijke doelen en grondslagen voor de verwerking van bijzondere persoonsgegevens en hoe deze kunnen worden vastgesteld;
- De mogelijke manieren waarop persoonsgegevens kunnen worden verkregen;
- De mogelijkheden om gegevens te delen met ketenpartners en de procedures die hierbij moeten worden gevolgd;
- Uitleg over (het vaststellen van) de doelbinding;
- Regels voor de zorgvuldige omgang met persoonsgegevens waaraan het personeel zich moet houden;
- Hoe medewerkers invulling moeten geven aan beveiliging (bijvoorbeeld alleen in goedgekeurde systemen opslaan, geen USB-sticks, computer beveiligen, geen printjes maken van lijsten et cetera);
- Uitwerking procedures voor invulling van de rechten van de betrokkene;
- Hoe invulling dient te worden gegeven aan transparantie en communicatie;
- Uitwerking van procedures voor klachten;
- Waar medewerkers terecht kunnen als zij vragen hebben over de verwerking van persoonsgegevens;
- Heldere consequenties voor het niet naleven van dit beleid.

2 Management en verantwoordelijkheid

Om privacybescherming werkbaar te maken moet de verantwoordelijkheid voor gegevensverwerkingen goed worden belegd. Daarnaast moeten binnen het veiligheidshuis en in de samenwerking met ketenpartners heldere afspraken worden gemaakt.

2.1 Wijs één of meer verantwoordelijken aan

Een belangrijke vervolgstap in het proces is het vaststellen van de formeel-juridische 'verantwoordelijke' voor de gegevensverwerking.[7] Voor iedere gegevensverwerking moet een verantwoordelijke worden aangewezen. De Wbp definieert de verantwoordelijke als 'diegene die het doel en de middelen voor de gegevensverwerking bepaalt.'

De formeel-juridische verantwoordelijkheid kan bij een natuurlijke persoon of een rechtspersoon liggen. Daarbij hoeft de verantwoordelijkheid voor alle verwerkingen in een keten niet bij één partij te liggen, er kunnen ook meerdere partijen verantwoordelijk zijn.

Indien meerdere partijen verantwoordelijk zijn voor de gegevensverwerking is het belangrijk dat duidelijke afspraken worden gemaakt over de wijze waarop over de verantwoordelijkheid naar buiten wordt gecommuniceerd en opgetreden. Het moet duidelijk zijn wie de verantwoordelijke is voor de verwerking van de persoonsgegevens van een betrokkene. De verantwoordelijke is namelijk het primaire aanspreekpunt voor de betrokkene, bijvoorbeeld voor het stellen van vragen over de verwerking. Meer in het bijzonder is het voor het uitoefenen van het inzage-, correctie- en verwijderingsrecht van de betrokkene van belang dat hij weet wie de verantwoordelijke is bij wie hij deze rechten geldend kan maken.

Bij het invullen van de verantwoordelijkheid moet daarom rekening worden gehouden met de perceptie van betrokkenen over wie de verantwoordelijke is. Deze perceptie kan namelijk verschillen van de formeel-juridische werkelijkheid. Vooral wanneer de betrokkene met medewerkers van verschillende organisaties wordt geconfronteerd die onder de gezamenlijke noemer 'veiligheidshuis' actief zijn, kan het onduidelijk zijn wie de primair verantwoordelijke is voor de verwerking. In een dergelijk geval kan de perceptie van de betrokkene zijn dat het veiligheidshuis de primair verantwoordelijke is voor de verwerking van zijn gegevens. In werkelijkheid kan de verantwoordelijkheid echter formeel bij ieder van de ketenpartners afzonderlijk zijn belegd. Houd hiermee rekening bij het inrichten van de verantwoordelijkheid en zorg voor duidelijke communicatie hierover naar de betrokkene toe.

Wanneer het veiligheidshuis geen rechtspersoonlijkheid heeft kan het ook geen drager zijn van rechten en plichten en dus geen verantwoordelijkheid hebben. In dit geval zal de verantwoordelijkheid voor de verwerking van persoonsgegevens anderszins moeten worden belegd, bijvoorbeeld bij de gemeente(n) waaronder het veiligheidshuis werkzaam is. Overigens leidt het enkele feit dat een veiligheidshuis wél rechtspersoonlijkheid heeft of onder een andere rechtspersoon valt niet gelijk tot een rechtsgeldige grondslag voor de verwerking van persoonsgegevens.

[7] Artikel 1, sub d, Wbp.

2.2 Interne verantwoordelijkheid

Ook intern moet iemand worden aangewezen die de verantwoordelijkheid voor het uitvoeren van het privacybeleid op zich neemt. Deze rol kan worden ingevuld door een privacy officer of functionaris gegevensbescherming. Belangrijk is dat een dergelijke interne verantwoordelijke voldoende middelen en autoriteit (doorzetmacht) heeft voor het uitvoeren van het privacy governance programma.

De intern verantwoordelijke dient als primair aanspreekpunt voor medewerkers over de verwerking van persoonsgegevens. Deze persoon moet daarom goed op de hoogte zijn van het wettelijke kader voor de verwerking van persoonsgegevens en de strategische doelen van het veiligheidshuis rondom privacy.

2.3 Definieer de samenwerking met ketenpartners

Naast het bepalen van de eigen positie, is het van belang dat het veiligheidshuis een beeld heeft van haar positie in het samenwerkingsverband en van de posities van de respectievelijke ketenpartners. Ook hierin moet duidelijk zijn met welk *doel* het veiligheidshuis in de samenwerking actief is en welke *rol* het veiligheidshuis hierin vervult. Hierin is niet alleen het beeld van belang dat het veiligheidshuis van zichzelf heeft, maar moet ook de perceptie van ketenpartners worden meegewogen.

Het veiligheidshuis moet een overzicht hebben van de betrokken ketenpartners, de gronden waarop deze partners zijn betrokken en hun respectievelijke doelen en rollen. De afzonderlijke ketenpartners zullen waarschijnlijk hun eigen belangen, wensen en behoeften hebben wanneer zij zich bij het samenwerkingsverband aansluiten. Om ervan verzekerd te zijn dat het onderling delen van gegevens op een effectieve en verantwoorde wijze geschiedt, is het van belang een overzicht te hebben van deze belangen, wensen en behoeften. Met behulp van een duidelijk overzicht kan per ketenpartner worden nagegaan of gegevensdeling toereikend, ter zake dienend en niet bovenmatig is. Ook helpt een duidelijk overzicht bij het waarborgen van de kwaliteit van de verwerkte gegevens. De verwerkte persoonsgegevens moeten namelijk, gelet op het doel waarvoor zij zijn verzameld of worden verwerkt, juist en nauwkeurig zijn.[8]

Ketenpartners hebben allemaal hun eigen juridische verantwoordelijkheid voor de gegevens die zij verwerken en delen. Het is daarom van belang dat per (soort) casusoverleg, alvorens aan het overleg te beginnen en gegevens onderling te delen, goed met elkaar wordt afgestemd welke gegevens gedurende welke fase in het proces en onder welke omstandigheden met elkaar mogen worden gedeeld (zie hiervoor ook de paragrafen 3.2 en 3.3 over doel en grondslag). Naast afspraken over de te delen gegevens, moeten ook afspraken worden gemaakt over de wijze waarop met (gedeelde) gegevens dient te worden omgegaan. Hierbij kan worden gedacht aan afspraken over beveiliging, bewaartermijnen of het verder gebruik van de gegevens.

Afspraken over de mate van gegevensdeling en zorgvuldigheid bij de verwerking van verstrekte gegevens helpen gegevensdeling te bevorderen en non-compliance tegen te gaan. Het overtreden van wettelijke bepalingen omtrent het delen van persoonsgegevens heeft

[8] Artikel 11 Wbp.

namelijk zijn weerslag op zowel de verstrekker als de ontvanger, alsmede op de gehele samenwerking.

2.4 Stel een samenwerkingsconvenant op

Een samenwerkingsconvenant is een document waarin de afspraken zijn vastgelegd die tussen de verschillende partijen die betrokken zijn in de behandeling van een specifieke casus zijn gemaakt. De verantwoordelijkheden, verhoudingen en taken van de afzonderlijke partijen worden in het samenwerkingsconvenant vastgelegd. Voorts zijn in het samenwerkingsconvenant de redenen voor en de afwegingen die voorafgingen aan de samenwerking opgenomen. Met behulp van een samenwerkingsconvenant worden de onderlinge verwachtingen gemanaged en de uitvoering daarvan gestroomlijnd.

Het kan voorkomen dat gedurende het verloop van een casus wordt besloten een nieuwe ketenpartner aan te trekken, bijvoorbeeld omdat dit noodzakelijk is voor het vinden van een oplossing voor de casus. Door de gronden en overwegingen die voorafgingen aan het aantrekken van deze partner op schrift te stellen, kan achteraf eenvoudig verantwoording hierover worden afgelegd. Ook kunnen de criteria hiervoor worden opgenomen in de informatie naar betrokkenen en andere (keten)partners, zodat steeds een duidelijke verwachting is over met wie, en onder welke omstandigheden, persoonsgegevens worden gedeeld (zie hiervoor ook Hoofdstuk 7: Transparantie). Door deze nieuwe partner, met opgave van redenen voor het aantrekken daarvan, toe te voegen aan het samenwerkingsconvenant, wordt deze nieuwe partner verplicht zich aan de bepalingen die daarin zijn opgenomen te houden. Op deze wijze kan het veiligheidshuis invloed uitoefenen op de manier waarop ook nieuw aangetrokken partners met de persoonsgegevens van betrokkenen omgaan.

Houd er rekening mee dat er door middel van een convenant geen nieuwe juridische grondslagen voor de verwerking kunnen worden gecreëerd. Het enkele feit dat er een convenant is betekent dus niet dat gegevens die eerst niet mochten worden verwerkt nu wel mogen worden verwerkt.

3 Legitimiteit van verwerkingen

Daar waar het onderdeel management en verantwoordelijkheid ziet op het krijgen van een goed overzicht van de betrokken partijen, de doelen en de onderlinge afspraken, ziet het onderdeel legitimiteit op het vaststellen of een gegevensverwerking überhaupt plaats mag vinden.

3.1 Inventariseer de gegevensverwerking

Nadat de rollen en verantwoordelijkheden voor gegevensverwerking duidelijk zijn belegd, moet inzichtelijk worden gemaakt *welke gegevens* daadwerkelijk in het veiligheidshuis worden verwerkt. Daarnaast moet worden nagegaan welke gegevens tijdens de samenwerking onderling worden gedeeld. Maak hierbij onderscheid tussen de verschillende soorten en categorieën gegevens die worden verwerkt. Afhankelijk van het soort gegeven, bijvoorbeeld bij een bijzonder persoonsgegeven, kunnen andere eisen aan de waarborgen ter bescherming van de privacy van de betrokkene worden gesteld.

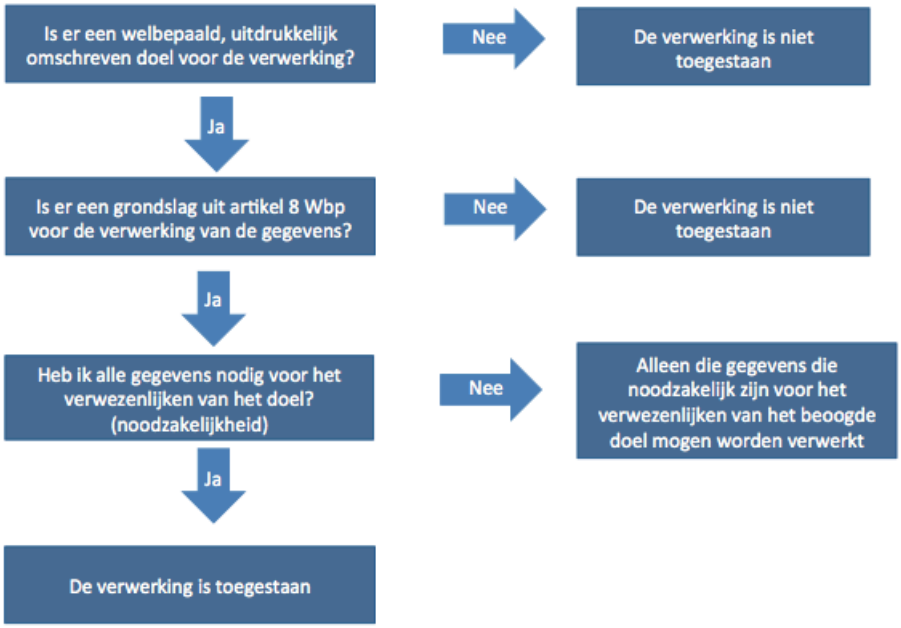
Nadat een inventarisatie is gemaakt van de gegevens die reeds worden verwerkt kan worden nagegaan of deze verwerkingen legitiem zijn. Deze inventarisatie dient daarmee als leidraad voor nieuwe verwerkingen.

3.2 Stel het doel voor de verwerking vast

Op grond van de Wbp mogen persoonsgegevens alleen worden verzameld indien dit gebeurt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.[9] Verder moet steeds worden nagegaan of de gegevens die worden verwerkt ook echt dat doel dienen, ter zake dienend en niet bovenmatig zijn.[10] Gegevens die niet noodzakelijk zijn voor het verwezenlijken van het beoogde doel mogen in principe niet worden verwerkt. Het begrip ‘noodzakelijk’ moet hierbij zo beperkt mogelijk worden uitgelegd: noodzakelijk is niet hetzelfde als handig.

Het volgende stroomschema kan helpen bij het vaststellen of de verwerking van persoonsgegevens in lijn is met het doelcriterium van de Wbp:

[9] Artikel 7 Wbp.
[10] Artikel 11 Wbp.



Tenzij de gegevensverwerking kan worden gebaseerd op ondubbelzinnige toestemming van de betrokkene (zie paragraaf 3.3.1.1.), moet gegevensverwerking noodzakelijk zijn voor het beoogde doel. De hoofdregels hierbij zijn dat wanneer het beoogde doel met minder gegevens kan worden bereikt, dat ook met minder gegevens moet (proportionaliteit) en dat wanneer het beoogde doel ook op een andere wijze kan worden verwezenlijkt, gegevensverwerking achterwege moet blijven (subsidiariteit).

Zie de handleiding voor verwerkers van persoonsgegevens van het Ministerie van Justitie voor meer detail.[11]

3.2.1 Doelbinding en casus op maat

Uit de bovenstaande 'doelbinding' vloeit voort dat gegevens niet voor andere doelen mogen worden gebruikt dan de doelen waarvoor zij oorspronkelijk zijn verzameld. In het veiligheidshuis wordt echter gewerkt met het casus op maat principe. Een casus die in het veiligheidshuis wordt behandeld bestaat uit verschillende procesfasen, waarbij bij iedere fase opnieuw wordt geëvalueerd of de huidige procesrichting de juiste is. Tijdens deze evaluatie kunnen nieuwe omstandigheden aan het licht komen of kan nieuwe kennis worden opgedaan die vergen dat het doel van het overleg wordt aangepast.

Wanneer het doel van de samenwerking gedurende het overleg verandert, bijvoorbeeld door gewijzigde omstandigheden of nieuwe kennis, mogen eerder in het proces verwerkte gegevens alleen verder worden verwerkt/gedeeld indien dit nieuwe doel verenigbaar is met het oorspronkelijke doel van het casusoverleg.[12] Het veiligheidshuis moet procedures inrichten die er voor zorgen dat gegevens niet voor doelen worden aangewend die niet

[11] De Handleiding voor Verwerkers van Persoonsgegevens, Wet bescherming persoonsgegevens, April 2002 van het Ministerie van Justitie kan worden gevonden via: http://www.rijksoverheid.nl/documenten-en-publicaties/brochures/2006/07/13/handleiding-wet-bescherming-persoonsgegevens.html
[12] Artikel 9 Wbp.

verenigbaar zijn met het doel waarvoor de gegevens zijn verzameld. Om na te gaan of een nieuw doel verenigbaar is met het oorspronkelijke doel kan bijvoorbeeld een checklist worden opgesteld. Deze checklist moet een aantal criteria bieden om te beoordelen of het gebruik van de gegevens in de nieuwe context is toegestaan. Elementen die bepalend zijn voor de vraag of een nieuw doel verenigbaar is met het oorspronkelijke doel zijn:

- De verwantschap tussen het nieuwe en oorspronkelijke doel: een nauwere verwantschap zal eerder de verenigbaarheidstoets doorstaan dan twee verder van elkaar afstaande doelen.
- De aard van de gegevens: Naar mate de gevoeligheid van een gegeven toeneemt, zal ook de onverenigbaarheid met nieuwe doeleinden toenemen. Wanneer een gegeven als gevoelig is aan te merken, bijvoorbeeld wanneer het gaat om medische gegevens, zal verwerking voor een ander dan het oorspronkelijke doel minder snel als verenigbaar kunnen worden aangemerkt.
- De mogelijke gevolgen voor de betrokkene bij de nieuwe verwerking: de invloed van de verwerking op de betrokkene kan een indicatie zijn voor de verenigbaarheid van het nieuwe doel met het oorspronkelijke doel.
- De wijze van verkrijging van de gegevens: wanneer de gegevens buiten de betrokkene om zijn verkregen heeft dit invloed op de toets of een verdere verwerking verenigbaar is met het oorspronkelijke doel.
- De getroffen of voorgenomen waarborgen: de getroffen maatregelen zijn van invloed op de toets of het nieuwe doel verenigbaar is met het oorspronkelijke doel. Hierbij kan bijvoorbeeld worden gedacht aan informatievoorziening en mogelijkheid tot verzet.[13]

3.3 Bepaal grondslag voor gegevensverwerking en gegevensdeling

Zoals in paragraaf 3.2 is toegelicht mogen persoonsgegevens alleen worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen. Een doel is alleen gerechtvaardigd, als het gebaseerd kan worden op één van de zes grondslagen uit artikel 8 van de Wbp. Niet alleen het veiligheidshuis heeft een grondslag nodig voor gegevensverwerking, ook de (keten)partners hebben een grondslag nodig, bijvoorbeeld voor gegevensdeling met het veiligheidshuis en/of andere (keten)partners. Hieronder worden de grondslagen kort toegelicht:

3.3.1 De grondslagen toegelicht

Artikel 8a Wbp: ondubbelzinnige toestemming van de betrokkene

Wanneer toestemming de grondslag vormt voor gegevensdeling, moet die toestemming voldoen aan de eisen die de Wbp daaraan stelt. De toestemming dient een vrije, specifieke en op informatie berustende wilsuiting te zijn, waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.

Vrij

[13] P.C. Knol & G.J. Zwenne, Tekst en Commentaar Telecommunicatierecht, derde druk, Kluwer, p. 569

Het is van belang dat de betrokkene daadwerkelijk een vrije keuze heeft. Met andere woorden, aan weigering mogen geen negatieve gevolgen kleven voor de betrokkene. Immers, deze kunnen ertoe leiden dat de betrokkene toestemt enkel om deze gevolgen te vermijden.

Specifiek

De toestemming moet betrekking hebben op duidelijke en afgebakende doelen. “Wij verwerken uw gegevens in het belang van uw gezondheid en veiligheid” is onvoldoende specifiek.

Op informatie berustend

In het verlengde van het voorgaande ligt de eis dat de toestemming op informatie moet berusten. Als het voor de betrokkene volstrekt onduidelijk is wat er met zijn gegevens gebeurt, dan kan de betrokkene geen rechtsgeldige toestemming geven.

De grondslag toestemming kan in het kader van het veiligheidshuis alleen gebruikt worden voor vrijwillige trajecten. Alle trajecten waarbij drang of dwang aan de orde is, daarvan kunnen de bijbehorende verwerkingen niet op toestemming worden gebaseerd.

Artikel 8b Wbp: de gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is

Deze grondslag zal over het algemeen niet opgaan voor de veiligheidshuizen. Deze grondslag ziet op de uitvoering van contracten.

Artikel 8c Wbp: de gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is

Deze grondslag kan worden gebruikt wanneer er een wettelijke plicht is om gegevens te verwerken (bijvoorbeeld loonadministratie voor de Belastingdienst). Deze grondslag betreft een expliciete wettelijke plicht die is opgelegd aan de verantwoordelijke, niet een morele plicht die afgeleid wordt uit hogere wetgeving (zoals bijvoorbeeld de grondwet). Ook deze grondslag zal voor casusoverleg maar beperkt bruikbaar zijn.

Artikel 8d Wbp: de gegevensverwerking is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene

Wanneer gegevensverwerking nodig is om mensen te helpen die zich in een acuut levensbedreigende situatie bevinden of verwerking anderszins nodig is om een vitaal belang van de betrokkene te waarborgen, dan kan deze grondslag worden gebruikt. Hoewel veiligheidshuizen mensen met vaak grote problemen helpen, zal in de meeste gevallen deze grondslag toch niet opgaan omdat er niet door het gebruik van gegevens een direct (levens)gevaar wordt afgewend.

Artikel 8e Wbp: de gegevensverwerking is noodzakelijk voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt

Deze grondslag kan gebruikt worden door publiekrechtelijke organen (ministeries, uitvoeringsinstanties, OM, gemeenten) als voor de uitoefening van een aan hen opgedragen

wettelijke taak de verwerking van persoonsgegevens noodzakelijk is. Deze grondslag kan – afhankelijk van de situatie – worden toegepast door diverse ketenpartners.

Artikel 8f Wbp: de gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert

Om een beroep op deze grondslag te kunnen doen is het cruciaal dat de verwerking noodzakelijk is met het oog op het belang van de verantwoordelijke of een derde én het belang van degene van wie de gegevens worden verwerkt niet prevaleert. De verantwoordelijke dient voor zichzelf verschillende vragen te beantwoorden:

- Kan het doel dat met de verwerking wordt nagestreefd ook langs andere weg (zonder verwerking) worden bereikt?
- Worden alleen gegevens gebruikt die noodzakelijk zijn om het doel te bereiken?
- Wat is het belang dat de verwerking van persoonsgegeven rechtvaardigt?
- Wordt met de verwerking een inbreuk gemaakt op belangen of fundamentele rechten van degene wiens gegevens worden verwerkt en zo ja, dient dan - afhankelijk van de ernst van de inbreuk - gegevensverwerking niet achterwege te blijven?
- Is de verwerking evenredig aan het nagestreefde doel?[14]

Vanwege het technische juridische karakter van de grondslagen uit de Wbp raden wij aan om een interne of externe privacy specialist te raadplegen om te bepalen welke grondslag per soort casusoverleg toepasbaar is.

3.3.2 Grondslag en casus op maat

De Wbp vereist dat de grondslag voor de verwerking van persoonsgegevens voorafgaand aan de verwerking is vastgesteld. Hieruit vloeit voort dat vooraf helder moet zijn wat het doel is, wie de verantwoordelijke is, wat de voor het doel noodzakelijke gegevens zijn en wie de betrokken partijen zijn. In het kader van het casusoverleg in het verband van het veiligheidshuis, met name daar waar het gaat om maatwerk (casus op maat), zijn deze aspecten niet altijd op voorhand duidelijk vast te stellen. De reden hiervoor is dat een casus van triage tot overleg zich in de tijd ontwikkelt (opschaling, afschaling, betrekken nieuwe ketenpartners et cetera).

Wanneer het niet op voorhand duidelijk is welke persoonsgegevens worden verwerkt ten behoeve van welke doelen en met de betrokkenheid van welke partijen, dan zal per geval moeten worden beoordeeld of het verwerken en delen van gegevens rechtmatig is. Dit zal binnen het concept van casus op maat bij complexe multi-problematiek vaak het geval zijn. Wanneer de situatie van een casusoverleg (wezenlijk) verandert moet ook een nieuwe afweging worden gemaakt omtrent de proportionaliteit en subsidiariteit (en mogelijk ook grondslagen voor de verwerking). Dit is met name relevant wanneer een overleg wordt

[14] Wbp Naslag, hoofdstuk 2, artikel 8 sub f. Zie http://www.cbpweb.nl/wbpnaslag/2/paginas/wbp-artikel-8-f.aspx

uitgebreid met nieuwe ketenpartners, in het bijzonder wanneer het gaat om partijen buiten de zorg- en justitieketen (bijvoorbeeld woningbouwcorporaties of maatschappelijk werk organisaties).

Voordeel van de casus op maat aanpak is dat – in tegenstelling tot de gestandaardiseerde overlegstructuur – per procesfase wordt onderzocht welke partner noodzakelijk is voor het voortzetten van het overleg. Grote triagetafels en casusoverleggen waar vanaf het begin met veel partijen gegevens worden bekeken en gedeeld staan op gespannen voet met de privacywetgeving zolang niet helder is waarom elke partij inzage nodig heeft. Met behulp van het casus op maat principe kan per procesfase verantwoording worden afgelegd voor de aanwezige partners bij het casusoverleg. Dit komt de rechtmatigheid van de gegevens ten goede.

Het is begrijpelijk dat het voor het veiligheidshuis en de daarbinnen actieve ketenpartners met het oog op effectiviteit en efficiëntie niet goed mogelijk is om iedere aparte casus (extern) te laten toetsen op rechtmatigheid. Om toch telkens een goede privacyafweging te kunnen maken, zonder al teveel juridisch maatwerk, is het aan te bevelen om duidelijke criteria en werkprocessen op te stellen. Op basis van eenduidige werkprocessen en criteria kan makkelijker per geval worden beoordeeld of gegevens wel of niet gedeeld mogen worden. In de volgende paragrafen wordt hier nader op ingegaan.

3.4 Stel criteria vast voor triage en het op/afschalen van casus

Een belangrijk vraagstuk binnen ketensamenwerking en ketenoverleg in het kader van het veiligheidshuis is wanneer gegevens over een betrokkene mogen worden gedeeld en met wie. Uitgangspunt is dat gegevens alleen mogen worden verwerkt als dat noodzakelijk is en dan alleen met die partners wier betrokkenheid noodzakelijk is.

Door de criteria voor triage en het op/afschalen van casusoverleg te koppelen aan voor die beslissing noodzakelijke gegevens en betrokken partijen (met een onderscheid tussen DAT en WAT gegevens) kan voorkomen worden dat bovenmatig gegevens worden gedeeld (zie ook de volgende paragraaf). Wanneer te weinig gegevens beschikbaar zijn, of niet alle relevante partijen aan tafel zitten, kan besloten worden om het overleg uit te breiden.

Het vooraf opstellen van criteria creëert uniformiteit, gaat willekeur tegen en maakt dat eenvoudig verantwoording door medewerkers en ketenpartners kan worden afgelegd over de reden waarom de casus wel of niet in samenwerkingsverband is besproken. Deze aanpak is ook in lijn met de wens om te komen tot ‘casus op maat’.

3.5 Stel criteria vast voor gegevensdeling

Door duidelijk vast te leggen wanneer welke persoonsgegevens onderling mogen worden gedeeld, wordt onrechtmatige gegevensdeling voorkomen of beperkt, en rechtmatige gegevensdeling bevordert. Met name wanneer het veiligheidshuis of (keten)partners niet op de hoogte zijn over wanneer het onderling delen van (gevoelige) persoonsgegevens is toegestaan, kan het voorkomen dat gegevensdeling uitblijft uit angst dat dit onrechtmatig is. Dit is niet in het belang van de samenwerking. Door duidelijke criteria op te stellen, waarmee de gegevensdeling rechtmatig is als aan die criteria is voldaan, kan deze onzekerheid worden weggenomen. Voorts kan met deze zelfde criteria worden voorkomen dat niet de juiste, of te veel gegevens onderling worden gedeeld.

Houd er rekening mee dat de privacyregels die van toepassing zijn op de gegevens in principe van de verstrekkende organisatie 'overgeërfd' worden naar het samenwerkingsverband. De gegevens mogen bijvoorbeeld niet voor andere doeleinden worden gebruikt dan waarvoor zij zijn verstrekt binnen het samenwerkingsverband. Ook moet een vergelijkbaar niveau van beveiliging worden gehanteerd.

3.6 Stel de procesinrichting vast

Het is raadzaam het proces van intake, triagering, op- en afschaling en casusoverleg expliciet te beschrijven. Deze beschrijving is behulpzaam bij het per processtap bepalen of persoonsgegevens nodig zijn, waar de gegevens voor nodig zijn, welke gegevens dit zijn, wie de processtap uitvoert en met welke partijen gegevens worden gedeeld.

Het proces van gegevensverwerking visueel inzichtelijk maken geeft houvast bij het volgen van gegevensstromen en maakt het voor (nieuwe) partners eenvoudiger de juiste koers te bepalen.

Vragen die als leidraad kunnen dienen voor de procesinrichting:

- Hoe wordt een casus aangemeld en wanneer komt deze casus bij het veiligheidshuis terecht?
- Hoe worden intake en triagering vormgegeven en welke partijen zijn daarbij betrokken?
- Wanneer worden welke ketenpartners betrokken bij de triagering?
- Wat zijn de criteria voor het opstarten/opschalen/afschalen van een bepaald type casusoverleg?
- Waar wordt bepaald welke ketenpartners moeten worden betrokken in het casusoverleg?
- Wie van de ketenpartners kan gegevens inzien tijdens het casusoverleg?
- Wie van de ketenpartners kan gegevens aanvullen/corrigeren/verwijderen?
- Wordt de betrokkene geïnformeerd en zo ja, wanneer en door wie?

3.7 Stel een privacyconvenant op

Om privacy binnen de ketensamenwerking te waarborgen, is het belangrijk dat ook de ketenpartners privacy op een verantwoorde manier binnen hun organisatie beleggen. Om ervoor te zorgen dat ketenpartners op verantwoorde wijze omgaan met de gegevens die binnen het kader van het veiligheidshuis worden gedeeld kan een privacy convenant worden opgesteld. Een privacyconvenant bevat afspraken tussen het veiligheidshuis en de verschillende ketenpartners over de gewenste omgang met persoonsgegevens. Daarnaast geeft een dergelijk convenant invulling aan de vereisten van de Wbp. Wanneer een privacy-convenant door ketenpartners wordt getekend, verplichten zij zich aan de bepalingen die daarin zijn opgenomen te houden. Hiermee wordt uniformiteit van verwerkingen gecreëerd.

Door het initiatief te nemen met betrekking tot het opstellen van het privacy convenant, of duidelijke eisen hiervoor te stellen, kan het veiligheidshuis invloed uitoefenen op de manier waarop bij ketenpartners met (gedeelde) persoonsgegevens wordt omgegaan. Zo kunnen bijvoorbeeld minimale beveiligingsmaatregelen worden afgedwongen. Dit versterkt het vertrouwen van het veiligheidshuis en de ketenpartners onderling dat op een zorgvuldige manier met gedeelde gegevens wordt omgegaan. Dit vertrouwen helpt gegevensdeling te bevorderen.

In tegenstelling tot een samenwerkingsconvenant, waarin afspraken over de wijze van samenwerking zijn opgenomen, richt een privacyconvenant zich op de manier waarop met persoonsgegevens moet worden omgegaan. Het is ook mogelijk de elementen van beide afzonderlijke convenanten te combineren tot één privacy- en samenwerkingsconvenant.

Let wel op: een convenant kan geen wetgeving vervangen of nieuwe wettelijke bevoegdheden creëren. Een convenant is enkel een afspraak tussen de tekenende partijen, waarmee zij zich verbinden zich aan die afspraak te houden. Een wettelijke verplichting die aan een partij is opgelegd kan niet via een convenant worden omzeild. Wanneer in een convenant bijvoorbeeld afspraken zijn vastgelegd over het gebruik van het BSN van een betrokkene, terwijl dit gebruik op grond van de Wbp niet is toegestaan, prevaleert het in de wet bepaalde. Wel kunnen in een convenant consequenties worden verbonden aan het niet voldoen aan de daarin gemaakte afspraken. Deze consequenties zijn bindend voor iedereen die het convenant heeft ondertekend.

3.8 Documenteer de gegevensverwerkingen

Documenteer de gegevensverwerkingen die geïnventariseerd zijn. Wanneer nieuwe verwerkingen worden gedaan, dan moeten deze verwerkingen ook worden gedocumenteerd. Gegevensverwerkingen kunnen bijvoorbeeld worden vastgelegd in Excel sheets, Word documenten, databases en speciaal daarvoor ontwikkelde softwareprogramma's.

Het documenteren van gegevensverwerkingen is noodzakelijk om verantwoording af te kunnen leggen. In de aankomende Europese Verordening Gegevensbescherming is het documenteren van verwerkingen daarnaast verplicht gesteld. Wanneer gegevens worden verwerkt moeten op grond van de Verordening Gegevensbescherming in ieder geval de volgende aspecten van de verwerking worden gedocumenteerd:

- het doel van de verwerking;
- de grondslag voor de verwerking;
- de motivering van deze grondslag;
- de voor de verwerking verantwoordelijke entiteit;
- de gebruikte gegevens.

Verder is het belangrijk dat de documentatie up-to-date is en direct op verzoek aan de toezichthouder kan worden verstrekt.

3.9 Maak inzage, correctie en verwijderingsprocedures

Op grond van de Wbp heeft de betrokkene een aantal rechten die deze kan inroepen met betrekking tot de verwerking van zijn of haar persoonsgegevens. Meer specifiek gaat het om het recht op inzage en het recht op correctie en verwijdering.

Het inzagerecht geeft de betrokkene het recht om bij de verantwoordelijke een verzoek te doen om mee te delen welke persoonsgegevens over hem worden verwerkt. De verantwoordelijke heeft de plicht om binnen vier weken schriftelijk mee te delen of er persoonsgegevens over hem worden verwerkt.[15] Indien dat het geval is, moet hij een

[15] Artikel 35, lid 1, Wbp.

volledig overzicht van de verwerkte persoonsgegevens meezenden. Dit overzicht moet, in begrijpelijke vorm, bevatten:

- een omschrijving van het doel of de doeleinden voor de verwerking;
- de categorieën gegevens waarop de verwerking betrekking heeft;
- de ontvangers of categorieën ontvangers van de gegevens; en
- beschikbare informatie over de herkomst van de gegevens. [16]

In reactie op een inzageverzoek heeft de betrokkene op grond van de Wbp recht op correctie en/of verwijdering. De betrokkene kan het veiligheidshuis verzoeken (op hem of haar betrekking hebbende persoonsgegevens) te verbeteren, aan te vullen, te verwijderen, of af te schermen. Er kunnen echter goede redenen zijn om gegevens niet aan te passen (bijvoorbeeld omdat ze wel kloppen, maar de betrokkene onwelgevallig zijn) of te verwijderen, zoals de bescherming van rechten en vrijheid van anderen.[17]

Het veiligheidshuis en/of haar ketenpartners (afhankelijk van wie de verantwoordelijke voor de gegevensverwerking is) moeten procedures opstellen om invulling te geven aan inzage-, correctie- en verwijderingsverzoeken. Vaste procedures zorgen voor compliance en zekerheid voor de medewerkers die met dergelijke verzoeken worden geconfronteerd, omtrent de manier waarop aan dergelijke verzoeken moet worden voldaan.

Een dergelijke procedure moet de volgende elementen bevatten:

- Een portaal waar de betrokkene terecht kan (website, email adres, postadres);
- Regels omtrent het vaststellen van de identiteit van de betrokkene;
- Een duidelijk proces om de gegevens te verzamelen en te communiceren;
- Controle dat dit binnen de gestelde termijn gebeurt (28 dagen);
- Motivering van afwijzingen van de verzoeken.

3.10 Bepaal bewaartermijnen

Het veiligheidshuis en/of haar ketenpartners (afhankelijk van wie de verantwoordelijke voor de gegevensverwerking is) moeten bij het verzamelen van de gegevens de daarvoor geldende 'bewaartermijn' vaststellen.

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld.[18] In sommige gevallen is de bewaartermijn voor de verwerking van persoonsgegevens wettelijk vastgesteld. Voor het overgrote deel van de gegevens zijn echter geen vaste bewaartermijnen vastgesteld. Het is een taak van de verantwoordelijke om voorafgaand aan de verwerking van persoonsgegevens de bewaartermijn af te stemmen op de doeleinden waarvoor zij worden verwerkt. Per doel en situatie kan de noodzakelijke verwerkingsperiode - en dus bewaartermijn - verschillen.

Na afloop van de bewaartermijn dienen de persoonsgegevens te worden geanonimiseerd of vernietigd.

---

[16] Artikel 35, lid 2, Wbp.
[17] Weigering van een verzoek op inzage, correctie of verwijdering kan alleen op grond van één van de redenen van artikel 43 Wbp.
[18] Artikel 10 Wbp.

4 Privacycultuur en bewustzijn

Procedures zijn niets waard als ze niet worden begrepen en (goed) gevolgd. Een belangrijke waarborg voor een zorgvuldige omgang met persoonsgegevens in de praktijk is de bedrijfscultuur: hoe wordt privacy op dagelijkse basis gemanaged? Hierbij moet niet alleen worden gekeken naar de bedrijfscultuur in het veiligheidshuis zelf, maar ook in relatie tot de (keten)partners.

Privacy als onderdeel van de bedrijfscultuur betekent dat iedereen in het veiligheidshuis en bij de ketenpartners zich bewust is van privacy wanneer zij persoonsgegevens verwerken. Door kennis en bewustwording over privacy te vergroten worden privacy inbreuken tegengegaan. Verder kan kennis over toegestane verwerkingen (waaronder het delen van persoonsgegevens met derden) ervoor zorgen dat rechtmatige gegevensdeling wordt bevorderd. Ongegronde angsten en onzekerheden die nu bij ketenpartners leiden tot het niet delen van gegevens kunnen zo worden weggenomen.

Het veiligheidshuis moet een plan opstellen om het privacybewustzijn te vergroten. Een onderdeel hiervan is het actief communiceren van het privacybeleid en ondersteuning bieden bij de uitvoering hiervan. Dit kan bijvoorbeeld door het opzetten van workshops, interne trainingen of colleges over privacy. Naast bijeenkomsten kunnen medewerkers ook gefaciliteerd worden door privacyhulpmiddelen als checklists, ‘Frequently Asked Questions’ en informatiefolders over privacybeleid. Deze voorlichting kan worden aangeboden aan nieuwe medewerkers en partners, maar ook als terugkerende thema-activiteit. Daarnaast kan een privacy officer (als deze is aangesteld) dienen als vast aanspreekpunt voor vragen of opmerkingen van medewerkers.

5 Veiligheid

Een doelbewuste inrichting van de beveiliging van persoonsgegevens maakt deel uit van de privacy governance van het veiligheidshuis. De verantwoordelijke is verplicht passende 'technische en organisatorische maatregelen' te nemen om diefstal of verlies van persoonsgegevens te voorkomen.[19] Om een inschatting te kunnen maken van een passend niveau van beveiliging dient naar een aantal zaken te worden gekeken, te weten: 1) de stand van de techniek, waarbij wordt gekeken naar de huidige technische mogelijkheden voor het beveiligen van gegevens 2) de kosten voor de tenuitvoerlegging van de beveiligingsmaatregelen en 3) de risico's die de verwerking met zich meebrengen.

De wetgever verplicht niet dat altijd de zwaarst mogelijke beveiliging moet worden toegepast. Bij de beveiliging van persoonsgegevens is het belangrijk dat de te treffen maatregelen worden afgestemd op bedreigingen die realistisch zijn, gezien de aard van de persoonsgegevens in relatie tot de omvang en de verwerkingen daarvan. Hierdoor kan het 'risico van verlies of onrechtmatige verwerking' tot een aanvaardbaar niveau worden beperkt. Daarnaast dienen de genomen maatregelen er mede op te zijn gericht onnodige verwerkingen van persoonsgegevens te voorkomen.

Beveiliging is niet alleen iets van de IT-afdeling. Beveiliging moet binnen de gehele organisatie zijn belegd, van werknemers tot aan het management van het veiligheidshuis. Door een duidelijk beleid omtrent beveiliging te formuleren kunnen risico's worden beperkt of zelfs voorkomen.

Beveiligingsproblemen die resulteren in datalekken kunnen grote invloed hebben op de reputatie van de veiligheidshuizen. Daarnaast kunnen door de toezichthouder in de nabije toekomst fikse boetes worden opgelegd wanneer een datalek is geconstateerd en de beveiliging onvoldoende blijkt te zijn geweest. Voorts is de wetgever momenteel bezig met een nieuwe wet waarbij een verplichting wordt ingevoerd om melding te doen van datalekken bij de toezichthouder en eventueel bij de betrokkene.

5.1 Stel een beveiligingsbeleid vast

Een apart document waarin eisen worden gesteld aan de beveiliging van de persoonsgegevens in het veiligheidshuis draagt bij aan de compliance en risico-beperking van de gegevensverwerking. In dit document moet worden beschreven welke maatregelen moeten worden genomen om verlies of diefstal van de gegevens te voorkomen. Denk hierbij aan maatregelen die door de IT-afdeling moeten worden genomen en maatregelen die werknemers moeten nemen of procedures die zij moeten volgen.

5.2 Werk het beleid uit in concrete maatregelen

Op basis van het beleid moet een goede informatiebeveiliging worden ingericht. Het gaat te ver om deze in deze handreiking te beschrijven. Voor wat betreft de informatiebeveiliging kan worden aangesloten bij de *Richtsnoeren beveiliging van persoonsgegevens* van het Cbp, de *Code voor Informatiebeveiliging* (de ISO 27001 standaard) en het *Voorschrift*

[19] Artikel 13 Wbp.

Informatiebeveiliging Rijksdienst (een standaard voor de rijksoverheid, maar ook heel nuttig voor lagere overheden en andere organisaties).

Aan werknemers kunnen ook specifieke maatregelen worden opgelegd, zoals het verplicht stellen van een gebruikersnaam en een wachtwoord, waarbij criteria worden gesteld aan de moeilijkheidsgraad van het wachtwoord. Andere concrete maatregelen waaraan kan worden gedacht zijn

- Het verbieden om documenten mee naar huis te nemen;
- Verbieden om gebruik te maken van persoonlijke e-mail voor het versturen van documenten die persoonsgegevens bevatten;
- Verbieden zulke documenten in openbare cloud-services zoals Dropbox of Google Drive.

Verder kunnen procedures worden opgesteld voor meer risicovolle verwerkingen (zoals het raadplegen van de intern verantwoordelijke bij de verwerking van bijzondere persoonsgegevens).

5.3 Stel een incident response plan op

Wanneer onverhoopt toch een inbreuk in de beveiliging is geconstateerd, is het belangrijk een plan van aanpak te hebben. Een dergelijk plan wordt aangeduid met de term ‘incident response plan’.

Met behulp van een Incident Response plan wordt duidelijkheid geschapen over de stappen die door de verschillende betrokken partijen moeten worden genomen in geval van een beveiligingsinbreuk of datalek. Hiermee wordt voorkomen dat veel kostbare tijd verloren gaat, verkeerde aannames worden gedaan en verschillende (of onjuiste) boodschappen worden verkondigd aan de buitenwereld.

Vragen die bij het opstellen van een incident response plan als leidraad kunnen dienen zijn:

- Welke afdelingen heb ik nodig wanneer een beveiligingslek zich heeft voorgedaan? (IT, management, communicatie, juridisch et cetera)
- Welke (risico-beperkende) maatregelen moeten worden genomen?
- Hoe communiceren we naar de buitenwereld over het lek?
- Moet ik het lek melden bij de toezichthouder?
- Moet ik het lek melden bij de betrokkene?

6 Nieuwe casusoverleggen

In de praktijk kan het voorkomen dat het veiligheidshuis na verloop van tijd nieuwe soorten casusoverleggen moet faciliteren. Hierbij rijst de vraag of het gebruik van reeds door het veiligheidshuis of ketenpartners verwerkte gegevens in deze nieuwe casusoverleggen toelaatbaar is.

Doorslaggevend voor het beantwoorden van deze vraag is of het gebruik van eerder verwerkte persoonsgegevens in dit nieuw soort casusoverleg verenigbaar is met het oorspronkelijke doel waarvoor de gegevens zijn verzameld. Wanneer het gebruik verenigbaar is met het oorspronkelijke doel van de verwerking door het veiligheidshuis of de ketenpartners, kunnen reeds verzamelde gegevens worden gebruikt (zie paragraaf 3.2).

Wanneer het gebruik van reeds verwerkte persoonsgegevens in het nieuwe casusoverleg niet verenigbaar is met het oorspronkelijke doel dat door de veiligheidshuizen is vastgesteld voor de werkzaamheden die zij tot dan toe hebben verricht, is het gebruik van de gegevens niet toegestaan. In dat geval moet voor deze nieuwe casusoverleggen een zelfstandig doel worden bepaald. De rechtmatigheidstoets moet voor dit nieuwe doel dan ook worden gedaan.

Het is niet voldoende om de paraplu van de oorspronkelijke doelbinding te veranderen, dan wel op te rekken, waardoor de nieuwe casusoverleggen hieronder geschaard kunnen worden (zie paragraaf 3.1). Het is daarom aan te raden bij ieder nieuw casusoverleg een privacy-analyse uit te voeren om na te gaan of de voorgenomen verwerkingen, waaronder het gebruik van reeds voorhanden zijnde gegevens, is toegestaan.

7 Transparantie

7.1 Definieer een extern privacybeleid en communiceer dit

Om verantwoording af te leggen aan de buitenwereld en duidelijkheid te geven over de omgang met persoonsgegevens moet een extern privacybeleid worden gecommuniceerd. Dit kan bijvoorbeeld via een 'privacy statement'. Een privacy statement is een document waarin wordt uitgelegd op welke wijze het veiligheidshuis met privacy en persoonsgegevens omgaat. In een privacy statement komt minimaal aan de orde:

- wie de verantwoordelijke voor de gegevensverwerking is;
- welke persoonsgegevens worden verwerkt;
- met welk doel deze worden verwerkt; en
- op welke grondslag de verwerking is gebaseerd.

Daarnaast is het privacy statement een goede plek om informatie te geven over de rechten van de betrokkene en alle andere informatie die het vertrouwen in een goede omgang met persoonsgegevens rondom het veiligheidshuis versterkt.

7.2 Geef invulling aan de informatieplicht naar de betrokkene toe

Het is de plicht van de verantwoordelijke om uit eigen beweging informatie over de gegevensverwerking aan de betrokkene te verstrekken. Wanneer de verantwoordelijke gegevens (laat) verzamelen bij de betrokkene zelf, dan moet hij de betrokkene direct informeren over het doel van de verwerking. Alleen in die gevallen waar de betrokkene al op de hoogte is, kan de informatieverstrekking achterwege blijven. Wanneer de verantwoordelijkheid bij verschillende partijen ligt, moet duidelijk worden afgesproken welke partij naar de betrokkene toe optreedt als primair aanspreekpunt.

De omvang van de informatieplicht is niet verder uitgewerkt in de Wbp, behalve dat de informatie minimaal de identiteit van de verantwoordelijke en het doel van de verwerking moet omvatten.[20] Verder moet de verantwoordelijke nadere informatie verstrekken "voor zover dat gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen".[21] Het wordt daarom wel betoogd dat betrokkene ook geïnformeerd dient te worden over of dan wel hoe de verantwoordelijke invulling geeft aan de vereisten van de Wbp, zoals de rechten van de betrokkene, de beveiliging en de kwaliteit van de persoonsgegevens. Een manier voor de verantwoordelijke om invulling te geven aan de informatieplicht naar de betrokkene toe is door middel van het opstellen van een informatiefolder waarin alle bovenstaande elementen worden meegenomen.

Communicatie naar de betrokkene over het feit dat deze wordt besproken in het veiligheidshuis is niet altijd wenselijk of in het belang van het casusoverleg. Door hier voorafgaand afwegingen voor op schrift te stellen, kan voor ieder casusoverleg worden

[20] Artikel 33, lid 2, Wbp.
[21] Artikel 33, lid 3, Wbp.

bepaald of communicatie wel of niet moet plaatsvinden en kan in gevallen waarin niet gecommuniceerd wordt duidelijk verantwoording hierover worden afgelegd.

7.3 Melding bij het College bescherming persoonsgegevens

In het kader van de transparantie van gegevensverwerkingen dienen deze in veel gevallen te worden gemeld bij de toezichthouder voor gegevensbescherming in Nederland, het College bescherming persoonsgegevens (Cbp).[22]

Wanneer de verantwoordelijke een Functionaris voor de gegevensbescherming (FG) heeft, dan moet de melding bij de FG worden gedaan. Verwerkingen die zijn vrijgesteld van melding op grond van het Vrijstellingsbesluit, hoeven in het geheel niet te worden gemeld.[23] Het Cbp heeft een handreiking bij het Vrijstellingsbesluit Wbp opgesteld dat helpt beoordelen of een verwerking van persoonsgegevens is vrijgesteld van melding.[24]

De verantwoordelijke moet zelf beoordelen of de verwerking van persoonsgegevens moet worden gemeld. Bij twijfel raadt het Cbp aan om de verwerking te melden. Het is ook de verantwoordelijkheid van de verantwoordelijke om de melding op een juiste en volledige wijze te doen. Het niet of onvolledig doen van melding kan een strafbaar feit opleveren (artikel 75 Wbp).

Het meldingenregister van het Cbp is openbaar en online raadpleegbaar.[25] Melding kan via een online programma, of een te downloaden en printen formulier worden gedaan. Dit formulier is voorzien van een invulhandleiding.[26]

Houd er rekening mee dat een melding bij het Cbp niet betekent dat de verwerking legitiem is, of is goedgekeurd door het Cbp!

[22] Artikel 27 Wbp.
[23] Vrijstellingsbesluit Wbp.
[24] Cbp, Handreiking Vrijstellingsbesluit Wbp, via http://www.cbpweb.nl.
[25] Cbp, Wbp-meldingenregister, via http://www.cbpweb.nl.
[26] Cbp, 'Meldingsprogramma verwerking persoonsgegevens', via http://www.cbpweb.nl/Pages/ind_melden_programma.aspx.

8 Monitoring en handhaving

Ten slotte is het belangrijk dat invulling wordt gegeven aan de onderdelen monitoring en handhaving van een privacy governance plan. Dit is de laatste stap in het uitvoeren van een privacy governance programma, waarbij de inventarisatie uit paragraaf 8.2 als begin kan dienen als beginpunt van het verder optimaliseren van het privacy governance plan. Deze handreiking kan daarmee als terugkerend cyclisch proces worden doorlopen (zie Deel 1).

8.1 Handhaaf het privacy beleid

Beleid en procedures zijn niet effectief als geen gevolg wordt gegeven aan het niet-nakomen ervan. Daarom moet ook worden nagedacht over de wijze waarop invulling wordt gegeven aan handhaving, zowel in het veiligheidshuis als in de relatie met (keten)partners. Adequate handhaving onderstreept het belang van privacy en gegevensbescherming in en rondom het veiligheidshuis.

Handhaving kan plaatsvinden in allerlei vormen. Van het benoemen en evalueren van incidenten in functioneringsgesprekken en berispingen, tot (tijdelijke) uitsluiting van gegevensdeling bij herhaaldelijke handelingen in strijd met het privacy beleid.

Wil handhaving van het beleid überhaupt mogelijk zijn, dan moet wel duidelijk zijn voor de medewerkers (intern) en voor de ketenpartners (extern) wat de regels zijn. Zonder heldere regels kan niet worden verwacht van medewerkers en ketenpartners dat zij zich aan de afspraken houden. Hierbij is het ook van belang dat de regels voor iedereen logisch, begrijpelijk en uitvoerbaar zijn. Wanneer de regels te ingewikkeld of te streng zijn, dan zal weerstand ontstaan tegen het privacybeleid.

8.2 Monitor het privacy programma

Afspraken, waarborgen en afbakeningen, al dan niet vastgelegd in procedures, moeten in de praktijk correct worden toegepast. De verantwoordelijke voor het privacy beleid (zie paragraaf 3.2) moet toezicht houden op de naleving hiervan door medewerkers en ketenpartners en waar nodig handhavend optreden.

Daarnaast kan door deze verantwoordelijke periodiek worden nagegaan of het beleid in de praktijk werkbaar is. Het is aan te raden klachten en opmerkingen over of problemen met bestaand beleid te inventariseren. De verantwoordelijke kan de resultaten van een dergelijke inventarisatie rapporteren aan het management. Het management kan besluiten of procedures of beleid moeten worden aangepast om deze beter te laten aansluiten bij de praktijk en kan nagegaan op welke onderdelen extra aandacht is vereist met betrekking tot bescherming van privacy en hier de middelen voor vrij maken.

Ook veranderingen in wet- en regelgeving die van toepassing is op de gegevensverwerking in het veiligheidshuis moeten worden bijgehouden om na te gaan of bestaande processen en beleid moeten worden aangepast.