centrum informatiebeveiliging en privacybescherming

Grip op Privacy

Privacy Governance

Een handleiding voor de implementatie en borging van privacy in organisaties

14 augustus 2020 - Versie 3.2

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan echter voorkomen dat er toch sprake is van omissies, onjuistheden en/of gedateerdheid. Het is altijd de verantwoordelijkheid van de lezer zelf dit te beoordelen en desgewenst te corrigeren indien hij zich baseert op of gebruik maakt van een CIP-publicatie.

© Centrum Informatiebeveiliging en Privacybescherming.
Voor dit werk geldt een Creative Commons Naamsvermelding GelijkDelen 4.0 licentie, verleend door het CIP. Zie https://creativecommons.org/licenses/by-sa/4.0/

Colofon

Titel	Privacy Governance - Een handleiding voor de implementatie en borging van privacy in organisaties
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming
Status	Versie 3.2 Becommentarieerde praktijk, zie: https://cip-overheid.nl/totstandkoming
Auteur	Marcel Koers; eindredactie: Ruud de Bruijn
Bijdragen en review	Leden van de CIP Domeingroep Privacy, Elleke Oosterwijk, Ruud de Bruijn
Datum	14 augustus 2020
Filenaam	20200814 Handleiding Privacy Governance v3_2.docx
Download	https://cip-overheid.nl

Considerans

CIP-producten steunen op kennis van mensen uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt.

Opmerkingen, inhoudelijk of redactioneel commentaar bij deze uitgave kun je melden op https://www.cip-overheid.nl/contact/.

Wij stellen suggesties en ideeën voor verbetering of doorontwikkeling zeer op prijs.

Inhoud

Voorwoord: privacy als verstandige bedrijfsvoering 5

Leeswijzer: opzet van het document 6

Deel 1: Privacygovernance 8

1 Inleiding: aan het management 8

2 Privacygovernance 10

2.1 Privacy vanuit veranderperspectief 10

2.2 Privacy Volwassenheidsmodel 12

2.3 Groei, de ACT-doelen en het ACT-team 12

2.4 Het slim kiezen van de incrementen per proces 16

2.5 Vinger aan de pols: risicoanalyse (DPIA) en selfassessment (PriSa). 17

2.6 Groeien in volwassenheid: wat kost het? 18

2.7 De grootte van de organisatie 18

2.8 Kritische succesfactoren: COBIT 19

3 Het privacybeschermingsprogramma als veranderprogramma 20

3.1 Kritische succesfactoren algemeen: samenhang 21

3.2 Kritische succesfactoren in het beleidsdomein 24

3.3 Kritische succesfactoren in het uitvoeringsdomein 27

3.4 Kritische succesfactoren in het control-/beheerdomein 32

Deel 2: Toelichtingen 36

4 Toelichting op het toepassen van de Privacy Baseline 37

4.1 Privacy beleid - B.01 37

4.2 Organisatorische inbedding - B.02 40

4.3 Risicomanagement - B.03 42

4.4 Vastleggen doel gegevensverwerking - U.01 43

4.5 Gegevensmanagement - U.02 44

4.6 Kwaliteitsmanagement - U.03 45

4.7 Doorgifte van persoonsgegevens - U.07 45

4.8 Intern toezicht - C.01 46

5 Toelichting op verandermanagement 48

5.1 Slim implementeren van privacy 48

5.2 Veranderen gaat niet vanzelf 53

5.3 Het ACT-team en de organisatie als één team 60

Referenties 65

Bijlage 1: Grip op privacy 69

Bijlage 2: De ACT-doelen 71

Voorwoord: privacy als verstandige bedrijfsvoering

Toen in het voorjaar van 2017 de eerste concepten van dit document werden besproken, begon 'privacy' meer dan voorheen bij een breder publiek de aandacht te trekken. Dat kwam vooral door toedoen acties in onder meer het Europese parlement en een Britse Lagerhuiscommissie naar aanleiding van een aantal fikse schandalen en het ongrijpbare gedrag van de grote dataverzamelaars annex - wederverkopers als Google, Apple, Facebook en dergelijke. De toen nog in de maak zijnde Algemene Verordening Gegevensbescherming (AVG) en de latere Nederlandse Uitvoeringswet (de UAVG) zijn er een direct gevolg van [1][2]. Nederland bracht, nog juist voor de komst van de AVG, de Meldplicht Datalekken in 2016 het onderwerp 'privacy' als issue ineens dicht bij huis: bedrijven, organisaties, verenigingen en kleine zelfstandigen moesten vrezen voor boetes als zij hun privacybescherming niet op orde hadden.

Voldoen aan privacywetgeving *omdat er privacywetgeving is* kan gemakkelijk uitgelegd worden: wetsbepalingen zijn concrete aanwijzingen waarop een organisatie maatregelen kan inzetten en iedereen begrijpt dat eventuele boetes en imagoschade een organisatie geen goed doen. Voldoen aan privacywetgeving *omdat het een principieel wereldwijd grondrecht van je klanten betreft*, is toch nog iets anders. Hoe krijg je het privacy-gedachtegoed als een onbetwiste vanzelfsprekendheid in het DNA van je bedrijf, in de genen van je werknemers? En hoe hou je vervolgens iedereen, en ook de nieuwelingen, enthousiast en voortdurend 'aware'?

Ondertussen zijn we anno 2020 wel vertrouwd met termen als 'privacy by design' en 'by default', en zien we er zelfs ook de bedrijfsmatige voordelen van. Maar dat was in 2017, zeker in den brede, nog niet zo. 'Privacy' was zelfs wat mysterieus en ongrijpbaar: wat is het precies en hoe regel je zoiets? Achteraf kunnen we zeggen: door je organisatie ook privacy-minded by design en by default te maken. En hoe doe je zoiets? Daarover gaat deze handleiding.

In de serie 'Grip op privacy' dient de Privacy Baseline [3] als basis en leidraad voor het voldoen aan de wettelijke vereisten voor het verwerken van persoonsgegevens. Privacy Governance vult dat aan vanuit het perspectief van de implementatie en borging van privacy als verstandige bedrijfsvoering. Voor directie, managers en beïnvloeders in bedrijven en organisaties.

Zoals alle documenten en producten in de reeks 'Grip op Privacy' is ook deze handleiding tot stand gekomen door nauwe samenwerking met en tussen verschillende partijen en personen uit het CIP-netwerk. Hun bijdragen, reviews en commentaren geven de auteurs het vertrouwen dat de methode 'Grip op privacy' voldoende draagvlak heeft voor een brede toepassing en verdere ontwikkeling.[1]

De auteurs danken iedereen die op enigerlei wijze een bijdrage hebben geleverd aan het samenstellen van dit document.

[1] Voor een korte video over de productlijn 'Grip op privacy', ga naar https://cip-overheid.nl/productcategorie%C3%ABn-en-worshops/producten/privacy-bescherming/.

Leeswijzer: opzet van het document

Dit document laat zien hoe organisaties privacy kunnen organiseren, laten groeien en borgen. Dit geheel van managementprocessen verstaan we doorgaans onder de term 'governance'.

Het is natuurlijk niet de bedoeling hier de theorieën over bedrijfsvoering en verandermanagement te bespreken. Wel is geprobeerd, met name in Deel 2, om in aanmerking komende uitgangspunten hier specifiek in het licht te stellen van de implementatie van privacy in de organisatie.

Dit document beschrijft hoe zij, die verantwoordelijk zijn voor het op orde brengen van de privacymanagementprocessen, deze verantwoordelijkheid samen met de bestaande organisatie effectief en efficiënt kunnen vormgeven. Het gaat over samenwerking tussen de betrokken stakeholders en de staande organisatie. Niet door het afdwingen ervan, maar door de betrokken partijen in hun kracht te zetten en ervoor te zorgen dat de juiste verantwoordelijkheden bij de juiste personen komen te liggen.

We zijn niet helemaal gelukkig met de term hand*leiding*: dat klinkt al snel te resoluut. Het gaat immers over gedrag van mensen in organisaties, en daarbij spelen oneindig veel variabelen een rol. Maar we weten niet direct een alternatief dat toch een beetje in lijn blijft met de overige publicaties in Grip op Privacy. Laat dit document een inspiratiebron en hulp zijn om op ideeën te komen, tips en trucs op te doen, een doel en koers te bepalen en daar een kansrijke uitvoering aan te geven.

De *Handleiding Privacy Governance* bestaat uit 2 delen:

1. Privacygovernance.

   Het zwaartepunt van Deel 1 is hoofdstuk 3: Het privacybeschermingsprogramma als veranderprogramma. Daarin worden de puntsgewijs de kritische succesfactoren benoemd voor het inrichten van privacy in de organisatie vanuit een organisatie-veranderperspectief en het proactief gebruik van het Privacy Volwassenheidsmodel [5] daarbij. Om de succesfactoren goed te kunnen plaatsen gaat Deel 1 ook (kort) in op de achtergrond en context van waaruit de veranderstrategie en de succesfactoren zijn gekozen.

2. Toelichtingen.

   Deel 2 geeft nadere toelichting en verdieping:

   - In hoofdstuk 4 vind je toelichtingen en uitbreidingen bij de kritische succesfactoren in relatie tot de Privacy Baseline.
   - Hoofdstuk 5 is gewijd aan verandermanagement in het teken van de groei naar privacyvolwassenheid.

Bij deze versie

De veranderingen in deze versie ten opzichte van de versie 3.1 zijn vooral cosmetisch en redactioneel van aard. De styling is aangepast aan de actuele templates die CIP nu gebruikt voor zijn publicaties, er is onderhoud gepleegd (toegankelijkheid, foutherstel, suggesties van gebruikers, referenties en links zijn nagelopen) en de inleidende teksten zijn waar nodig enigszins herzien.

Inhoudelijk gezien is de toevoeging van een verwijzing naar de hulpproducten van CIP ten aanzien van inkoop (zie paragraaf 4.3.2: Hulp bij inkoop, in Deel 2) de enige aanpassing van betekenis.

Over CIP

CIP is het Centrum voor informatiebeveiliging en privacybescherming van, voor en door overheidsorganisaties. Het is opgericht voor informatie-uitwisseling en kennisdeling ter verbetering van de informatieveiligheid van de overheidsdienstverlening en heeft zich ontwikkeld tot een publiek-private netwerkorganisatie, waarin ook gespecialiseerde marktorganisaties als kennispartners deelnemen. Kennis die in de aangesloten organisaties aanwezig is op het vlak van informatiebeveiliging en privacybescherming wordt binnen de samenwerking in CIP-verband op verschillende manieren gedeeld en toegankelijk gemaakt. Voldragen producten worden op de publieke site van het CIP gepubliceerd.

Door meer samen te doen en zo mogelijk te uniformeren draagt het CIP ook bij aan het optimaal gebruik van overheidsmiddelen.

De publicaties van het CIP worden in principe *om niet* ter beschikking gesteld en kunnen, met inachtneming van de voorwaarden van Creative Commons Naamsvermelding/Gelijk Delen, vrijelijk gebruikt worden, zie voor de licentievoorwaarden: https://creativecommons.org/licenses/by-sa/3.0/nl/.

Deel 1: Privacygovernance

1 Inleiding: aan het management

Niet alleen bij organisaties en bedrijven[2], vanwege de aangescherpte verplichtingen, maar ook breed maatschappelijk is 'privacy' een veelbesproken thema geworden. Het heeft zich ontworsteld aan het imago van door activisme opgeworpen hinderlijke bijkomstigheid voor organisaties die persoonsgegevens verwerken. Waar de aandacht aanvankelijk vooral uitging naar het risico op reputatieschade, mogelijke vervolging, boetes en schadeclaims, wordt goede privacyborging nu steeds meer gezien als onderdeel van excellente dienstverlening en welbewust ingezet als marketingstrategie die vertrouwen wint bij klanten en stakeholders. Deze handleiding is geschreven voor managers in alle sectoren die privacy in hun organisatie willen implementeren, borgen of verbeteren.

De noodzaak om privacy te borgen binnen een persoonsgegevens verwerkende organisatie wordt niet altijd op dezelfde wijze ervaren of gematerialiseerd. Deze handleiding is geënt op de stelling dat een deugdelijk privacybeleid, geënt op de privacywetgeving, uitgevoerd moet worden in een cyclisch governanceproces dat de gehele organisatie raakt en dat specifiek gewijd is aan het halen en borgen van privacydoelstellingen. Natuurlijk loopt de governance van privacy idealiter zoveel mogelijk mee in de algemene organisatiegovernance, maar privacy 'er even bij doen' is een onderschatting van het vraagstuk en geeft te weinig expliciete (bij)stuurmogelijkheden. Het risico is dan dat de compliance aan de wettelijke privacyvereisten aan de oppervlakte aardig geregeld lijkt, maar in werkelijkheid te mager of onvoldoende geïmplementeerd is. En dat kan je op flinke schade komen te staan.

Martin Luther King riep: "I Have a Dream". Hij riep niet "I Have a Plan". Daar zou discussie over zijn gekomen. Ook voor privacybescherming geldt dat je beter eerst zorgt voor overeenstemming over gezamenlijke ambities, voordat je de stap maakt naar implementatiestrategieën en -plannen. Denk vanuit mensen en niet alleen vanuit de inhoud of verplichtingen.

Dit vraagt bij uitstek om het meer dan eenmalig doorlopen van een groeiproces, en daarvoor zijn duidelijke keuzes en een consequente en programmatische aansturing nodig. Voor verbetering, groei en borging van privacy is het nodig dat ambities en de daaraan verbonden ambitieniveaus bepaald, vastgelegd en vastgesteld zijn. Bovendien kost de implementatie van verbeteringen geld, en dat is nu eenmaal eerder terugverdiend wanneer deze kosten worden beperkt door een efficiënte en effectieve werkwijze.



Afbeelding 1: Martin Luther King "I Have a Dream".

De methode 'Grip op Privacy' ziet privacybescherming als een governanceproces. We vinden daarbij ook dat, gezien de aard van het onderwerp, de governance niet alleen van bovenaf aangestuurd moet worden, maar vooral ook van onderaf moet 'groeien'. Het Privacy Volwassenheidsmodel dient daarbij als een meetlat voor de groei. Wij zijn ervan overtuigd dat bewust en goed uitgevoerd privacybeleid door de klanten van de organisatie als kwaliteitskeurmerk wordt ervaren en medewerkers trots maakt.

[2] Bedrijven en organisaties: wij hanteren 'organisaties' voor beide aanduidingen, publiek en privaat.

Privacybescherming in een organisatie is concreet te duiden in voorschriften, processpecificaties en maatregelen, maar dat alléén is niet optimaal. Informationele privacy is de gangbare term voor het correct en volgens de wet omgaan met persoonsgegevens. Maar in algemene zin is 'privacy' een diffuus begrip. Zowel inhoudelijke argumenten als persoonlijke overtuigingen en drijfveren spelen een rol, zeker als implementatie keuzes en veranderingen in de organisatie met zich meebrengt. Het hele bedrijf moet meegaan in het belang van privacybescherming. Het moet 'in de vezels' van de organisatie gaan zitten. En ook dat is te vertalen in concrete actiepunten.

Samen met het Privacy Volwassenheidsmodel biedt deze handleiding zicht op een gestructureerd groeipad voor privacyprocessen, inclusief een aanpak voor de organieke inrichting om te groeien naar het volwassenheidsniveau dat past bij de visie en de missie van de organisatie ten aanzien van de privacybescherming.

Een zeer gewaardeerd hulpstuk hierbij is het Privacy Selfassessment (PriSa) [5]. Het is in feite een checklist op basis van het Privacy volwassenheidsmodel en de Privacy Baseline. De score geeft vervolgens aan in welke mate de organisatie voldoet aan het vooraf op te geven gewenste volwassenheidsniveau – en wat er zonodig nog moet gebeuren om dat niveau te realiseren. Je kunt de test in groepsverband maken of de uitkomsten van de deelnemers met elkaar vergelijken. Het Selfassessment dient zo niet alleen als een instrument om de privacy te bevorderen, maar ook als een awareness booster in de organisatie.

Recentelijk heeft CIP ook de ICO Wizard uitgebracht: een hulpmiddel voor veilig aanbesteden en inkopen van pakketten met het oog op cybersecurity [6]. Met de ICO Wizard krijg je zicht op dreigingen en risico's en hulp bij het stellen van scherpe eisen die passen bij de producten/diensten die je aanbesteedt en die je meegeeft aan de inschrijvers. Beide producten, PriSa en ICO, en de genoemde documenten vind je op de website van CIP: https://cip-overheid.nl.

Doe de zelftest, bepaal de ambities, en richt een privacyprogramma in dat de organisatie langs een realistisch groeipad naar het gewenste volwassenheidsniveau brengt.

2 Privacygovernance

Het doel van privacygovernance is verwoord in een definitie ervan:

Privacygovernance is het inbedden van privacy verhogende maatregelen (met de Privacy Baseline als basis) bij het inrichten en uitvoeren van de bedrijfsprocessen op basis van vastgestelde privacymanagementprocessen die cyclisch worden toegepast. Hierbij is inbegrepen het bewust maken van de betrokkenen[3] en de begeleiding bij het maken van de juiste keuzes, zodat privacy in een vroeg stadium wordt verankerd in de concretisering van de missie en visie van de organisatie, het verdienmodel indien van toepassing, en de processen.

Deze handleiding is geënt op de stelling dat een deugdelijk en bestendig privacybeleid, waarmee een organisatie compliant is aan de privacywetgeving, uitgevoerd moet worden in een cyclisch governanceproces dat in samenwerking met de gehele organisatie tot stand komt. Dit vraagt om duidelijke afstemming en keuzes, waarbij de keuzes worden omgezet in een consequente aansturing. Dit hoofdstuk behandelt de voornaamste elementen van deze visie en hoe je daaraan vorm kunt geven.

Met de Privacy Baseline in de hand kun je gefundeerd en gericht werken aan verbetering van de privacybescherming en/of bijstelling van het privacybeleid. De Baseline biedt een praktische opdeling van de wettelijke bepalingen naar aandachtsgebieden die aansluiten op de beleids-, uitvoerings- en controlprocessen die nodig zijn om tot compliance te komen. Meer hierover in paragraaf 2.3.2.

Stapsgewijze groei en het managen van ambities vragen om overzicht op wat moet worden ingericht. Je moet ook goed weten waarop gelet moet worden en welk pad je kiest. Door het onderkennen van de juiste indicatoren kan iedere organisatie en ieder organisatieonderdeel het veranderprogramma inrichten en finetunen naar de vereisten en mogelijkheden van de specifieke situatie in de organisatie. Hoofdstuk 3 van beschrijft algemene voorwaarden en kritische succesfactoren voor het veranderprogramma en geeft waar mogelijk aanvullende informatie om dit succesvol uit te voeren.

2.1 Privacy vanuit veranderperspectief

Om aantoonbaar en transparant te kunnen voldoen aan de privacy wet- en regelgeving is het inrichten van privacymanagementprocessen een vereiste. Privacygovernance kan niet los staan van bestaande managementprocessen. Door te kiezen voor een aanpak die de privacyprocessen nestelt in de bestaande processen betrek je de organisatie er maximaal bij en kun je de aanwezige kennis en energie maximaal benutten. Kies je voor het neerzetten van privacyprocessen naast de bestaande processen, dan moet alle kennis naast de bestaande organisatie opgebouwd worden en bestaat de kans dat de organisatie zich niet betrokken of zelf overvallen voelt.

Je moet privacy bewust organiseren. De voorgestelde en naar ons inzicht noodzakelijke betrokkenheid van de hele organisatie kun je op verschillende manieren bereiken. Wij kiezen in dit verband voor interne, kleine teams die de 'lokale' veranderingen op (deel)procesniveau of afdelingsniveau faciliteren. Natuurlijk moet er centrale sturing en op allerlei niveaus afstemming zijn, maar organische groei begint in de cellen. Door het de organisatie 'zelf' te laten doen is de kans op betrokkenheid en creatieve

[3] De aanduiding 'betrokkene(n)' kan in dit document twee betekenissen hebben: een betrokkene, zoals in de AVG wordt bedoeld, is degene over wie een (persoons)gegeven informatie bevat. In de meeste gevallen zal deze betekenis aan de orde zijn. Wij gebruiken de term echter ook voor diegenen, die de verwerking uitvoeren, of daar anderszins, bijvoorbeeld als ontwerper of beleidsbepaler, bij betrokken zijn; in deze passage is de tweede betekenis bedoeld. Tenslotte komt het ook een enkele keer voor dat we beide groeperingen tegelijkertijd ermee aanduiden.

energie het grootst. Bovendien: in een doorsnee organisatie is één persoon meestal niet in staat het gehele privacylandschap te overzien en te beheren.

Uiteraard moet de organisatie hiervoor groot genoeg zijn. Maar ook bij een organisatie met weinig medewerkers is het belangrijk de rol, status en dynamiek van een veranderteam te onderkennen. Het gaat ook in kleine organisaties immers net zo goed om het organiseren van betrokkenheid van onderaf. Vaak is het ook in kleine bezettingen mogelijk door middel van een tijdelijke samenwerking van daarvoor (deels) vrijgestelde medewerkers om de gestelde privacydoelstellingen te bereiken, in dit geval: de bescherming van persoonsgegevens naar het gewenste niveau te brengen. Het idee lanceren en erop vertrouwen dat het wel 'vanzelf' tussen de dagelijkse routines door tot een goed resultaat zal leiden, is maar zelden een vruchtbare aanpak.

Als je, zoals wij, gelooft in deze aanpak, dan is in grotere organisaties het formeren van meer dan een aanjaag- en implementatieteam een noodzaak. Met de complexiteit van de organisatie en haar processen neemt het aantal potentieel aan te grijpen zwakke punten toe, en deze zullen bovendien verspreid zijn over en/of tussen verschillende afdelingen. Afdelingen die allemaal eigen processen en applicaties hanteren en qua privacygevoeligheid nogal kunnen verschillen.

Wij noemen deze implementatieteams "ACT" teams. Act betekent niet toevallig 'doen' in het Engels, maar staat in Grip op Privacy tevens voor: Afscherming, Corrigeerbaarheid en Transparantie. Paragraaf 2.3 hieronder gaat hier nader op in.

Het realiseren van privacy past, zeker bij wat complexe organisaties, zelden in een big bang of 'one size fits all' scenario. Althans: wij raden dat niet aan. De privacyambitie kan per organisatieonderdeel verschillend zijn en afhankelijk worden gesteld van de risico's die worden gelopen bij de verwerking van persoonsgegevens, in het bijzonder de vertrouwelijke of gevoelige gegevens[4]. Hierdoor hoeven processen die in orde en 'in-place' zijn bijvoorbeeld niet meer ingericht te worden. Bestaande processen kunnen beter gebruikt worden voor verdere groei in volwassenheid. Nieuwe processen zijn alleen nodig als bestaande processen daarvoor geen potentieel bieden.

De keuze voor een groei vanuit de organisatieonderdelen sluit aan op de aanpak die gelegen is in componenten van privacygovernance zelf, zoals het uitvoeren van DPIA's[5][6] en selfassessment (PriSa) [7]. Groei vanuit de staande organisatie wordt mogelijk door de hier opgedane kennis en ervaring te benutten en door te vertalen naar organisatiebreed gedeelde kennis en ervaring. Deze gedeelde kennis en ervaring wordt weer benut om te komen tot uniform en gedragen beleid en processen.

---

[4] De AVG kent de term 'gevoelige gegevens', maar spreekt van 'bijzondere gegevens'.

[5] De Nederlandse vertaling van de AVG introduceert de "Gegegevens Effect Beoordeling (GEB)" voor wat daarvoor bekend stond als PIA: Privacy Impact Analyse. Tegenwoordig is de afkorting 'DPIA' gangbaar (Data Protection Impact Assessment).

[6] Het verschil tussen PIA/DPIA en PriSa kan het eenvoudigst getypeerd worden met: een (D)PIA kijkt naar een onderdeel van de organisatie of een proces; PriSa betreft de gehele organisatie. (D)PIA betreft het inschatten van privacy-risoco's; met PsiSa stel je (bij voorkeur in groepsverband) het niveau van privacyvolwassenheid vast. Beide instrumenten geven aanwijzingen voor verbetertrajecten.

2.2 Privacy Volwassenheidsmodel

De aard van de gegevensverwerking(en) in een organisatie is in hoge mate bepalend voor het ambitieniveau dat je ten minste moet nastreven. Hoe vertrouwelijker de gegevens zijn die een organisatie verwerkt, des te hoger moet het volwassenheidsniveau zijn om er zeker van te zijn dat de privacybescherming op een passende manier is of kan worden ingevuld en gegarandeerd.

In het Privacy Volwassenheidsmodel is per norm van de Baseline beschreven waaraan voldaan moet zijn om een bepaald volwassenheidsniveau te bereiken. Er worden 5 volwassenheidsniveaus onderscheiden, grofweg van geen dan wel of versnipperde aandacht voor privacy, tot perfecte organisatiebrede beheersing en benutting van de privacybescherming. Een niveau geeft daarbij de mate aan, waarin de 'organisatie van privacy' is gesystematiseerd en geïnternaliseerd in de organisatie.

> Deze handleiding laat iedereen vrij in het na te streven ambitiesniveau, *maar richt zich op het behalen en onderhouden van niveau 3* en vormt daarmee een opstap naar een vrij te kiezen hoger ambitieniveau.

Op voorhand is niveau 3 een redelijk volwassenheidsniveau voor organisaties die persoonsgegevens verwerken. Het is doorgaans voldoende om de compliancy-toets te doorstaan en het is tevens een niveau dat voor grotere en kleinere organisaties alleszins haalbaar is.

Door een organisatie te laten groeien volgens de stappen van het Privacy Volwassenheidsmodel kun je de omslag die de organisatie moet maken terugbrengen tot een reeks van kleinere veranderingen. Het benutten van bestaande verhoudingen en kennis maakt het mogelijk de kracht van de eigen organisatie te gebruiken en in te zetten in de beoogde verbetering van de privacyprocessen. Bestaande verhoudingen veranderen niet zozeer, maar worden wel meer expliciet gemaakt; privacybescherming wordt niet als een extra belasting, maar als aandachtspunt meegenomen in de bedrijfsvoering.

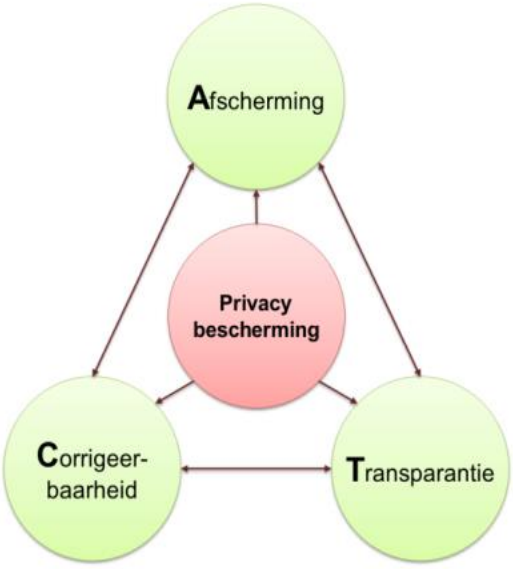
2.3 Groei, de ACT-doelen en het ACT-team

Volwassenheidsmodellen worden in de regel door organisaties ingezet om te bepalen hoe de organisatie organisatiebreed gevorderd is met het voldoen aan gestelde ambities – in deze context: voldoen aan de privacywetgeving.

Maar de opeenvolgende niveaus kun je ook proactief gebruiken om opeenvolgende haalbare ambities in beeld te krijgen en stapsgewijs te kunnen groeien naar je doel. Het behaalde privacyvolwassenheidsniveau wordt bepaald door de mate waarin de organisatie aan de criteria van de Privacy Baseline voldoet.

In de Privacy Baseline zijn de doelen van privacybescherming beschreven, kort aangeduid als de 'ACT-doelen': Afscherming, Corrigeerbaarheid en Transparantie. Het realiseren van de ACT-doelen is mogelijk door te voldoen aan de daaraan gekoppelde criteria. Deze criteria worden beschreven in de Privacy Baseline en geven aan *wat* gedaan moet worden.

Daarmee is echter nog niet beschreven *hoe* je dat doet en in je organisatie ingevoerd en geborgd krijgt. Deze handleiding geeft daarvoor praktische handvatten en kritische succesfactoren. Overigens is de Baseline zelf al een praktische handreiking om 'Grip op Privacy' te krijgen, want die is zó opgezet dat de criteria een cyclisch governanceproces van beleidsvorming, uitvoering en control vormen.



Figuur 1: Privacybescherming als resultante van ACT.

Groei in volwassenheid betekent meer grip op de complexiteit van de organisatie: veranderingen vinden niet plaats binnen het werk van één persoon (niveau 1) of binnen één afdeling (niveau 2), maar vinden steeds meer in samenhang plaats binnen de gehele organisatie. Deze samenwerking kun je faciliteren door wat wij hier ACT-teams zullen noemen: een al dan niet tijdelijk verband van personen uit diverse geledingen van de organisatie, die verantwoordelijk zijn of worden voor het op niveau brengen van de ACT-doelstellingen en het door de organisatie gekozen volwassenheidsniveau.

De expliciete vorming van een of meer ACT-teams bevordert de algehele beheersing van de veranderoperatie, maar is bovenal ook een statement dat de beoogde verbetering van de privacy serieus genomen wordt. Zij bieden tevens de ideale landingsplaats voor het inzetten van de in de lijn en op de werkvloer aanwezige energie en expertise, hard nodig voor het opzetten en verwerken van DPIA's bijvoorbeeld, en het bevorderen van de betrokkenheid van de gehele organisatie.

- Meer over het ACT-team vind je in paragraaf 5.3 van de toelichting: Het ACT-team en de organisatie als één team.
- De passages over de ACT-doelen uit de Privacy Baseline zijn voor het gemak hier herhaald in Bijlage 2.

2.3.1 Ambities doen groeien, niet wetten of commando's

Martin Luther King had geen plan, althans: dat zei hij niet hardop. Het verschil is dat een droom nog geen voorschot neemt op de wijze van realiseren. Privacybescherming in een organisatie is heel concreet te duiden in voorschriften, maatregelen en processpecificaties, maar de *noodzaak* om privacy te borgen binnen een persoonsgegevens verwerkende organisatie wordt niet altijd op dezelfde wijze ervaren of gematerialiseerd: iedere medewerker moet meegaan in het belang van privacybescherming. Het moet, zoals al gezegd, in de 'vezels' van de organisatie gaan zitten. En ook dat is te vertalen in concrete actiepunten.

De drang om een (tussen)doel te bereiken is afhankelijk van de redenen die je ziet om grip te krijgen op privacy. Het is belangrijk de ambities gedragen te krijgen en pas daarna door te vertalen naar de wijze waarop en het tempo waarin je deze ambities wilt bereiken. Vervolgens vraagt bestendiging of groei om het meer dan eenmalig doorlopen van een proces. En dat vraagt om duidelijke en bovenal gedragen keuzes (doelen). Voor verbetering, groei en borging is het nodig dat ambities en de daaraan verbonden ambitieniveaus bepaald, vastgelegd en vastgesteld zijn. Bovendien kost de implementatie

van verbeteringen geld, en dat is nu eenmaal eerder terugverdiend wanneer deze kosten worden beperkt door een efficiënte en effectieve werkwijze.

Precies dat bereik je naar onze stellige overtuiging veel beter langs de lijnen van gedeelde ambities, de inzet van aanwezige ervaring en uitgaan van de menselijke maat voor groei. Ook, en misschien wel: juist bij het thema privacy geldt dat je beter eerst zorgt voor overeenstemming over de gezamenlijke doelen en ambities, voordat je de stap maakt naar implementatiestrategieën en plannen[7].

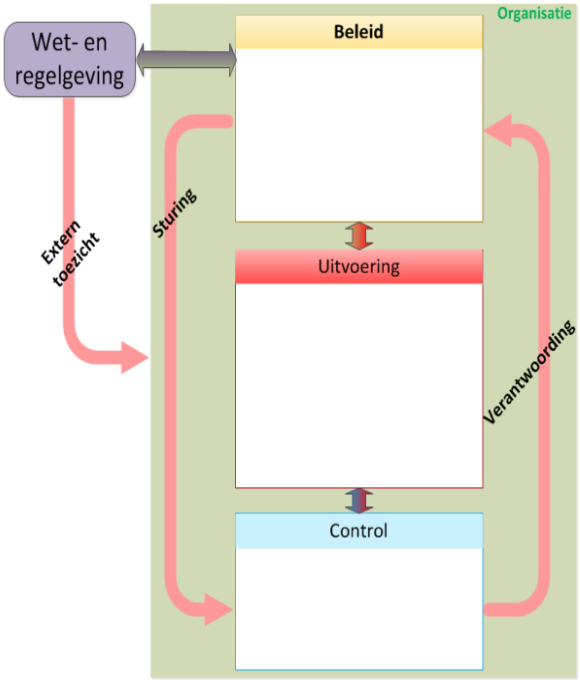
> De *haalbaarheid* van de ambitie om privacy te borgen hangt nauw samen met de redenen om de privacy te beschermen.
> In een organisatie is dat bij voorkeur een *gedeelde* ambitie: één zwakke schakel kan immers het hele privacybeleid teniet doen.

2.3.2 De Privacy Baseline als basis om te groeien

Voor het kunnen overzien van het landschap en het bewaken van de samenhang is de Privacy Baseline een belangrijke hulp. De ordening in de domeinen Beleid, Uitvoering en Control geeft in een cyclisch proces sturing aan het leervermogen van de organisatie.

Het voordeel van deze aanpak is dat wijzigingen in wetgeving, ambitie of omgeving eerder, efficiënter en beter kunnen worden geduid. Tegelijkertijd worden de eventueel noodzakelijke aanpassingen binnen de organisatie en van de gegevensverwerking trefzeker gepland, geïnitieerd en bewaakt.

Een groeifase kan begeleid worden doorlopen aan de hand van het standaard PDCA-model. In dit model worden doelstellingen en de aanpak (Plan) bereikt door het uitzetten van de activiteiten (Do), het bewaken (Check) van voortgang middels de gerapporteerde prestaties en het desgewenst bijsturen of verduidelijken (Act, ook wel aangeduid als 'Correct') van de doelstellingen en de aanpak.

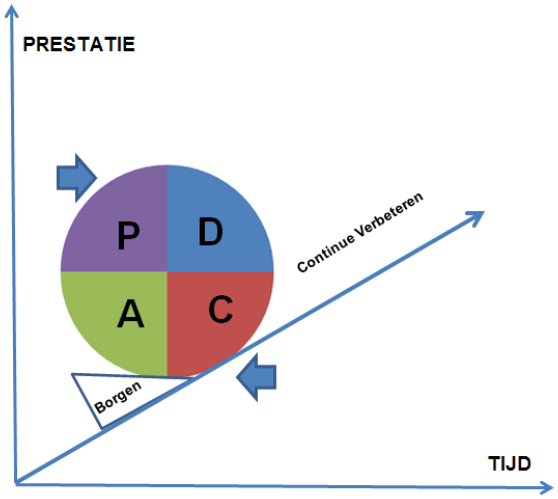


Figuur 2: Het cyclische proces van Beleid, Uitvoering en Control is gebaseerd op het standaard PDCA-model.

[7] Een aanpak die helpt doelstellingen en ambities te vertalen naar inspanningen en activiteiten is bijvoorbeeld de VIP-behandeling zoals besproken in Kooreman 2009. [8]

'Groeien' doe je het meest efficiënt door het borgen van tussentijdse resultaten, het communiceren van de behaalde successen en waarderen van degenen die dit hebben mogelijk gemaakt binnen de organisatie.

Ook communicatie over de voortgang en het succes van het project is interactief het meest effectief bij het borgen van tussenresultaten. De effectiviteit van de werkzaamheden wordt vergroot door deze communicatie niet te beperken tot alleen de eigen organisatie, maar ook openheid te bieden buiten de eigen organisatie, naar de klanten en stakeholders.



Figuur 3: Groeien door tussenresultaten te borgen.

Veranderingen zijn vluchtig wanneer je ze niet kunt 'beetpakken'. Leg ze vast om ze te kunnen vieren en blijvende waarde te creëren.

2.3.3 Het stapsgewijs benutten van kennis: inside-out benadering

Top-down en bottom-up zijn bekende strategieën om beleid en uitvoering op één lijn te brengen. Beide aanpakken kennen voor- en nadelen. Een top-down aanpak is met name goed toepasbaar in nieuw in te richten organisaties. Het geeft, in de ideale situatie, direct duidelijkheid over wat moet gebeuren. In bestaande organisaties is veel kennis beschikbaar over de uitvoerbaarheid van beleid op tactisch en operationeel niveau. Dit is kennis die nuttig of zelfs essentieel is om grip op privacy met succes te realiseren. Directe betrokkenheid vanuit de uitvoering verhoogt de slaagkans van de invoering.

In de Privacy Baseline staat de uitvoering centraal en zijn het beleidsdomein en het controldomein sturend voor de uitvoering. Om hier naar toe te groeien kan de zogenaamde inside-out benadering worden gekozen, waarbij de aanwezige kennis van de uitvoering bottom-up wordt benut om te komen tot organisatiebreed beleid en organisatiebrede control. In termen van volwassenheidsniveau gesproken: op niveau 1 en 2 bestaat deze kennis op afdelingsniveau. Op niveau 1 is er kennis over de uitvoering; op niveau 2 is er op afdelingsniveau kennis over het beleid en het in control komen. Vanaf niveau 3 is kennis op organisatieniveau in plaats van op afdelingsniveau sturend.

Deze groei in sturing is in onderstaande tabel gevisualiseerd[8,9].

[8] Zie hoofdstuk 2 van het Privacy volwassenheidsmodel.

[9] Over SIVA zie: W.N.B. Tewarie, SIVA, Methodiek voor de ontwikkeling van auditreferentiekaders, VU University Press, Amsterdam 2014

Tabel 1: de relatie tussen SIVA lagenstructuur en de CMMI Levels.

SIVA lagenstructuur (CMMi levels)	Level 0 Ad hoc	Level 1 Informeel	Level 2 Beheerst	Level 3 Vastgesteld	Level 4 Kwantitatief beheerst	Level 5 Geoptimaliseerd
Algemeen Beleidsdomein						
Specifiek Beleidsdomein						
Uitvoerend domein						
Specifiek Control domein						
Algemeen control domein						

Je benut de kracht van de organisatie door de inside-out benadering te hanteren. Hierbij worden op de lagere volwassenheidsniveaus eerst de processen binnen het uitvoeringsdomein op een hoger niveau gebracht. Binnen de uitvoering zit veel kennis en zijn beleidskeuzes impliciet gemaakt.

Door eerst deze processen op een hoger niveau te brengen benut je deze impliciete kennis en kunnen beleidskeuzes worden bekrachtigd of worden bijgesteld. Pas op niveau 3 is centraal beleid meer leidend en kunnen controles op een gewenst niveau gebracht worden. Vanaf niveau 4 kan begonnen worden met het op nog hoger niveau brengen van de organisatie, door de prestaties beter meetbaar te maken en centraal sturing te geven aan de kwaliteit het grip-op-privacyproces. Op niveau 5 werkt de organisatie consequent volgens een strakke sturing vanuit het topmanagement.

In de inside-out benadering stemmen afdelingen in de uitvoering met elkaar af. Dit vergroot gedeelde kennis en uniformiteit. Hoewel dit om zorgvuldige afstemming vraagt, is het voordeel dat men betrokken is en dat de groei van volwassenheidsniveau level 0 of 1 naar 2 en 3 geleidelijk en ingebed geschiedt. Desinvesteringen vanwege niet bij de uitvoering passende organisatorische en technische maatregelen worden zo voorkomen.

> Hanteer een inside-out benadering, waarbij de kennis van afdelingen wordt benut; alignment van beleid/control en de uitvoering kan zo worden gewaarborgd en desinvesteringen worden voorkomen.

2.4 Het slim kiezen van de incrementen per proces

Hoe snel wil je groeien? Hoe snel kan of mag het gaan? Ambities worden haalbaar gehouden door ze te baseren op beschikbare kennis, leervermogen en kunde van medewerkers. Het groeiproces wordt zodoende een geleidelijk leerproces, waarbij de organisatie en haar medewerkers actief worden betrokken.

Veel procesverbeteringen kunnen worden doorgevoerd zonder afhankelijkheid van het volwassenheidsniveau van andere processen. In situaties waarin voor een bepaald privacyproces de verbeterpunten moeilijk grijpbaar te maken zijn, kun je ervoor kiezen dit specifieke proces in volwassenheid achter te laten lopen ten opzichte van andere privacyprocessen. Hierdoor ontstaat een evolutionaire groei en blijven de ambities haalbaar en worden desinvesteringen voorkomen.

Het management moet een beslissing nemen welk groeipad gekozen wordt. De in deze notitie voorgestelde groei is gebaseerd op de groei in volwassenheid, waarbij, gegeven het leervermogen van de organisatie, de kracht van de eigen organisatie wordt benut. In het tweede deel gaat paragraaf 5: "Toelichting op verandermanagement" daar verder op in.

Een natuurlijke evolutionaire groei biedt een geleidelijk groeipad,
waarbij ambities haalbaar worden gehouden, de organisatie geleidelijk leert
en desinvesteringen worden voorkomen.

2.5 Vinger aan de pols: risicoanalyse (DPIA) en selfassessment (PriSa).

Deze handleiding geeft organisaties handvatten om grip op privacy te krijgen. Om in deze aanpak succesvol te zijn moeten de risico's en de inspanningen van de implementatie van maatregelen worden begrepen. Hiervoor moeten risico's, de noodzaak van adequate controles en de kansen die het biedt om de bedrijfsvoering te verbeteren duidelijk worden.

Instrumenten om zwakheden in de privacybescherming en verbeterpunten en -plaatsen te ontdekken zijn de Privacy Self Assessment (PriSa) en de Data Protection Impact Assessment (DPIA); zij brengen privacyrisico's in (delen van) de bedrijfsvoering aan het licht en maken ze bespreekbaar. Een DPIA pas je toe op procesniveau; een PriSa heeft betrekking op de hele organisatie of een organisatieonderdeel.

In een PriSa wordt de volwassenheid van de privacyprocessen bepaald en wordt de gap met het ambitieniveau van de organisatie ten aanzien van de privacyprocessen duidelijk. In een DPIA wordt een inhoudelijke toets uitgevoerd en per gegevensverwerking de gap met de wet- en regelgeving bepaald[10].

Een organisatie kan van beide instrumenten de uitkomsten combineren om een compleet beeld te krijgen over welke organisatorische (procesmatige) en welke inhoudelijke maatregelen nog nodig zijn om de privacybescherming op niveau te krijgen. De PriSa en de DPIA's bieden zo een 'privacy gapanalyse'.

Voor een privacy gapanalyse zijn ook andere werkwijzen en instrumenten beschikbaar, die kunnen variëren in oriëntatie of specialisatie. Maar allemaal moeten ze de privacyrisico's van een specifieke verzameling, de (verdere) verwerking en bewaring of vernietiging van persoonsgegevens op systematische wijze identificeren en lokaliseren.

Het is natuurlijk raadzaam dergelijke analyses in een zo vroeg mogelijk stadium uit te voeren, zodat een organisatie maatregelen kan nemen nog voordat het risico zich daadwerkelijk voordoet en er

[10] Uit een DPIA zelf blijkt niet welke concrete maatregelen er genomen moeten worden. Maar door de risico's van een gegevensverwerking in kaart te brengen kan een verwerkingsverantwoordelijke en/of een verwerker van persoonsgegevens bepalen welke maatregelen nodig en passend zijn.

schade ontstaat voor de organisatie en betrokkene. De analyses passen daarmee heel goed binnen de methode Grip op Privacy en het hanteren van een groeimodel. Gebruik ze om een *nulmeting* te doen voor een volgende cyclus in de groei naar een hoger volwassenheidsniveau; of voor bevestiging van het vermoeden dat het bestaande niveau niet meer of juist nog wel voldoet.

> Zet de Privacy Self Assessment (PriSa) en de Data Protection Impact Assessment (DPIA) in voor inventarisatie van risico's en te nemen organisatorische en inhoudelijke maatregelen.

Bedenk daarbij dat het herhaald uitvoeren van een analyse minder tijd kost dan het uitvoeren van de eerste analyse. Het meer en meer op orde hebben van de privacybescherming betekent dat de voor de analyse benodigde informatie steeds gemakkelijker voorhanden is.

In plaats van of in aanvulling op een zelf uitgevoerde PriSa en een DPIA kan je ook kiezen voor het inzetten van een externe partij. Een voordeel van een externe partij is mogelijk dat 'vreemde ogen dwingen'. Tevens kan hun expertise gebruikt worden om de maatregelen op te stellen of uit te werken.

2.6 Groeien in volwassenheid: wat kost het?

Kosten en inspanningen verschillen per organisatie. Daar valt op deze plaats niets concreet over te zeggen. Maar het is goed te bedenken dat van elke persoonsgegevens verwerkende organisatie steeds méér verwacht wordt vanwege meer stringente handhaving van de privacywetgeving, meer publieke aandacht en de toename van het aantal verwerkingen van persoonsgegevens. Het niet of onvoldoende investeren in privacy wordt financieel riskant door de zekerheid dat fouten en ongelukken zich zullen voordoen. Deze zullen vroeger of later gaan opvallen in de maatschappij en dan mogelijk tot aanzienlijk meer kosten leiden dan proactief handelen om deze gang van zaken te voorkomen.

Groei in volwassenheid betekent ook het borgen van de reeds gedane investeringen in de privacy. Want als de processen niet meegroeien met de omvang en complexiteit van de organisatie, dan neemt de volwassenheid van de organisatie af en zullen de investeringen, die nodig zijn om weer op een passend volwassenheidsniveau terug te komen, steeds meer toenemen.

2.7 De grootte van de organisatie

Organisaties verschillen in cultuur, aansturing, structuur, bedrijfsdoelstellingen, klanten en grootte. De groei in volwassenheid betekent dat taken worden samengevoegd en meer centraal worden ingevuld.

Kleine organisaties hebben doorgaans korte(re) communicatielijnen en een informeler karakter. Groei in volwassenheid verandert deze karakteristieken bij kleine organisaties minder dan bij grote organisaties. Daarnaast is de impact en de benodigde effort voor kleine organisaties doorgaans beperkter, communicatielijnen worden niet direct (veel) langer.

De omvang van een organisatie is van invloed op de wijze waarop groei naar meer volwassenheid kan plaatsvinden. Maar de grootte van de organisatie is niet of maar beperkt relevant voor de keuze om een volwassenheidsmodel te hanteren. *Wel vraagt de groei in volwassenheid vrijwel altijd om een meer formele werkwijze*. Het voordeel daarvan is meer transparantie, omdat keuzes binnen de organisatie worden vastgelegd en daardoor beter gedeeld kunnen worden.

2.8 Kritische succesfactoren: COBIT

De doelstellingen van privacybescherming en de processen die daarbij horen staan niet los van de bedrijfsdoelstellingen. Door de doelstellingen van privacybescherming in lijn te brengen met de bedrijfsdoelstellingen ben je veel beter in staat de privacybescherming concreet te organiseren, te meten en te sturen.

2.8.1 COBIT Management guidelines

De COBIT Management guidelines [9]. beschrijven hoe governance in te richten binnen het IT-domein. Deze guidelines beschrijven de kritische succesfactoren, de belangrijkste taken, doelstellingen en metrieken voor het invoeren van de COBIT-processen. De COBIT (Control OBjectives for Information related Technologies) is een open industriestandaard voor het beheer, controle en beveiliging van informatietechnologie. De guidelines vormen dan ook een belangrijk voorbeeld van wat je moet regelen om in control te komen en zijn daarom als input gebruikt voor dit document.

Om grip te krijgen op privacy binnen je organisatie zijn *kritische succesfactoren* belangrijke aandachtspunten en acties. Dit document beschrijft die voor het privacydomein.

Niet overgenomen van de COBIT Management guidelines is het meetbaar maken van de doelstellingen. In plaats daarvan besteedt deze handleiding meer aandacht aan het aspect *verandermanagement*. Hiervoor is gekozen omdat privacygovernance in deze handleiding meer gaat over veranderen van de organisatie, dan over het meetbaar maken van de resultaten. Dit laatste speelt meer op volwassenheidsniveau 4 en niet op de niveaus 1, 2 en 3. Dit document richt zich dus op het bereiken van niveau 3 van het Privacy Volwassenheidsmodel, niet op het meetbaar maken van niveau 4.

2.8.2 Kritische succesfactoren voor privacy

De kritische succesfactoren in deze handleiding zijn voor het ACT-team en het management de belangrijkste aandachtspunten en acties die onder controle moeten zijn. Zij zijn gekozen op basis van een analyse vanuit het perspectief van verandermanagement en een analyse van de KSF's van de COBIT Management guidelines.

De KSF's vormen daarmee de sleutels tot de implementatie van de Privacy Baseline op de verschillende niveaus binnen de organisatie. KSF's kunnen technisch, organisatorisch en procedureel van aard zijn.

Verderop maken we nog onderscheid tussen de KSF's voor:

- Privacy als veranderprogramma: van belang voor het topmanagement en ACT-team;
- De realisatie van de afzonderlijke criteria: van belang voor de verantwoordelijken binnen de privacyprocessen.

Groei in volwassenheid vraagt altijd om een meer formele werkwijze.

3 Het privacybeschermingsprogramma als veranderprogramma

In de eerste helft van dit eerste deel van deze handleiding hebben we een lans gebroken voor een veranderstrategie die zich richt op het *betrekken van de staande organisatie*: bij het formuleren van ambities, de korte- en langetermijndoelen en een geleidelijke, haalbare groei, waarbij de aanwezige expertise, ideeën en sentimenten alle aandacht krijgen en zoveel mogelijk benut worden. De aard van het onderwerp 'privacy' rechtvaardigt ons inziens een dergelijke 'menselijke maat aanpak' boven het eenzijdig van bovenaf vaststellen van termijndoelen in een resultaatgericht afrekenmodel.

Het komt - hopen wij - maar zelden voor dat een serieuze, professionele gegevensverwerkende organisatie nog helemaal geen privacybeschermende maatregelen heeft genomen, al is het maar op een intuïtief niveau. Er valt altijd ergens bij aan te sluiten. En dat herhaalt zich steeds bij het streven om van het bestaande volwassenheidsniveau naar het naasthogere te komen. Het toepassen van een te strakke programmatische aanpak daarbij is, naarmate de organisatie complexer is, vermoedelijk niet verstandig, niet alleen voor de efficiëntie maar ook omdat de programmatische aanpak in alle niveauvarianten steeds dezelfde is.

De voorgestelde aanpak wil niet zeggen dat er geen harde criteria kunnen worden gehanteerd of termijnen kunnen worden gesteld aan de verwezenlijking van de ambities. De kwaliteit van privacybescherming in de organisatie is wel degelijk ook in heel concrete termen te definiëren en te meten. Privacybescherming vraagt immers niet alleen om een gemeenschappelijk verantwoordelijkheidsbesef en een gedeeld concept van respectvol omgaan met andermans gegevens, er zijn ook heel concrete maatregelen en procesinrichtingen voor nodig om dit besef materieel waar te kunnen maken. En om dat coherent, consequent, doelgericht en uiteindelijk ook meetbaar te realiseren is een programmatische aanpak wel degelijk nodig.

Privacygovernance richt de privacyprocessen in, zodat de privacybescherming voldoet aan de vereisten die in de wet worden gesteld en het volwassenheidsniveau van de processen aansluit op het volwassenheidsniveau dat de organisatie ambieert.
De kans op succes wordt groter door daarbij aandacht te hebben voor de KSF's.

In de volgende paragrafen worden achtereenvolgens KSF's benoemd en toegelicht die belangrijk zijn:

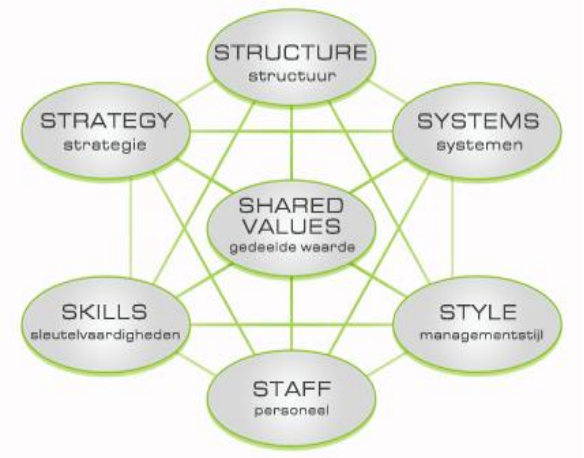
- 3.1 in het algemeen bij veranderingen in organisaties die met privacy te maken hebben;
- 3.2 voor het beleidsdomein;
- 3.3 voor het uitvoeringsdomein;
- 3.4 voor het control- en beheerdomein.

De KSF's voor beleid, uitvoering en control zijn direct gerelateerd aan de criteria in de Privacy Baseline. De daarbij gebruikte aanduidingen als B.01, U.04, C.02 zijn verwijzingen naar de overeenkomstig gelabelde principes in de Privacy Baseline.

3.1 Kritische succesfactoren algemeen: samenhang

KSF's kunnen op verschillende manieren verdeeld zijn over de factoren die bepalend zijn voor het succes van een veranderprogramma. Het 7S model kan daarbij behulpzaam zijn [10]. Het model van McKinsey combineert rationele en harde elementen met emotionele en zachte elementen en leent zich uitermate goed voor het achterhalen van sterktes en zwaktes in de onderneming.

Aan de hand van zeven vaste factoren kun je de prestaties van een onderneming analyseren. Deze factoren moeten integraal worden beschouwd en beïnvloed, om zo een effectieve en efficiënte organisatie te realiseren. De benadering van elk van de 7 factoren beïnvloedt ook de andere 6 en moet deze daarom ook ondersteunen. Op deze manier worden alle factoren, en daarmee de gehele organisatie, versterkt.



Voor elk van de 7 factoren in het overzicht hieronder worden KSF's genoemd die algemeen gelden, maar zoveel mogelijk naar de governance van Privacy worden toegeschreven.

3.1.1 Strategie

- De privacybeschermingsstrategie ondersteunt de bedrijfsstrategie.
- De ambitie voor het beschermen van de privacy is duidelijk, wordt gecommuniceerd naar alle disciplines en wordt begrepen en omarmd.
- De strategie voor de verbetering is gebaseerd op waar de organisatie naar toe wil groeien.
- De organisatie beschikt over heldere en meetbare doelen voor privacybescherming, die aansluiten bij de missie en doelen van de organisatie als geheel.
- De organisatie heeft een privacybeleid dat door het management is bekrachtigd en wordt uitgedragen.
- Privacybescherming maakt een integraal deel uit van de plannen van de organisatie.
- De aanpak is zowel gericht op het benoemen van de uit te voeren activiteiten, als het meegeven van meer algemene richtlijnen voor het ACT-team.
- De aanpak is vertaald in vastgelegde ambities, stappenplannen en benodigde migraties.
- De aanpak bevat roadmaps [17] en migratiestrategieën, die de kracht van de organisatie benutten om vanuit de huidige stand van de verwerking van persoonsgegevens mee te nemen naar de toekomstige situatie.

3.1.2 Staf

- Het management geeft tijd, ruimte en middelen aan de ACT-doelen.
- Binnen het management spreekt men elkaar aan op motivatie en voorbeeldgedrag.
- Het commitment van het management is gebaseerd op gevalideerde informatie en een gestructureerde en transparante besluitvorming.
- Privacybeschermers zijn bevoegd om onderzoek te doen en aanwijzingen te geven.
- De organisatie heeft een functionaris gegevensbescherming (FG) met een goede taakomschrijving en het juiste mandaat om de nodige taken uit te voeren.
- Het management onderschrijft de aanpak om te groeien in volwassenheid en benadrukt de noodzaak van communicatie, begrip en naleving.

3.1.3 Systemen

- De aanpak is gebaseerd op een Privacy GAP-analyse, waarvoor de Privacy Baseline en het Privacy Volwassenheidsmodel de basis vormen. Een groeifase start met een GAP-analyse, bijvoorbeeld met behulp van DPIA/PriSa. Op basis van een GAP-analyse worden de leerdoelen binnen een groeifase benoemd.
- Privacybescherming maakt zoveel mogelijk integraal deel uit van bestaande werkwijzen en procedures.
- Werkwijzen en procedures zijn beschreven, toegewezen en bekend gemaakt.
- Er is een projectrisicoanalysemethode binnen de organisatie gedefinieerd en deze wordt gehanteerd.
- Iedereen die betrokken is bij het proces is doelbewust en heeft de nodige informatie over de werking van de privacyprocessen en over de gevolgen van beslissingen die in dit kader worden genomen.
- Er is een continu proces van kwaliteitsverbetering.
- Privacybescherming wordt meegenomen in de wijzigingsprocessen van de gegevensverwerkingen en systemen.
- De privacygovernancecyclus loopt synchroon aan de overige governanceprocessen in de organisatie, zodat de activiteiten ten behoeve van privacy optimaal afgestemd kunnen zijn op die van de andere governanceprocessen.
- De processen, diensten en functies die nodig zijn voor het resultaat liggen vast, maar zijn flexibel en kunnen veranderen, met een transparant wijzigingsproces.
- Budgetten zijn actueel, bevatten de end-to-end uitgaven en hebben herkenbare verantwoordelijke budgethouders.

3.1.4 Structuur

- De organisatie kent een heldere structuur, waarin verantwoordelijkheden zijn benoemd en is vastgelegd welke personen daarvoor verantwoordelijk zijn.
- De rollen en taken van medewerkers, managers en het ACT-team zijn vastgelegd.

- Het is bekend hoe processen moeten worden geïmplementeerd en wie verantwoordelijk is voor de prestaties.
- Er is een ACT-team benoemd en aan de slag met het bieden van structuur en overzicht.
- Het ACT-team communiceert zijn doelstellingen en resultaten naar alle organisatieniveaus.
- De verantwoordelijkheden voor het realiseren, het bijhouden en het communiceren van de verwachte voordelen van privacybescherming zijn helder belegd.

3.1.5 Shared Values

- Bekend moet zijn of de organisatie risicomijdend of risicodragend is; de strategie en uitingen zijn hierop afgestemd.
- Er zijn middelen beschikbaar om privacybescherming te bevorderen in de kennis, houding en het gedrag van alle medewerkers in de organisatie en eventuele onderaannemers.
- Er wordt een beroep gedaan op algemeen geldende waarden, zoals bijvoorbeeld 'aanspreekbaar handelen'.
- De veranderingen zijn afgestemd op de capaciteit van de organisatie zodat effectief invoeren mogelijk is.
- Investeringen zijn beoordeeld op korte- en langetermijneffecten, gevolgen voor andere verwerkingen en afdelingen en toegevoegde waarde voor de organisatie.

3.1.6 Stijl

- De bedrijfscultuur is gevestigd en stabiel, inclusief een positieve samenwerking tussen organisatieonderdelen, teamwork en een voortdurend oog voor procesverbetering.
- Er is een praktijk van open uitwisseling van informatie over gebeurtenissen en een goede relatie met leveranciers en derden die de inzet van passende oplossingen bevordert.
- Er is evenwicht tussen de time-to-market en de kwaliteit van de dienstverlening. Hierbij is rekening gehouden met de eisen vanuit de lijnorganisatie en de bedrijfsdoelstellingen.
- De organisatie is vertrouwd met de stijl van leidinggeven en de gangbare 'tone-of-voice'. De wijze van communiceren is hierop afgestemd.
- De planning voorziet in de mogelijkheid om prioriteiten te bepalen en aan te passen al naar gelang de risicopositie dat vereist.
- Investeringsbeslissingen worden gepresenteerd met opties en alternatieven, waarna duidelijke keuzes gemaakt kunnen worden op basis van de effecten, voordelen, realisatiedatum en haalbaarheid.
- De overgang van de taken en veranderingen van het ACT-team naar de staande organisatie is afgesproken en vastgelegd als een beheerd proces.

3.1.7 Skills

- Er zijn ervaren en deskundige projectmanagers beschikbaar.

- De vereiste kwaliteiten van het personeel (opleiding, overdracht van informatie, het moreel, etc.) zijn bekend en sluiten aan op de vereiste vaardigheden.
- Er is een goed begrip van de mogelijkheden en beperkingen van de organisatie en het ACT-team in het uitvoeren van de veranderingen.
- Doelgroepen beschikken over juiste vaardigheden om gewenst gedrag te vertonen.
- De organisatie kent de branche en het branchebeleid ten aanzien van privacy en de daarin gemaakte keuzes en oplossingen.

3.2 Kritische succesfactoren in het beleidsdomein

Vanuit het beleidsdomein wordt duidelijkheid gegeven, zodat men wéét waaraan de organisatie zich te houden heeft. Vanuit het beleid laat men daarbij niets aan het toeval over. Duidelijkheid wordt gegeven door het implementeren van de Privacy Baseline in de governance van de organisatie.

3.2.1 Privacybeleid - B.01

De ontwikkeling van het privacybeleid komt bij voorkeur iteratief tot stand, waarbij de hele organisatie bij de hand wordt genomen, zodat iedereen goed begrijpt waarom welke keuzes worden gemaakt. Het resultaat van het proces is het beleidsdocument met daarin het privacybeleid. Het privacybeleid geeft aan op welke wijze door het treffen van maatregelen voldaan wordt aan de van toepassing zijnde wet- en regelgeving. Omdat de wet- en regelgeving externe factoren zijn die kunnen veranderen, is periodieke review nodig om vast te stellen of het beleid nog voldoet. Maar ook interne factoren, zoals onvoldoende effectiviteit van het beleid en gewijzigde missie of visie, kunnen het nodig maken om te komen tot aanpassing van het beleid. Het volstaat dus niet om eenmalig het beleid op te stellen en niet meer aan te passen.

Doelstelling en realisatie

Het doel van het privacybeleid is om op en strategisch organisatieniveau duidelijkheid te geven over de inrichtingskeuzes die gemaakt zijn ten aanzien van privacybescherming en te waarborgen dat de gegevensverwerking op een rechtmatige wijze plaatsvindt. Het maakt de uitvoerende units van de organisatie duidelijk wat er exact wordt verwacht opdat persoonsgegevens rechtmatig zullen worden verwerkt. Input voor het privacybeleid is de wet- en regelgeving en de kennis en ervaring binnen de organisatie over de status van de privacybescherming. De Privacy Baseline en het Privacy Volwassenheidsmodel kunnen worden gebruikt als modellen om te bepalen waarop het beleid antwoord moet geven en om de organisatie te laten groeien in volwassenheid.

Kritische succesfactoren

Helder beleid:

- De mate waarin de organisatie compliant wil zijn is bekend (ambitie). Er is daarbij een duidelijk verband en afstemming tussen het privacybeleid en de bedrijfsstrategie.
- Het (privacy)beleid is onderworpen aan een succesvolle juridische toetsing en goedkeuring.
- De organisatie kent de sector en de daar geldende sectorspecifieke wet- en regelgeving.
- De privacydoelstellingen en het privacybeleid zijn helder gedefinieerd, duidelijk gearticuleerd, en de uitingen zijn afgestemd op de doelgroepen en zijn gecommuniceerd.

- De reikwijdte van het beleid is duidelijk, doordat is bijgehouden waar persoonsgegevens worden verwerkt (criterium U.02 Gegevensmanagement; in de Privacy Baseline: Register van verwerkingsactiviteiten).

Sturend beleid:

- Wijzigingen in het beleid zijn duidelijk, bekend en worden planmatig doorgevoerd.
- Investeringen in privacybescherming zijn beoordeeld op korte- en langetermijneffecten, gevolgen voor andere verwerkingen en afdelingen, toegevoegde waarde voor de organisatie en de naleving van de architectuurprincipes.
- De criteria voor investeringen zijn gedefinieerd en er is een helder en bekend goedkeuringsproces.
- De privacygerelateerde budgetten zijn actueel en hebben herkenbare verantwoordelijken.

Cyclisch beleid:

- Er is een feedbackmechanisme geïmplementeerd voor het optimaliseren en continu verbeteren van het beleid.
- Er is een hoge mate van standaardisatie van het beleid, processen en procedures.

3.2.2 Organieke inbedding - B.02

Organieke inbedding van privacy binnen de organisatie betekent het toewijzen van Taken, Verantwoordelijkheden en Bevoegdheden (TVB's[11]) aan personen die vanuit hun functie en positie invulling kunnen geven aan de doelstellingen van het privacybeschermingsbeleid. Afspraken over de onderlinge verwachtingen worden gemaakt door het vastleggen van een goede, inzichtelijke taakverdeling en de daartoe benodigde middelen en rapportagelijnen. Input voor de organisatorische inbedding zijn het organogram van de organisatie en gesprekken met de stakeholders binnen de organisatie.

Kritische succesfactoren

Organisatie:

- De processen, diensten en functies die nodig zijn voor het realiseren van de ACT-doelen liggen vast, maar zijn flexibel en aanpasbaar met een transparant wijzigingsproces.
- De essentiële privacyfuncties worden expliciet benoemd in het organisatiemodel, met duidelijk omschreven TVB's.
- De privacy-organisatie is flexibel aan te passen aan veranderende situaties en kan inspelen op crisissituaties.
- Er zijn duidelijke beleids-, uitvoerings- controlprocessen, met segregatie van functies.
- Er is duidelijkheid over wie deelverantwoordelijk en wie eindverantwoordelijk is voor een taak. Dit groeit mee met de volwassenheid van de organisatie.
- Voor iedere gegevensverwerking is duidelijk wie eindverantwoordelijk is voor de privacy.

[11] TVB: gangbare term voor bij een functie horende beschrijving van Taken, Verantwoordelijkheden en Bevoegdheden; bij voorkeur in een 'TVB-matrix' vastgelegd in relatie tot de overige functies in de organisatie.

- Op organisatieniveau is duidelijk wie eindverantwoordelijk is voor de privacy.
- Binnen de privacy-organisatie is ruimte voor succesvolle samenwerking en een open houding.
- De verantwoordelijken voor privacybescherming zijn georganiseerd; zij worden betrokken bij alle processen voor de totstandkoming van een gegevensverwerking.
- Door het nemen van verantwoordelijkheden te stimuleren ontwikkelt de organisatie zich, groeien individuen en verbetert de samenwerking.
- Het management geeft het goede voorbeeld.
- Het management ondersteunt skills-doelstellingen (zoals bedoeld in paragraaf 3.1.7) ten aanzien van de privacy-organisatie.
- De privacyprocessen zijn nauw geïntegreerd in de gelijkende processen.

Middelen:

- Er is een proces om het bewustzijn, begrip en naleving van beleid te bepalen en desgewenst bij te sturen.
- Gebruik kennismanagement, workflowtechnieken en geautomatiseerde hulpmiddelen voor het ontwikkelen, verspreiden en handhaven van procedures.
- Plannen om de hiaten in de kennis op te vullen worden gerealiseerd.
- Een veranderde gegevensverwerking en visie op privacybescherming worden consequent doorvertaald naar de opleiding en werving van personeel.
- Identificeer en budgetteer alle aan de organieke inbedding gerelateerde kosten.
- Er is een trainingsprogramma voor de belanghebbenden, zodat er een gemeenschappelijk gedeeld beeld kan ontstaan over privacy en het te hanteren privacybeleid.
- De trainingsprogramma's zijn gebudgetteerd en er zijn resources, faciliteiten en trainers.

3.2.3 Risicomanagement, Privacy by Design en de DPIA - B.03

Risicomanagement is een continu proces dat de (privacy)risico's signaleert, beoordeelt en risico's verkleint en bewaakt. Input voor het bepalen van de risico's zijn het samenhangende beeld van de verwerkingsarchitectuur en de ontwerpen van de gegevensverwerkingen - met als basis de principes van Privacy by Design [11].

Het bepalen van privacyrisico's, bijvoorbeeld met een DPIA, brengt in beeld welke maatregelen nodig zijn zodat de verwerking van de persoonsgegevens aan het belang van de betrokkene en de organisatie voldoet. Minimaal voert de verantwoordelijke voor de gegevensverwerking DPIA's uit.

Kritische succesfactoren

- Er is een actueel, compleet en duidelijk overzicht waaruit duidelijk wordt waar risicoanalyses moeten worden uitgevoerd; onder invloed van de AVG wordt dit doorgaans het "register van verwerkingsactiviteiten" genoemd (U.02).
- Kennis en ervaring met het hanteren van de principes van Privacy by Design is voorhanden en georganiseerd.
- Bekend is door welke verantwoordelijken de principes van Privacy by Design worden bewaakt.

- Bekend is door welke verantwoordelijken de risicobeoordelingen/DPIA's uitgevoerd moeten worden.
- Kennis en ervaring met het uitvoeren van risicobeoordelingen/DPIA's is voorhanden en georganiseerd.
- Gestructureerde risico-informatie wordt onderhouden, gevoed door DPIA's en het melden van privacy-incidenten.
- De focus van de beoordeling van de privacyrisico's is in de eerste plaats gericht op de echte bedreigingen en minder op de theoretische risico's.
- De resultaten van DPIA's worden beoordeeld op mogelijke datalekken.
- Verantwoordelijkheden en procedures voor het doorvoeren van verbeteringen als gevolg van de privacyrisico's liggen vast.
- Risicobeoordelingen/DPIA's worden periodiek uitgevoerd.
- De te investeren tijd en inspanning zijn in overeenstemming met de omvang en vertrouwelijkheid van de persoonsgegevens.

3.3 Kritische succesfactoren in het uitvoeringsdomein

De uitvoering is waar het gebeurt: de handmatige en geautomatiseerde verwerkingsprocessen, inclusief de bijbehorende IT-systemen. Belangrijk is dat wat er gebeurt in lijn is met de vereisten en de ambities (het beleid). Daar waar ruimte voor compromissen is, komen die weloverwogen tot stand en niet noodgedwongen en ad hoc.

3.3.1 Doelbinding gegevensverwerking - U.01

Het vastleggen van het doel van de gegevensverwerkingen zorgt ervoor dat voor ieder persoonsgegeven de keuze om te verwerken weloverwogen en te rechtvaardigen wordt gemaakt. Het doel moet daarvoor welbepaald en uitdrukkelijk omschreven zijn vóórdat de verwerking begint en er moet getoetst worden of de verwerking van de gegevens noodzakelijk is voor het bereiken van het doel en er geen privacyvriendelijk(er) alternatief voorhanden is. Input voor het bepalen van het doel zijn: het privacybeleid (B.01) inclusief de geldende wet- en regelgeving, en overzicht op de verwerkingen, samen met de bijdrage vanuit gegevensmanagement (U.02).

Het resultaat van de vastlegging vormt een belangrijk instrument voor de informatieverstrekking aan betrokkenen (U.05) en de processen binnen het controldomein (C.01 - C.03).

Kritische succesfactoren

- Er is een duidelijke, begrepen en aanvaarde methode voor systeemontwikkeling van gegevensverwerkingen en begrip van de levenscyclus van de verwerking.
- Een gegevensverwerking is gedefinieerd, inclusief de context, zodat een duidelijk beeld bestaat van de lopende werkzaamheden. investeringen en de gebruikte en beoogde technologie.
- De keuze om persoonsgegevens te verwerken is beoordeeld op de korte- en langetermijneffecten, gevolgen voor andere verwerkingen en afdelingen, toegevoegde waarde voor de organisatie en de naleving van de wet- en regelgeving.

- De beslissing om persoonsgegevens te verwerken wordt gemaakt na een expliciete afweging, waarbij *dataminimalisatie* het uitgangspunt is: bij het verzamelen en verwerken van persoonsgegevens worden niet meer gegevens gebruikt dan nodig is om het doel waarvoor ze gebruikt zullen worden te bereiken.
- Op basis van U.01 is de legitimiteit van de gegevensverwerkingen bepaald. Handvatten om de rechtmatigheid en de noodzaak te bepalen zijn beschreven in paragraaf 3.1 van het document Privacy by Design: Overwegingen bij de verwerking van persoonsgegevens.
- De keuze om persoonsgegevens te verwerken is of wordt mede genomen op basis van de afweging of de verwerking bijdraagt aan het doel van de verwerking en of ook met minder persoonsgegevens het doel kan worden bereikt. Een juiste afweging kan de kosten van de naleving van wet- en regelgeving (aanzienlijk) beperken.
- De afwegingen om persoonsgegevens te verwerken en de resultaten van de juridische toetsing en goedkeuring zijn per gegeven vastgelegd (U.02).

3.3.2 Register van verwerkingsactiviteiten - U.02

Het bijhouden van het register van verwerkingsactiviteiten, inclusief gegevensmanagement, heeft tot doel te ervoor te zorgen dat iedere verwerking van een persoonsgegeven aan de wettelijke vereisten voldoet én bekend is. Het register creëert overzicht, voorkomt onnodige gegevensuitwisseling, zowel intern als extern, en maakt kwaliteitsmanagement volgens criterium U.03 mogelijk.

De doelen van de verwerking, de daarbij geldende wet- en regelgeving en het overzicht op de verwerkingen zijn input voor gegevensmanagement en worden gebruikt om de doelen scherp en duidelijk te houden. Het resultaat van gegevensmanagement is een beschrijving van ieder gegeven en een overzicht en samenhang van gegevens ten behoeve van de processen binnen het controldomein.

Om daarbij een overzicht te hebben van hoe en door wie gegevens worden verzameld en verwerkt en wat de onderlinge samenhang en afhankelijkheden zijn van de verwerkingen, processen en technische systemen, is het vaststellen van de *verwerkingsarchitectuur* een vereiste.

> Alleen aan de hand van een compleet beeld kun je aantonen dat de organisatie bedrijfsbreed grip op privacy heeft.

Kritische succesfactoren

- Een proces voor het beheer van (persoons)gegevens is beschikbaar.
- Gegevensmanagement is organisatiebreed ingericht; gegevensmanagers hebben voldoende hoog niveau en voldoende bevoegdheden om het gegevensmodel, inclusief gegevensdefinities, te beheren.
- De verantwoordelijken voor het beheer zijn bekend en geaccepteerd.
- De vastlegging van het gegevensmodel en de metagegevens zijn volledig en up-to-date en beschikbaar.
- Gegevensdefinities zijn gedocumenteerd, gecommuniceerd en worden gebruikt.

- De keuze voor het verwerken van een persoonsgegeven wordt duidelijk gedocumenteerd en bewaakt.
- Het overzicht in de vorm van een gegevensmodel is eenvoudig en duidelijk.
- Het gegevensmodel en de metagegevens definiëren en sturen de gegevensverwerking.
- Geautomatiseerde ondersteuning van het beheer van de metagegevens zorgt voor het beheren en bewaken van de samenhang tussen de onderdelen van de IT- en applicatiearchitectuur, informatiearchitectuur, gegevensdefinities, gegevensclassificaties en veiligheidsniveaus.

3.3.3 Kwaliteitsmanagement - U.03

Kwaliteitsmanagement zorgt ervoor en bewaakt dat de verwerking van persoonsgegevens correct gebeurt en niet leidt tot nadelige gevolgen in de persoonlijke levenssfeer van betrokkenen. Is dit toch het geval dan corrigeert kwaliteitsmanagement. De kwaliteit van de gegevens wordt continu bewaakt.

De kwaliteitsprocessen zijn daarmee integraal onderdeel van de primaire bedrijfsprocessen. Zij kunnen betrokkenen laten zien of hun persoonsgegevens nog actueel en correct zijn (C.02). Zij herbergen de processen die persoonsgegevens kunnen corrigeren of verwijderen.

Kritische succesfactoren

- Het borgen van privacy in de bedrijfsprocessen is gedefinieerd, overeengekomen en ingericht om de kwaliteitsborging uit te voeren.
- Betrokkenen kunnen door middel van toegang de (on)juistheid van de gegevens controleren.
- De kwaliteit van persoonsgegevens wordt door de organisatie bepaald met duidelijke rollen voor de kwaliteitsborgingprocessen en procedures voor kwaliteitscontrole.
- De verantwoordelijkheden voor de integriteitseisen en de integriteit zijn duidelijk en zijn in de gehele organisatie geaccepteerd.
- Er heerst een positieve kwaliteitscultuur, bevorderd door alle lagen van het management.
- Elke gegevensverwerking kent processen voor een goede kwaliteitsborging.
- Het belang van de integriteit van gegevens wordt duidelijk gecommuniceerd en meegenomen in de ontwikkeling van de verwerkingsprocessen.
- De kwaliteit van de gegeven en de correctie van onjuiste gegevens vindt plaats bij ontvangst van de gegevens, zodat onjuiste conclusies door onjuiste gegevens direct na ontvangst al worden voorkomen.
- (Vermoedelijk) onjuiste gegevens worden in quarantaine gehouden totdat ze zijn gecontroleerd en zonodig gecorrigeerd.
- Effectieve detectiemethoden worden gebruikt om de nauwkeurigheid en integriteit van de gegevens te bewaken.
- Handmatige gegevensinvoer is tot een minimum beperkt.

3.3.4 Het beveiligen van persoonsgegevens - U.04

Informatiebeveiliging heeft tot doel eventuele gevolgen van beveiligingsincidenten te beperken. De maatregelen bestaan uit organisatorische, technische en fysieke maatregelen die gebaseerd zijn op een

(organisatieafhankelijke) risicoanalyse en wettelijke verplichtingen (waaronder de (U)AVG). Informatiebeveiliging vult criterium U.04 van de privacyvereisten in. Het is dus een misvatting dat privacybescherming onderdeel is van informatiebeveiliging. Informatiebeveiliging is een van de instrumenten voor privacybescherming.

Daar waar maatregelen voor informatiebeveiliging en privacybescherming overeenkomsten vertonen, kunnen taken en verantwoordelijkheden worden gedeeld en kunnen taken gecombineerd worden uitgevoerd.

Kritische succesfactoren

- Beveiligingsrisico's in de gegevensverwerking zijn proactief bepaald en zijn duidelijk toegewezen aan de verantwoordelijken.
- Bij het uitvoeren van de risicoanalyses is er extra aandacht voor bijzondere persoonsgegevens en uniek identificerende gegevens.
- Er is een beveiligingsplan dat het bewustzijn vergroot, duidelijk beleid en normen stelt, een kosteneffectieve en duurzame uitvoering initieert en de controle en handhaving bepaalt.
- Het besef leeft dat een goed beveiligingsplan tijd nodig heeft om te evolueren.
- Op bedrijfsniveau wordt over informatiebeveiliging aan het senior management gerapporteerd en is er één verantwoordelijke voor het uitvoeren van het veiligheidsplan.
- Er zijn procedures voor het officieel certificeren en accrediteren van de beveiliging van systemen.
- Management en medewerkers hebben een gemeenschappelijke visie op de beveiligingseisen, kwetsbaarheden en bedreigingen; ze begrijpen en accepteren hun eigen en elkaars verantwoordelijkheden ten aanzien van de informatiebeveiliging.
- Er is goede kennis van passende beveiligingsoplossingen in de markt.
- Een open uitwisseling over ontwikkelingen en goede relaties met leveranciers en derden bevordert de inzet van passende oplossingen.
- Het beveiligingsbeleid is in overeenstemming met de beveiligingsrisicobeoordelingen en de beveiligingsprocessen.
- Rapportages over de status van de informatiebeveiliging worden periodiek gedeeld met het management, de IT- en de lijnorganisatie.
- Monitoring van de beveiliging vindt plaats en het resultaat wordt tot en met senior managementniveau geëvalueerd. Eventuele noodzakelijke of gewenste acties worden afgesproken en vertaald naar oplossingen en eventuele gevolgen voor de begroting.
- De beveiligingsfunctie heeft de middelen en het vermogen te reageren op beveiligingsincidenten als ze zich voordoen, ze op te sporen, te analysen, te registreren en erover te rapporteren. Denk hierbij niet alleen aan inbreuken door hackers, maar ook bijvoorbeeld aan datalekken.

3.3.5 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens - U.05

Het verstrekken van informatie dient ervoor transparant te zijn naar betrokkenen over het verzamelen en het verwerken, inclusief eventuele doorgifte, van de persoonsgegevens over betrokkene. Om dit te kunnen doen moet een actueel overzicht bekend en inzichtelijk gedocumenteerd zijn (U.02) van waar, hoe en door wie de gegevens worden verwerkt.

Kritische succesfactoren

- Er is vooraf bepaald of er een *informatieplicht* aan betrokkenen is.
- De eisen die aan de informatieverstrekking aan betrokkenen wordt gesteld zijn duidelijk en worden gehanteerd.
- De uitleg over hoe de privacy is gewaarborgd (privacyverklaring), is uitgedrukt in voor betrokkenen begrijpbare taal en up-to-date.
- Er is een Frequently Asked Questions (FAQ's), antwoorden zijn up-to-date, gemakkelijk toegankelijk en begrijpelijk voor de doelgroep.
- Er is een duidelijke en gemakkelijk toegankelijke klachtenprocedure.
- Er is een klachtafhandelingsproces dat is aangehaakt bij kwaliteitsmanagement.

3.3.6 Bewaren van persoonsgegevens - U.06

Het beperken van de bewaartermijn van persoonsgegevens moet ertoe leiden dat de gegevens niet langer worden bewaard dan nodig voor het doel of de doelen waarvoor ze zijn verzameld.

Input voor het bepalen van de bewaartermijn zijn de doelen die door gegevensmanagement zijn gedocumenteerd. Afspraken over het beperken van de bewaartermijn worden gemaakt met de verantwoordelijke(n) voor de verwerking(en). Voor sommige gegevens gelden wettelijke bewaarplichten en -termijnen, bijvoorbeeld - maar niet alleen - vanwege de Archiefwet [12].

Kritische succesfactoren

- Van alle gegevens die worden bewaard is de noodzaak van het bewaren bepaald. Als de noodzaak niet voldoende is, wordt het gegeven niet bewaard.
- (Sectorspecifieke) wetgeving over bewaartermijnen is bekend.
- De bewaartermijn en de gronden ervoor worden vastgelegd door gegevensmanagement.
- Bij het technisch ontwerp van de gegevensopslag wordt rekening gehouden met de maatregelen voor het verwijderen of anonimiseren van de gegevens; hoe dit te doen is vastgelegd in een procedure[12].
- Bij het ontwerp van de verwerkingen is rekening gehouden met het verwijderen dan wel anonimiseren van de gegevens.

[12] Merk op dat een geanonimiseerd gegeven geen persoonsgegeven in de zin van de AVG meer is, want immers niet meer tot een natuurlijke levende persoon herleidbaar. Pas op: een gepseudonimiseerd gegeven valt nog wél onder de AVG. Meer hierover kun je vinden in de CIP-publicatie "Testen met persoonsgegevens" [13].

3.3.7 Doorgifte persoonsgegevens - U.07

Het procesmatig inrichten van de doorgifte van persoonsgegevens aan 'derde partijen' moet borgen dat altijd goede afspraken bestaan over het beschermen van de privacy in en na het doorgifteproces. De organisatie die aanlevert is en blijft immers eindverantwoordelijk om aan de wet- en regelgeving te voldoen, tenzij het eigenaarschap van een gegeven expliciet wordt overgedragen en er dus een nieuwe verantwoordelijke voor de (nieuwe!) verwerking is. Persoonsgegevens worden alleen doorgegeven nadat:

- Aan de in U.07 beschreven eisen voor de doorgifte is voldaan;
- De afspraken in een overeenkomst zijn vastgelegd;
- Alle daarvoor vereiste maatregelen aantoonbaar zijn ingericht.

Kritische succesfactoren

- Er is een formeel, aanvaard, begrepen en gehandhaafd proces voor de selectie en inzet van partijen aan wie persoonsgegevens worden en zijn doorgegeven.
- Er is bekend welk deel van de verwerking, inclusief toegang tot de verwerking, buiten de Europese Unie plaatsvindt, zodat bekend is of rekening gehouden moet worden met lokale wetgeving buiten de Europese Unie.
- Er is een aanpak gedefinieerd om weloverwogen keuzes te maken tussen interne en externe verwerking van (delen van) de gegevensverwerking (uitbesteding).
- Contracten met de partijen aan wie persoonsgegevens worden doorgegeven zijn met goed gevolg onderworpen aan een juridische toetsing en goedkeuring.
- Er zijn goed gedefinieerde contracten met derde partijen (onderaannemers).
- Een interne contractmanager is het single point of contact met en voor de partijen aan wie persoonsgegevens worden doorgegeven.
- Er is een duidelijke definitie van verantwoordelijkheden en aansprakelijkheden van de partijen aan wie persoonsgegevens worden en zijn doorgegeven.
- De relaties met derde partijen zijn goed ontwikkeld.
- De aanleverende organisatie behoudt verantwoordelijkheid en voert controle uit op de verwerking van persoonsgegevens buiten de eigen organisatie.
- De partijen aan wie persoonsgegevens worden doorgegeven hebben een gedocumenteerde voorziening in werking voor het rapporteren over de privacybescherming.
- Ook bij de partijen aan wie persoonsgegevens worden doorgegeven zijn informatiebeveiliging en kwaliteitsmanagement beschreven en aantoonbaar in werking.

3.4 Kritische succesfactoren in het control-/beheerdomein

Binnen het control-/beheerdomein gaat het over het bieden van transparantie over de privacybescherming, zowel intern als extern. Dit gaat verder dan het waarborgen dat de juiste dingen gebeuren. Het moet aantoonbaar gewaarborgd ('gecertificeerd') zijn.

3.4.1 Intern toezicht - C.01

Het toezicht binnen de eigen organisatie heeft tot doel vast te stellen of de gegevensverwerkingen rechtmatig zijn en of daarvoor de juiste maatregelen zijn getroffen, zodat voldaan wordt aan de eisen van de AVG, sectorspecifieke wetgeving en/of een (eventuele) Gedragscode [14].

Toezicht is mogelijk doordat vanuit de uitvoering wordt gerapporteerd over hoe aan de wettelijke vereisten wordt voldaan en welke technische en organisatorische maatregelen daarvoor zijn genomen. Bevindingen vormen de input voor het compliancyproces, zodat de verwerking van de persoonsgegevens kan worden bijgestuurd, al dan niet door het bijstellen of uitbreiden van het beleid. Bevindingen kunnen het gevolg zijn van veranderde wet- en regelgeving, nieuwe inzichten, ambities of ervaringen.

Kritische succesfactoren

- Het interne toezicht wordt als onderdeel van het compliancyproces gedefinieerd met een duidelijk doel, gedocumenteerd en geïmplementeerd, op basis van zakelijke behoeften en verplichtingen en met eenduidige verantwoordelijkheden.
- Een positieve kwaliteitscultuur wordt consequent bevorderd door alle lagen van het management, zodat er een duidelijk commitment van het management is om op te treden bij tekortkomingen in de interne controle.
- De activiteiten zijn geïntegreerd in het governanceproces en het leiderschapsgedrag.
- De verantwoordelijkheden, inclusief de gedelegeerde verantwoordelijkheden, voor het aantonen van de compliancy zijn vastgesteld en gecommuniceerd.
- Er is een onafhankelijke partij die toezicht houdt op de uitvoering van de compliancyprocessen en die de mate van compliancy beoordeelt.
- Er is een keuze gemaakt voor benodigde middelen, inclusief de elektronische hulpmiddelen.
- Het rapportageproces dat nodig is voor toezicht is afgesproken en past bij de uitvoering.
- Actuele managementrapportages zijn tijdig beschikbaar.
- Aan het definiëren en maken van rapportages zijn eisen gesteld.
- Het vereiste kennisniveau voor het maken van de planningen, evaluaties, registraties en de rapportages zijn bekend.
- Het management bepaalt welke gegevensverwerkingen moeten worden gecontroleerd.
- Er is een gedetailleerd controlproces gedefinieerd en actief.
- Er is een proces gedefinieerd en actief voor het tijdig melden van gebreken in het controlproces.
- De interne controlegegevens zijn juist, volledig en tijdig.
- Er is een proces gedefinieerd en actief voor het delen van kennis over de interne controle van incidenten en te nemen maatregelen.
- De mate van compliancy en het volwassenheidsniveau zijn inzichtelijk en gepubliceerd.
- Er is een voortdurende afstemming over de behoeften met belanghebbenden.

- Er is een actieve samenwerking tussen de controleur en de gecontroleerde; deze samenwerking wordt aangemoedigd en bevorderd.

3.4.2 Toegang gegevensverwerking voor betrokkenen - C.02

Burgers moeten toegang hebben tot informatie over de gegevensverwerking die hen in staat stelt te beoordelen of de gegevensverwerking rechtmatig en correct plaatsvindt.

Hiervoor is het nodig dat toegang technisch of organisatorisch mogelijk is en dat bij het ontwerp van de gegevensverwerking en de realisatie met deze functionaliteit rekening is gehouden.

Kritische succesfactoren

- De aanspreekpunten en processen zijn ingericht om betrokkenen te ondersteunen bij hun informatievraag.
- De verwerkingen van persoonsgegevens zijn bijgehouden (U.02), inclusief de logica die ten grondslag ligt aan de verwerking.
- Lessen uit de vragen die gesteld zijn worden vertaald naar verbetervoorstellen in de informatieverstrekking naar betrokkenen en zo nodig het beleid.
- Er is deskundig klantgericht en klantondersteunend personeel beschikbaar om vragen te beantwoorden. Zo mogelijk is een webcare-team actief[13].
- Alle gebruikersvragen worden consequent geregistreerd.
- Gebruikersvragen die niet tijdig op een passende wijze kunnen worden opgelost worden geëscaleerd.
- Aan de vragensteller wordt een beoordeling van de antwoorden en de procedure gevraagd; deze beoordeling wordt geregistreerd en meegenomen in de verbetercyclus.

3.4.3 Meldplicht Datalekken - C.03

Een datalek wordt gemeld aan de Autoriteit Persoonsgegevens (AP) en de betrokkene als sprake is van een ernstige inbreuk op de beveiliging van persoonsgegevens die leidt tot (de aanzienlijke kans dat) ernstige nadelige gevolgen intreden voor de bescherming van persoonsgegevens. Het bieden van inzicht in de aard van het lek, de mogelijke gevolgen ervan en het aanbieden van advies hoe te handelen kan de (negatieve) consequenties voor de betrokkenen beperken.

Een datalek wordt doorgaans ontdekt of komt als incident binnen bij de verantwoordelijken voor informatiebeveiliging. Nadelige gevolgen van een datalek kunnen door het treffen van passende technische en procedurele maatregelen worden voorkomen of worden gematigd (bijvoorbeeld door toepassing van encryptie). Gedetailleerde kennis van de verwerkingen en de toegepaste maatregelen is hierbij een noodzakelijke bron van informatie (U.04). Als deze maatregelen niet zijn toegepast of restrisico's laten bestaan dan moet het datalek als ernstig worden beschouwd en binnen 72 uur aan de AP worden gemeld, al naar gelang de verdere omstandigheden ook aan de betrokkenen.

[13] Een webcareteam is een afdeling die alle interactie op sociale media namens het bedrijf verzorgt (https://www.marketingtermen.nl/begrip/webcareteam). Organisaties kunnen dit ook uitbesteden.

Kritische succesfactoren

- Er is een procedure om na een melding het bestaan, de oorzaak en de gevolgen van de inbreuk te bepalen en vast te leggen dat dit is gebeurd.
- In geval van uitbestede verwerkingen van gegevens liggen de verantwoordelijkheden en de aansprakelijkheden van alle betrokken partijen in overeenkomsten vast.
- De meldingsprocedure en de verantwoordelijkheden wordt duidelijk begrepen en kent een classificatie van de ernst van de meldingen; de classificatie bepaalt de prioriteit van de afhandeling.
- Degenen die betrokken zijn bij de procedure om de aard en gevolgen van de inbreuk te bepalen hebben kennis van de verschillende verschijningsvormen die een 'datalek' kan aannemen.
- De focus van de beoordeling van de privacyrisico's is op de echte bedreigingen. Om een goed beeld te hebben waar bedreigingen zich voordoen is een samenhangend beeld van de gegevensverwerkingen beschikbaar (U.02).
- Verantwoordelijkheden en procedures voor het doorvoeren van verbeteringen naar aanleiding van datalekincidenten liggen vast.
- Om de objectiviteit te verhogen kan een 'reality check' op de privacyrisico's en de voorgestelde maatregelen worden uitgevoerd door een derde partij; deze check wordt op gepaste tijdstippen herhaald.
- De resultaten van DPIA's zijn beoordeeld op mogelijke datalekken.
- Er is een procedure om een datalek te melden aan de Autoriteit(en).
- Er is een procedure om een datalek te melden aan betrokkene.
- Er is beschreven hoe en op basis van welke afweging de gegevensverwerking wordt gestopt na een melding.

Deel 2: Toelichtingen

In deel 1 hebben we de kritische succesfactoren beschreven en hoe je vorm kunt geven aan de verandering naar meer grip op privacy. We hebben daarbij soms verwezen naar toelichtingen in deel 2.

Je vindt deze toelichtingen in de volgende paragrafen. Op een aantal aspecten gaan we bovendien dieper in. Ze zijn bijeen gepakt in de volgende thema's:

- KSF's voor de realisatie van de criteria in de Privacy Baseline;
- Aandachtspunten voor het doorvoeren van een verandering;
- Aandachtspunten bij het samenstellen van een team en hoe een team de verandering op een door de organisatie gedragen manier mogelijk kan maken.

4 Toelichting op het toepassen van de Privacy Baseline

- In hoofdstuk 4 vind je toelichtingen en uitbreidingen bij de kritische succesfactoren in relatie tot de Privacy Baseline.
- Hoofdstuk 5 is gewijd aan verandermanagement in het teken van privacyvolwassenheid.

Sneak preview voor wie snel wil zien wat hem te wachten staat: kijk naar de lijstjes in de paragrafen 5.2.6 en 5.2.7.

4.1 Privacy beleid - B.01

Beleid wordt opgesteld door passende invulling te geven aan de volgende twee doelstellingen:

- **Transparantie over privacy:**
  Vanuit de wet- en regelgeving is transparantie vereist over hoe wordt omgegaan met de vertrouwelijkheid van persoonsgegevens. Deze transparantie is nodig voor enerzijds compliancy en accountability en anderzijds voor duidelijkheid naar de betrokkenen van wie persoonsgegevens worden verwerkt. Alledrie de motieven zijn wettelijke vereisten.
- **Sturing geven aan de implementatie en control:**
  Ambities qua te behalen privacydoelen en wat daarvoor nodig is verschillen in de praktijk per organisatie. De verschillen zijn ingegeven door verschillen van mening over prioriteit, de haalbaarheid en de termijnen, waarbinnen een en ander is te realiseren. Dit geldt ook voor het te behalen volwassenheidsniveau. Helderheid over de ambities is een vereiste om te komen tot realiseerbare ambities.

4.1.1 Het belang van het overzicht

De interne gegevenshuishouding van organisaties, zoals die gevat is in logische en technische datamodellen, is complex en hetzelfde geldt voor de geautomatiseerde systemen waar ze mee werken. Organisaties werken ook samen en delen en gebruiken daarbij gegevens afkomstig van andere organisaties. Het stelsel van gegevensverwerkingen dat daardoor ontstaat, is een keten met intensief verkeer tussen organisaties en verwerkingen, waarbij iedere verwerking zijn eigen doelbinding kent. Zo ontstaat een stelsel van doelbindingen en wettelijke grondslagen voor doorgifte van gegevens en dat moet beheerd kunnen worden.

Het creëren van overzicht op waar en door wie welke persoonsgegevens worden verwerkt, is een randvoorwaarde voor transparantie. Het hanteren van een architectuur, waarbij een overzicht wordt gegeven van de opgeslagen en gebruikte persoonsgegevens, de gegevensstromen en de verwerkingen met hun doelbindingen is een beproefde manier om inzicht te kunnen geven.

> Transparantie vraagt om overzicht, overzicht vraagt om een architectuur en architectuur vraagt om kennis om de architectuur beheersbaar te houden.

Om sturing te kunnen geven aan de organisatie bij het implementeren van het beleid en om te komen tot compliancy moeten verschillende administratieve processen worden ingericht. De vastlegging van de

verwerkingen zijn administratieve processen, waarbij meerdere partijen betrokken zijn. Wie betrokken is, is beschreven in de TVB-matrix.

> De administratieve processen geven overzicht op de verwerking van persoonsgegevens door en namens de organisatie.

4.1.2 Sturend beleid

Alleen met een duidelijke visie van het management kan de organisatie zich bewust zijn van het belang van privacybescherming en wordt het realiseren van de ACT-privacydoelstellingen mogelijk. Het management moet zich een beeld vormen van hoe de organisatie zich naar buiten (maar ook naar binnen) wil positioneren met het waarborgen van de privacy, de risico's op imagoschade en de mate waarin de organisatie transparant wil zijn. De visie van de organisatie op de waarde van privacy-bescherming is bepalend voor de maatregelen die worden genomen voor de gegevensverwerking en de maatregelen die worden genomen om aantoonbaar in control te zijn. Belangrijk is dat die visie wordt vastgelegd in het (privacy)beleid van de organisatie.

Bij sturend beleid horen budgetten. Het tijdstip waarop de visie - de ambitie - moet zijn gerealiseerd en of de organisatie al maatregelen heeft getroffen zijn mede bepalend voor het tijdschema van een privacyprogramma en de beschikbaar te stellen budgetten.

> Het beleid geeft helderheid aan de organisatie en de betrokkenen over de ambitie, de inzet van de bestaande organisatie, het tijdpad en hoe hier invulling aan gegeven wordt.

4.1.3 Helder beleid

Het schrijven van helder beleid is voor velen niet een vanzelfsprekendheid. Daarnaast is het ook voor de meer ervaren beleidsmakers niet iets wat in handomdraai gebeurt. De mate waarin kennis van de wet- en regelgeving beschikbaar is en de mate waarin de inhoudsdeskundigen betrokken kunnen worden zijn bepalend als het beleid vanuit het niets 'in een groene weide' moet worden ontwikkeld. Beter is het om uit te gaan van best practices in andere organisaties en deze aanvankelijk met zo weinig mogelijk aanpassingen naar de eigen situatie te vertalen.

Bij het schrijven van helder privacybeleid moet je rekening houden met de doelgroep. Hierbij is er in ieder geval onderscheid te maken tussen het beleid voor intern gebruik en beleidsteksten voor extern gebruik.

- Beleid voor intern gebruik: hiervoor kan gebruik gemaakt worden van criterium B.01, dat beschrijft hoe invulling wordt gegeven aan de wet- en regelgeving, inclusief de eventuele sectorspecifieke wet- en regelgeving en/of gedragscode. Privacybeleid beslaat meerdere aandachtgebieden. Door het privacybeleid op te splitsen naar de verschillende

aandachtsgebieden, zoals in de Privacy Baseline staat beschreven, kun je beleidsonderdelen toewijzen aan de daarvoor verantwoordelijke(n).

- Beleid voor extern gebruik: hiervoor is in ieder geval een privacyverklaring nodig. Adresseer daarin zeker de volgende punten:
  - De privacyverklaring geeft duidelijkheid over de volgende onderwerpen:
    - Welke persoonsgegevens worden verzameld.
    - Voor welk doel worden de verzamelde persoonsgegevens verwerkt en welke (sectorspecifieke) wet- en regelgeving en/of gedragscode wordt gehanteerd.
    - Hoe de betrokkene controle kan blijven houden over de verzamelde persoonsgegevens door ze in te zien, te corrigeren en zo mogelijk te laten verwijderen.
    - Hoe wordt omgegaan met (de duur van) het bewaren van de persoonsgegevens.
    - Met welk doel worden de verzamelde persoonsgegevens gedeeld met andere organisaties, welke afspraken worden daarbij gemaakt en hoe worden de betrokken daarover vooraf geïnformeerd (zie U.07 in deel 1 om welke afspraken het gaat).
    - Hoe de betrokkene controle heeft over de afgesloten contracten met derden en hoe betrokkene hierover *vooraf* wordt geïnformeerd, zodat hij/zij controle heeft over de persoonsgegevens die met derden worden gedeeld.
    - Welke trackinggegevens, zoals surfgedrag, worden bijgehouden. Als deze gegevens in een cookie zijn opgeslagen, maak dan de betrokkene duidelijk dat de cookies weer verwijderd kunnen worden.
    - Hoe wordt omgegaan met vragen of klachten betreffende de privacy en de beveiliging van de persoonsgegevens.
    - Hoe veranderingen als gevolg van wijzigingen in wet- en regelgeving of de visie of bedrijfsstrategie worden doorgevoerd in de privacyverklaring.
    - Vermeld de datum van de privacyverklaring in het document zelf.
  - Geef per onderwerp, als de beschrijving niet voor zichzelf spreekt, een korte uitleg van de betekenis van het onderwerp in *voor de betrokkene* begrijpelijke en toegankelijke vorm
  - Hou de verklaring kort en bondig, voorkom het gebruik van vaktermen en geef daar waar het gebruik van de vaktermen niet vermeden kan worden, ook weer kort en bondig uitleg.

Kort en bondig is overigens relatief: bij het gebruik van het taalniveau B1, wat is aanbevolen[14], worden teksten doorgaans langer door de noodzaak om meer expliciet uit te schrijven. Een goede tip: laat je teksten (professioneel) testen door beoogde lezers.

[14] Op internet is gemakkelijk alle informatie over taalniveaus of taalniveau B1 te vinden.

4.2 Organisatorische inbedding - B.02

4.2.1 Groeien in volwassenheid

De Baseline laat duidelijk zien dat de verantwoordelijkheid voor privacy, gezien de verscheidenheid aan kennisgebieden, een gedeelde verantwoordelijkheid is. Hoewel één (natuurlijke) persoon de (juridische) eindverantwoordelijkheid heeft, vraagt het invullen van de taken, verantwoordelijkheden en bevoegdheden (TVB) om afspraken tussen de verschillende betrokkenen in de kennisgebieden.

Hoe de verschillende verantwoordelijkheden ingevuld moeten worden, verschilt aanzienlijk per organisatie en daarmee per situatie. Dit komt enerzijds door verschillen in omvang van organisaties en anderzijds door verschillen in organisatievolwassenheid. Bij lage volwassenheid liggen veel taken en verantwoordelijkheden decentraal en is de centrale aansturing en bewaking beperkt of afwezig.

Door de TVB aan te laten sluiten op de ambitie van de organisatie kunnen de in de TVB vastgelegde taken, verantwoordelijkheden en bevoegdheden meegroeien met de groei in volwassenheid van de organisatie. Zo voorkom je dat taken en verantwoordelijkheden neergelegd worden bij organisatieonderdelen die daar niet de kennis en expertise voor hebben.

Het advies is daarom om bij het opzetten van de TVB, bijvoorbeeld in een TVB matrix, te beginnen met een analyse van de volwassenheid. Deze analyse maakt duidelijk waar verantwoordelijkheden liggen. Daarmee verkrijg je een beeld van waar taken en bevoegdheden belegd zijn (de IST-situatie). Door het uitspreken en op organisatieniveau vastleggen van het ambitieniveau in de privacyvolwassenheid (de SOLL-situatie) wordt een groeipad uitvoerbaar en haalbaar. De Privacy Baseline en het privacyvolwassenheidsmodel helpen de TVB's af te stemmen op de behoefte van de organisatie (de IST door te laten groeien naar de SOLL situatie).

> Vanuit de actuele volwassenheid (IST) wordt een groeipad voor het beleggen van TVB's opgesteld dat meegroeit met de groei in volwassenheid naar het ambitieniveau (SOLL) en dat op organisatieniveau is vastgelegd.

Dit vraagt om:

- Een overzicht van de bestaande functies en hun taken en verantwoordelijkheden en hun raakvlakken met het privacydomein.
- Inzicht in hun onderlinge verhoudingen, zoals hiërarchische relaties.
- Kennis van en overzicht op taken binnen het privacydomein en de omvang van de taken.
- Inzicht in welke taken aan welke functies kunnen worden toegewezen en eventueel welke aanvullende functie nodig zijn. Voor deze functies worden de bevoegdheden en verantwoordelijkheden aangepast aan de nieuwe taken.
- Inzicht in welke taken door de functionarissen kunnen worden uitgevoerd en of zij daarvoor voldoende tijd, kennis en vaardigheden hebben.

Het overzicht en het inzicht beperkt zich niet tot alleen de eigen organisatie, maar moet zich ook uitstrekken naar de verwerkings-ketenpartijen.

4.2.2 Eindverantwoordelijkheid op organisatieniveau

Waar de eindverantwoordelijkheid voor privacy wordt belegd verschilt per organisatie. Veelal is dat bij een jurist op de afdeling Juridische Zaken, een Chief Information Security Officer (CISO) of een IT-auditor, voor wie privacy dan een deeltaak is.

Wanneer een hogere volwassenheid bereikt moet worden kan privacy niet meer als parttime functie 'erbij' gedaan worden, vooral niet als het grotere organisaties betreft met een uitgebreide TVB-matrix.

Het aanwijzen van een eindverantwoordelijke is een minimum vereiste om invulling te geven aan privacygovernance en de groei in volwassenheid. Door de eindverantwoordelijkheid te borgen op organisatieniveau wordt voorkomen dat privacy wordt gezien als verantwoordelijkheid van een specifieke afdeling. De eindverantwoordelijke kan hierbij verantwoordelijk zijn voor de vastlegging van de resultaten van de privacybescherming. Hij heeft een directe lijn met het topmanagement, zoals de Raad van Bestuur of het College van B&W, zodat de governance voor privacy op organisatieniveau wordt geborgd en gestuurd kan worden via de afspraken die in de TVB zijn vastgelegd.

Het nakomen van de interne afspraken ten aanzien van privacy vraagt om een eindverantwoordelijke voor privacy en het borgen van de ambities op organisatieniveau.

4.2.3 Verantwoordelijkheid in ketens

Voor iedere gegevensverwerking moet duidelijk zijn wie verantwoordelijk is voor de privacy-bescherming. Ook in een ketensamenwerking moet de eindverantwoordelijkheid over de keten duidelijk zijn. Dit is gemakkelijker gezegd dan gedaan als in een samenwerkingsverband persoonsgegevens worden verzameld voor verschillende doelen en door verschillende ketenpartijen. De verantwoordelijke voor de ketenregie of een door hem of haar aangewezen persoon kan daarbij dienen als centraal aanspreekpunt. Hiermee kan er een verschil ontstaan tussen een juridische en een formele verantwoordelijkheid. Indien in een keten duidelijk te onderscheiden verwerkingen c.q. verwerkingsdoelen zijn, kan er voor gekozen worden meerdere verantwoordelijken aan te wijzen. Door de eindverantwoordelijkheid (voor het regelen hiervan) bij de ketenregie te laten kan tot een sluitend afsprakenstelsel worden gekomen.

Binnen dit afsprakenstelsel worden niet alleen de verantwoordelijkheden benoemd. Er wordt ook geborgd dat het delen van persoonsgegevens minimaal is en dat de kwaliteit van persoonsgegevens integraal wordt gegarandeerd. De verantwoordelijken zijn voor de verwerkingen van de persoonsgegevens het aanspreekpunt voor intern toezicht (C.01), betrokkenen (C.02) en in geval van een datalek voor de melding ervan (C.03). Het moet voor alle partijen duidelijk zijn wie deze verantwoordelijken zijn.

4.2.4 Opleiding van medewerkers

Privacyvereisten maken, door het hanteren van Privacy by Design, integraal deel uit van de werkprocessen en de informatiesystemen. Dit betekent dat zij ook onderdeel moeten zijn van de opleiding van de medewerkers die met de informatiesystemen moeten werken. Om te bepalen of de

medewerkers privacybewust zijn, kun je een kwaliteitssysteem gebruiken, waarvan de resultaten in de HRM-cyclus kunnen worden meegenomen.

> Bewustwording vraagt om het meenemen van de privacyvereisten in de opleiding van de medewerkers.

4.3 Risicomanagement - B.03

4.3.1 Criteria voor een investering

Oplossingen kosten doorgaans geld, direct of indirect. De wet staat toe dat je een redelijke afweging maakt tussen het doel en de kosten. Om te bepalen of een investering opweegt tegen de baten moet je weten welke privacyrisico's (en imagoschaderisico's) ermee afgedekt of verminderd worden. Daarvoor moet je allereerst bepalen of de maatregel waarom het gaat gebaseerd is op de risico's die zich voordoen en de mate waarin die zich voordoen, en welke alternatieven beschikbaar zijn. Te dure of complexe maatregelen leiden tot een onevenredig zware last en maken de dienstverlening duur; dat is niet in het belang van de betrokkene en niet in het belang van de organisatie.

4.3.2 Hulp bij inkoop

Veilig aanbesteden en inkopen vereist het stellen van scherpe eisen. CIP heeft enkele producten die kunnen helpen bij de bepaling van bedreigingen en risico's die je zou moeten overwegen bij de aankoop of het laten ontwikkelen van software. Met name de ICO Wizard is gericht op cybersecurity. Met de ICO Wizard selecteer je eisenpakketten die passen bij de producten/diensten die je aanbesteedt en die je meegeeft aan de inschrijvers. Het is een goed idee daarbij ook het privacyperspectief in de gaten te houden [6].

> Een 'passende privacymaatregel' is de uitkomst van een afweging tussen het privacyrisico en de impact c.q. kosten van de maatregel.

4.3.3 Risicomanagement als continu proces

Een DPIA [7] blijkt in de praktijk een nuttig instrument te zijn om vroegtijdig privacyrisico's te signaleren en maatregelen te nemen . Effectief beperken van de risico's is echter alleen mogelijk wanneer dit in alle fasen van de levenscyclus van een verwerking wordt meegenomen, dus ook en vooral al bij de bij het initieel bepalen van het doel van de verwerking (U.01) en bij het ontwerpen en ontwikkelen ervan (Privacy by Design [11]).

4.3.4 Risicomanagement en de focus van de DPIA

Bij een privacyrisicoanalyse wordt onderzoek gedaan naar de aanwezigheid van afwijkingen op de wetgeving. De DPIA is hierbij een belangrijk instrument. Een DPIA geeft zicht op een belangrijk deel

van de afwijkingen, echter niet alle afwijkingen. Het volgen van de Privacy Baseline om vast te stellen waar de praktijk afwijkt, geeft een volledig beeld van afwijkingen en dus privacyrisico's, inclusief aanwijzingen waar die afwijkingen binnen de organisatie moeten worden opgelost.

4.3.5 Elektronische hulpmiddelen

Het effect van de compliancymaatregelen kan met behulp van privacy management software worden beoordeeld en verbeterd. Regeldruk en groeiende erkenning van het belang van privacy zijn de belangrijkste redenen om daarvoor te kiezen. Meestal bevat privacy management software de volgende functionaliteit ter ondersteuning van het proces:

- Het uitvoeren van checks op de verwerking van persoonsgegevens tegen de eisen van de privacy regelgeving.
- Het volgen van incidenten die hebben geleid tot ongeautoriseerde openbaarmakingen (onderzoek, sanering en rapportage).
- Het analyseren en documenteren van gegevensstromen van persoonsgegevens:
  - De aard van de gegevens,
  - Het doel van de verwerking en
  - De verantwoordelijke voor de verwerking.
- Het vaststellen en het publiceren van het privacybeleid,
- Monitoring van het privacybewustzijn van de gebruikers: kennen gebruikers het beleid?

Een alternatief voor specifieke privacy management hulpmiddelen zijn Governance, Risk en Compliance (GRC) hulpmiddelen, zoals die gebruikt worden binnen het domein van informatiebeveiliging, waar vergelijkbare processen en beoordelingen plaatsvinden. Met GRC-tooling kun je geautomatiseerde bewaking zetten op compliance door het bewaken van de risico's en de afhandeling daarvan.

De complexiteit van het privacybeleid en het monitoren van de uitvoering zijn doorgaans de redenen om de activiteiten te automatiseren. De businesscase voor de keuze van GRC-tooling is afhankelijk van de omvang van de bedrijfsvoering en hoe belangrijk het voor de organisatie is dat compliancy wordt aangetoond.

4.4 Vastleggen doel gegevensverwerking - U.01

4.4.1 Gerechtvaardigd doel en dataminimalisatie.

Het vastleggen van een gerechtvaardigd doel van een gegevensverwerking op basis van criterium U.01 legt een deel van de legitimiteit van een gegevensverwerking vast. Om tot gerechtvaardigde doelen en dataminimalisatie te komen moet een proces worden ingericht, waarin de afweging wordt gemaakt welke wet- en regelgeving geldt en of dataminimalisatie mogelijk is. Binnen dit proces heeft gegevensmanagement (U.02) een belangrijke rol.

Als er een gerechtvaardigd doel is en er geldt geen uitzonderingsgrond, dan moet v*oorafgaand aan de verwerking* een melding worden gedaan aan de betrokkene om wiens persoonsgegevens het bij de bedoelde verwerking gaat. Legitimiteit gaat echter verder dan het hebben van een doel of het hebben van een uitzonderingsgrond.

Nauw verbonden met de legitimiteit is de *noodzakelijkheid* van het verwerken een persoonsgegeven. Het kan lonen om naar alternatieven te speuren en het persoonsgegeven zelf niet te verwerken.

Dat vermindert mogelijke risico's en kan de beheerlast van het compliant zijn aan de AVG verkleinen of wegnemen en zo een aanzienlijke kostenbesparing opleveren.

Een voorbeeld: wanneer een bepaalde inkomensgrens van belang is voor een besluit, dan is het niet nodig om te weten wat iemand verdient; het is voldoende om te weten of hij of zij onder of boven die grens zit.

Dataminimalisatie kan worden bereikt door bijvoorbeeld niet de gegevens te verzamelen en op basis van de verzamelde gegevens een beslissing te nemen, maar juist de gegevens bij de bron te laten en via een service de beslissing op te vragen.

Het voorkómen dat feitelijk onnodig persoonsgegevens verwerkt worden, wordt 'dataminimalisatie' genoemd. Zeker wanneer het bijzondere persoonsgegevens betreft kan dataminimalisatie zeer effectief zijn in het licht van privacybescherming.

4.4.2 De keuze om een persoonsgegeven wel of niet te verwerken

Is het doel van een verwerking *verenigbaar* met het oorspronkelijke doel waarvoor het (persoons)gegeven is verstrekt? Betrek hierbij expliciet (en leg afwegingen en besluiten vast):

- De verwantschap tussen het nieuwe en het 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, dan zal verwerking voor een ander dan het oorspronkelijke doel minder snel als verenigbaar kunnen worden aangemerkt.
- De mogelijke gevolgen van de nieuwe verwerking voor de betrokkene: 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, bijvoorbeeld via derde partijen, dan 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 bij de beoordeling of het nieuwe doel verenigbaar is met het oorspronkelijke doel. Hierbij kun je bijvoorbeeld denken aan informatievoorziening aan de betrokkene en mogelijkheid tot verzet.

4.5 Gegevensmanagement - U.02

Binnen het proces gegevensmanagement worden alle verzamelde en te verwerken (persoons)gegevens vastgelegd. Hierdoor ontstaat een overzicht op de gegevens, met daarin:

- Een beschrijving van ieder (persoons)gegeven (gegevensdefinitie).
- Het doel van de gegevensverwerking, waaraan getoetst kan worden of een gegeven toereikend, ter zake dienend en niet bovenmatig is.
- De herkomst van elk gegeven.

- Hoe en door wie gegevens zijn ontvangen.
- Wie eindverantwoordelijk is voor de afscherming van de (persoons)gegevens.
- Een overzicht van de uitwisselingen binnen en buiten de eigen organisatie.
    - Welke gegevens worden gedeeld;
    - Afspraken (contracten, opdrachtverlening, bevoegdheidsverlening).

Gangbare gegevensmanagmentsoftware kan bovendien de relaties tussen gegevens vastleggen en inzichtelijk maken.

4.6 Kwaliteitsmanagement - U.03

De processen voor kwaliteitsmanagement borgen de juistheid, nauwkeurigheid, actualiteit, volledigheid en bevorderen een correct gebruik van de gegevens. Hiertoe zijn processen ingericht voor:

- Onderzoek naar de gevolgen van het gebruik van onjuiste gegevens en hoe dit te ondervangen.
- Bewaking door middel van periodieke controles.
- Correctie, actualisering of verwijdering.
- Informeren van de betrokkene bij correctie.

Van belang is dat deze processen deel uitmaken van de primaire bedrijfsprocessen, zodat kwaliteitsmanagement niet separaat wordt opgezet of suboptimaal wordt vormgegeven.

4.7 Doorgifte van persoonsgegevens - U.07

4.7.1 Toelichtingen wetgeving buiten de Europese Unie

De wetgeving buiten de Europese Unie is complex en divers en vereist daarom een gedegen juridisch advies om de impact per doorgifte te kunnen bepalen. Ter *indicatie* van de complexiteit en de verschillen met de Europese Unie worden enkele wetgevingen buiten de EU kort omschreven.[15,16]

Privacy in de VS

Privacywetgeving in de VS beschermt de persoonsgegevens en de persoonlijke levenssfeer van personen, meer in het bijzonder: van Amerikaanse staatsburgers. Ze zijn sectorspecifiek, verschillen per staat, zijn gefragmenteerd en inconsistent en dat maakt het complex.

De Federal Trade Commission (FTC) is de facto privacy toezichthouder op het federaal niveau, maar heeft geen specifiek wettelijk mandaat. Evenmin bestaat er op federaal niveau privacywetgeving die de fragmentatie en daarmee de complexiteit reduceert.

Privacy-eisen die van belang zijn als je zaken doet met de VS of 'US-based companies' zijn de Generally Accepted Privacy Principles (GAPP), het (niet onomstreden) Privacy Shield en de privacy principes Organisatie voor Economische Samenwerking en Ontwikkeling (OESO). Alleen organisaties (in de VS)

[15] Let op: de informatie is summier en stamt grotendeels uit 2015. Wie actuelere informatie heeft over de privacyregels in genoemde gebieden en de huidige tekst kan aanvullen of corrigeren, nodigen wij van harte uit te reageren. Dat kan gemakkelijk via de contactpagina van de CIP-website https://cip-overheid.nl.

[16] Zie ook: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/internationale-privacywetgeving.

die zich hebben geconformeerd aan het EU-US Privacy Shield verdrag bieden m.b.t. niet-Amerikanen *in theorie* een passend beschermingsniveau.

Zij moeten zich hebben ingeschreven bij de Federal Trade Commission in het EU-US Privacy Shield register én ook actief de nodige maatregelen te hebben getroffen[17]. Hou ook rekening met de Cybersecurity Information Sharing Act (CISA).

Privacy in Canada

Landsdelen die vallen onder de Canadian Personal Information Protection and Electronic Documents Act bieden een passend beschermingsniveau. Maar let op: Onder meer Québec valt hier *niet* onder, waardoor de gegevens *niet* mogen worden doorgegeven aan een organisatie in Québec, tenzij sprake is van specifiek gronden voor rechtmatige doorgifte naar landen buiten de EU.

Privacy in Zuid Amerika

Privacy is goed verwoord in de grondwet van Zuid Amerikaanse landen en wordt versterkt door verschillende wetten en gerechtelijke precedenten in meerdere landen. De privacy regelgeving is op één lijn met de EU-richtlijnen en de Asia-Pacific Economic Cooperation (APEC) privacy principes. De Zuid-Amerikaanse wetten vereisen de melding van inbreuken en grensoverschrijdende gegevensstromen en dat de verwerkers van privacygevoelige informatie zich inschrijven bij een toezichthoudende autoriteit voor gegevensbescherming (DPA). De handhaving en een duidelijke uitwerking van de eisen zijn beperkt aanwezig.

Privacy in Azië / Pacific

Hoe privacy, in de betekenis van de persoonlijke levenssfeer en de bescherming van gegevens, in de wetgeving is opgenomen wordt bepaald door de cultuur, de filosofie van de overheid en economische omstandigheden. Hierdoor verschilt de wetgeving per land. Door de groeiende afhankelijkheid van elektronische diensten en netwerken neemt ook hier het bewustzijn en daarmee de verwachtingen toe. En daarmee ook de wetgeving. Soms wordt encryptie van spraak- en dataverkeer beperkt en worden individuen en bedrijven beperkt in de bescherming van hun eigen privacy omdat bepaalde beveiligingstechnologieën door de overheid niet worden toegestaan. Wetgeving kan heel diffuus zijn, doordat het beschermen van de persoonsgegevens en het binnenhalen van bedrijven afwisselend prioriteit krijgen. Aandacht voor meer informele regelgeving is eveneens nodig. Ook hier zal de regelgeving gaan evolueren.

4.8 Intern toezicht - C.01

4.8.1 Rapportages

Een belangrijk deel van de transparantie is gebaseerd op intern en extern toezicht. Het is wel van belang dat het verzamelen (laten rapporteren) en beoordelen van informatie wordt beperkt. Anders kan dit leiden tot te hoge overhead, verstoring van de bedrijfsvoering, maar ook tot rapportagemoeheid en

[17] De stand van zaken rondom het niet onomstreden Privacy Shield is ingewikkelder dan hier verwoord en bovendien in beweging. Let in dit verband bijvoorbeeld op het onlangs (16 juli 2020) uitgesproken negatieve oordeel van het Europese Hof van Justitie over de privacygaranties in de VS: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091nl.pdf; https://www.europa-nu.nl/id/vlaed3gss4zd/nieuws/eu_hof_amerikaanse_privacybescherming_eu?ctx=vhkejco8liwc&tab=0

onverschilligheid. Een te minimale verzamelen en beoordelen kan echter weer leiden tot te weinig controle en de daaraan verbonden risico's. De omvang moet enerzijds een voldoende mate van beheersing van risico's bieden en anderzijds voldoende vrijheden bieden om eigen keuzes te maken bij hoe gerapporteerd wordt.

5 Toelichting op verandermanagement

Het is natuurlijk niet de bedoeling hier de theorieën over 'verandermanagement' te bespreken; wel is getracht om in aanmerking komende uitgangspunten hier specifiek te richten op de implementatie van 'privacy' in de organisatie.

5.1 Slim implementeren van privacy

Volwassenheidsmodellen bieden organisaties kaders en instrumenten om het volwassenheidsniveau van de organisatie stapsgewijs te verhogen en transparanter te worden over hoe de organisatie de privacy beschermt. Zo kan de organisatie steeds beter aantonen 'grip op privacy' te hebben. Maar de modellen zijn, zoals betoogd in paragraaf 2.3.3, ook zeer bruikbaar om stapsgewijze, behapbare ambities te verwezenlijken of in gecontroleerde stappen systematisch toe te groeien naar de (hoge) ambities.

Met de keuze de organisatie te laten groeien op basis van volwassenheidsniveaus, is nog niet de keuze gemaakt *hoe* de groei het best kan worden doorlopen. Een juiste aanpak van de verandering die de organisatie wenst te realiseren is onontbeerlijk voor een efficiënte en daarmee slimme volwassenheidsgroei van de organisatie. Dat is voor de implementatie of verbetering van privacy niet anders. Om te komen tot een slimme aanpak moeten keuzes gemaakt worden:

Tabel 2: keuzehulp bij implementatie

1.	Hoe kunnen we sturing geven aan de veranderingen?	*Welke wijze van innoveren kiezen we?*
2.	Hoe houden we de stappen behapbaar?	*Welke implementatiestrategie kiezen we?*
3.	Hoe wordt de kennis benut?	*Is de aanpak "top down" , "bottom up" of "middle out"?*
4.	Welke stappen (incrementen) definiëren we in het groeipad.	*Kiezen we voor een "klassieke staged CMM aanpak", of voor een meer evolutionaire aanpak?*
5.	Hoe houden we de vinger aan de pols?	*Hoe nemen we nieuwe risico's mee?*
6.	Kiezen we voor meetbare resultaten?	*Hoe SMART maken we de resultaten per stap?*

5.1.1 Wijze van innoveren

Bij het bepalen van de implementatiestrategie kun je kiezen uit verschillende vormen van innovaties. Padovani e.a. [15] maakt onderscheid tussen autonome innovaties en systematische innovaties:

- *Autonome innovaties*: deze innovaties kunnen los van andere veranderingen worden gerealiseerd.
- *Systematische innovaties*: deze innovaties leveren alleen een bijdrage in combinatie met andere innovaties.

Als derde is een onderscheid te noemen tussen incrementele en radicale innovaties:

- *Incrementele innovatie*: bij incrementele of evolutionaire innovatie worden kleine veranderingen aan bestaande producten of diensten doorgevoerd.
- *Radicale innovatie (big-bang)*: bij radicale (big bang) innovatie worden nieuwe ontwerpconcepten vastgesteld.

De big bang aanpak kan toegepast worden als de lijnorganisatie stabiel is, dat wil zeggen: weinig of geen organisatieveranderingen doormaakt.

Voor een systematische aanpak kun je kiezen indien de veranderingen, die nodig zijn om grip op privacy te krijgen, afhankelijk zijn van andere innovaties. Bij een grote afhankelijkheid tussen veranderingen kan vaak beter gekozen worden voor een aanpak waarbij 'meegelift' wordt op andere veranderingen.

Indien de urgentie of de afhankelijkheid echt anders aangeeft, kun je kiezen voor een autonome aanpak. Het is wel nuttig na te gaan welke andere veranderingen doorgevoerd worden binnen de organisatie, teneinde door samenwerking tot een meer effectieve inzet van mensen en middelen te komen.

Door te kiezen voor een ondersteunende innovatie kun je het beste gebruik maken van de kennis en kunde en daarmee de kracht van de bestaande organisatie. Indien gekozen wordt voor een ontwrichtende aanpak dan is het vooraf bepalen van een gedeelde ambitie essentieel.

Door te kiezen voor een incrementele aanpak kan de aanpak aangepast worden aan veranderende omstandigheden, zodat ambities overeind en haalbaar blijven.

> Hoge ambities zijn goed, maar haalbare ambities, met een op de organisatie en op het moment afgestemde wijze van veranderen, zijn beter.
> Gebruik het Privacy Volwassenheidsmodel als basis om de ambities waar te maken.

5.1.2 Sturing geven aan de implementatie

Er kan op verschillende manieren sturing gegeven worden aan implementaties. Als de kracht van de staande organisatie wordt benut ontstaat een samenspel van inhoud, proces en relaties. Als het uiteindelijke plan inhoudelijk niet goed in elkaar zit en er geen afstemming plaatsvindt, is het risico aanwezig dat het plan niet tot een goed einde komt. De ervaring leert bijvoorbeeld dat juridische en financiële aspecten echt 'rond' moeten zijn en dat wat ieder 'erin stopt' en 'eruit haalt' in balans moeten zijn. Ook speelt mee dat iedereen op het podium een kloppend verhaal moet hebben in rationele termen en dat er persoonlijke reputaties op het spel staan[18].

[18] Voor inspiratie bij deze aspecten zie bijvoorbeeld Kaats (2012) [16].

Uit onderzoek van Kooreman (2009) [8] blijkt dat het voor projecten belangrijk is dat:

- De complexiteit van projecten (met veel gevarieerde doelen/ambities en aan elkaar gerelateerde onderdelen) beheerst wordt,
- Projecten minder zacht gemaakt moeten worden. Zachtheid houdt in dat er weinig duidelijkheid is in de doelen, dat er meerdere stakeholders zijn met verschillende verwachtingen.
- De onzekerheid, die ontstaat doordat veranderingen in de omgeving van invloed zijn op het project, gemanaged moet worden.

Als dit niet gebeurt dan wordt de kans groter dat een project niet binnen tijd en budget, of niet met de vereiste kwaliteit opgeleverd wordt. Een roadmap, bij voorkeur ondersteund met een visualisatie, helpt om te kunnen sturen. De roadmap moet de ambitie/doelen, veranderinspanningen en de afhankelijkheden weergeven [17].

De complexiteit neemt toe wanneer een project meerdere doelen/ambities heeft. Stakeholders kunnen een belang hebben bij:

- Het slagen (of niet slagen) van een project;
- Het beschikbaar stellen van middelen voor het project.

Transparantie is belangrijk, zeker als de stakeholder meer invloed heeft op de kans van slagen van het waarmaken van de ambitie ten aanzien van privacybescherming. Bij veranderingen bestaan er haast per definitie meerdere ambities. Dit maakt het moeilijk om duidelijke doelen te stellen aan de plannen.

Projecten zijn volgens Crawford en Pollack (2004) [18] in te delen in *harde* en *zachte* projecten. Of een project hard of zacht is kan worden bepaald op basis van:

1. De duidelijkheid van het doel;
2. De tastbaarheid van het doel;
3. De manier van het meten van succes (de instrumenten die gebruikt worden om te meten of het project succesvol is);
4. De beïnvloedbaarheid van het project (hoe vatbaar het project is voor externe invloeden);
5. Het aantal mogelijke alternatieve oplossingen;
6. De mate van participatie en de duidelijkheid in de rollen van teamleden;
7. Stakeholderverwachtingen (bij zachte projecten moet er meer interactie zijn tussen stakeholders dan in harde projecten).

De hardheid of zachtheid van een project bepaalt de slagingskans en daarmee de benodigde implementatiestrategie om de slagingskans te vergroten. Crawford en Pollack geven aan dat de zachte factoren een grote negatieve invloed hebben op de slaagkans van een project. *Het niet onder controle hebben van de zachte aspecten verhoogt de complexiteit van een project*. Door de zachte factoren harder te maken is de verandering makkelijker te meten, te managen en zijn projecten minder complex.

Privacybescherming naar een hoger volwassenheidsniveau brengen vraagt om een veranderaanpak met aandacht voor de zachte factoren en de daaraan verbonden risico's voor het waarmaken van de privacyambitie.

5.1.3 Pragmatische programmamanager

Het groeien naar volwassenheid vraagt om een dag-tot-dag programmamanager die werkt aan het bereiken van compliance van de organisatie en de doorgroei in volwassenheid. Deze programmamanager moet een gerespecteerde, pragmatische leider zijn met kennis van de operationele bedrijfsvoering en ruim sociaal netwerk binnen de organisatie. Een hoge lijnfunctionaris met slagkracht op het uitvoerende niveau en het vermogen om de juiste spelers in een kernteam te selecteren en aan te sturen kan hiervoor een aangewezen persoon zijn. Het kernteam bestaat verder uit vertegenwoordigers uit de afdelingen die het meest te maken hebben met de verschillende aandachtsgebieden uit de Privacy Baseline, bij voorkeur de managers.

In het implementatietraject en het groeitraject is het van belang dat zij die verantwoordelijk zijn voor de compliancy toegang krijgen tot de programmamanager, zodat in een zo vroeg mogelijk stadium waarschuwingen en aanbevelingen uit de organisatie meegenomen kunnen worden in de aanpak. Organiseer dit overigens zonder dat zij lid zijn van het kernteam, zodat een duidelijke scheiding van verantwoordelijkheden blijft bestaan. Bedenk ook dat compliance professionals, juristen en privacyfunctionarissen over het algemeen niet de meest geschikte mensen zijn voor het coördineren van een invoering. Daarentegen bezitten ze wel de juiste kennis om verbetervoorstellen te doen over het privacybeleid, de uitvoering en de controlprocessen.

Programmamanagement geeft pragmatisch sturing aan de keuzes van de organisatie om te komen tot compliancy.

5.1.4 Benutten van de kennis van de organisatie

Het implementeren van de processen om compliancy te bewerkstelligen leidt al snel tot een centraal gestuurde aanpak, waarbij van boven af uitgebreide beleidsdocumenten en procedures worden opgesteld. Het voordeel van een centraal aangestuurde aanpak is de top-down benadering, waarbij met commitment van het topmanagement sturing wordt gegeven aan het veranderproces. Het nadeel echter is dat een centrale aansturing snel leidt tot een aanpak waarbij de kennis over de mogelijkheden van de bestaande bedrijfsvoering ongezien en onbenut blijft. De tegenhanger is een meer bottom-up benadering waarbij deze kennis decentraal wel wordt benut. Ook hierbij ondersteunt de Privacy Baseline bij een pragmatische aanpak. Door te werken vanuit de aandachtsgebieden, kun je aansluiten op de bedrijfsvoering en zo de kennis binnen het bedrijf benutten.

Door het combineren van de top-down en de bottom-up benadering ontstaat een aanpak waarin bij het centraal management commitment wordt verkregen en decentraal de kennis wordt benut, tegen lagere kosten voor met name externe inhuur en met minder projectrisico's, doordat het gehele privacymanagement vraagstuk is opgesplitst in kleinere aandachtsgebieden.

Benut de decentraal beschikbare kennis binnen de aandachtsgebieden en faciliteer centraal de coördinatie over de aandachtsgebieden.

Een belangrijk onderdeel en opdracht voor het centrale management is het faciliteren van de kleine teams op het gebied van de wet- en regelgeving. Er moet grondige kennis voorhanden zijn van de wet- en regelgeving en begrip van de betekenis en implicaties ervan voor de verschillende aandachtsgebieden. De Privacy Baseline reikt de daarvoor benodigde kennis aan. Maar hoe eenduidig de Baseline ook is opgezet, het gevaar van een afwijkende interpretatie blijft bestaan en ook voortschrijdende jurisprudentie kan zaken in een ander licht zetten. Een juridische blik en achtergrond zijn daarom onontbeerlijk, liefst van een gespecialiseerde privacyjurist.

Door waar nodig de teams bij te staan en uitleg te geven bij de Baseline worden de wet- en regelgeving toegankelijker gemaakt en wordt een eenduidig gebruik van de Baseline en daarmee eenduidige implementatie van de wet- en regelgeving bevorderd.

Wijs een persoon aan die namens het kernteam de eenduidigheid van de interpretatie van de Privacy Baseline over de verschillende teams bewaakt.

Let erop dat de persoon die deze uitleg geeft aan de kleine teams dezelfde pragmatische aanpak hanteert bij de naleving als de programmamanager, anders veroorzaak je verwarring. Afstemming en overeenstemming over de interpretatie binnen het kernteam kan worden verkregen door de Privacy Baseline te bespreken en door te vertalen naar de implicaties voor governance en de daarbij te maken keuzes. Gebruik de Baseline bij het helder krijgen van de implicaties en de te maken keuzes.

5.1.5 Budgetten uit de reguliere begroting

Het is noodzakelijk om ontbrekende privacymaatregelen als onderscheiden activiteit mee te nemen in de aanvraag voor middelen in de bestaande begrotingscyclus. Door de cyclische privacyprocessen in de planning af te stemmen op de bestaande begrotingscyclus van de organisatie voorkom je onnodig tijdverlies en gedoe dat kan optreden wanneer je buiten de reguliere cyclus budget probeert vrij te krijgen. Geef privacy een prominente, onderscheiden plaats maar doe dat in – en niet naast de reguliere begroting.

Om de specifieke maatregelen te kunnen onderkennen zijn de rapportages van de verantwoordelijken die benoemd zijn in de TVB-matrix een vereiste. In feite start met het goedkeuren van de begroting een nieuwe cyclus in het proces om privacy op niveau te krijgen en te houden. Zo verandert de reactieve benadering van privacy ook budgettair in een proactieve benadering en is de organisatie in control op de aspecten sturen, beheersen, rapporteren en verantwoorden.

Het meenemen van privacy als onderwerp in de begroting, waarbij de benodigde maatregelen en de begroting zelf zijn gebaseerd op rapportages van de verantwoordelijken die benoemd zijn in de TVB-matrix, zijn kenmerken van de integrale werking van governance aan.

5.2 Veranderen gaat niet vanzelf

Privacybescherming en het neerzetten van een aanpak om grip op privacy te krijgen betekent het doorvoeren van een verandering. Dit vraagt om verandermanagement. Het veranderproces en in het bijzonder de veranderaanpak, de samenwerking en de eigen positie moeten gericht zijn op het meekrijgen van de organisatie en haar mensen, zodat zij privacy als integraal onderdeel van hun dienstverlening kunnen aanbieden.

Grote veranderingen leiden tot onzekerheden. Onzekerheden vragen om afspraken en om handhaving, waarvoor management nodig is. Het vraagt om het succesvol meegaan van iedere medewerker in het belang van privacybescherming. Het moet in de 'vezels', in de genen, van de organisatie gaan zitten. En ook dat is te vertalen in concrete actiepunten.

Geleide verandering is nodig om te komen tot het bedrijfsbreed toepassen en onderhouden van privacybeleid, en het rapporteren over behaalde en niet behaalde resultaten. Hanteer bij de opzet en de uitvoering van de governance een zakelijke degelijkheid:

- *Afspraak is afspraak*
  Governance is alleen mogelijk door te sturen op afspraken. Borg de afspraken in de lijnorganisatie door het definiëren van de te behalen doelen. Maak daarbij ook afspraken over de rapportage over de behaalde en niet behaalde resultaten. Gebruik daarbij het onderscheid dat de Privacy Baseline maakt tussen Beleid en Uitvoering.
- *Action learning*
  Bij het maken van afspraken worden altijd opeenvolgende haalbare doelen gesteld.
- *Professioneel organiseren*
  Ga na of het netwerk van betrokken medewerkers en afspraken professioneel zijn georganiseerd. Ga na of het nemen van beslissingen in de lijn is belegd, zodat beslissingen ook omgezet kunnen worden in het bijsturen op resultaten.
- *Rapportage over de behaalde resultaten*
  Rapporteren is een vak. Rapporteren is meer dan het weergeven van een afwijking door het noemen van cijfers. Neem de organisatie mee in de bevindingen en de ambities om privacybescherming op het juiste niveau te brengen.
- *Organiseren vanuit een team*
  Een ACT-team (zie paragraaf 5.3) vormt de basis van alle veranderingen. Het meebewegen met de organisatie en het sturen op proces en inhoud vraagt om een team waarin de betrokken afdelingen van de organisatie zijn vertegenwoordigd en dat als eenheid optreedt.
- *Borging van het resultaat*
  Een verandering is pas doorgevoerd, wanneer de resultaten zijn belegd in de staande organisatie.

5.2.1 Vergroten van de betrokkenheid van de lijnorganisatie.

Veranderingen doorvoeren in een organisatie is geen individuele activiteit. Gesprekken en uitleg aan de managementteams de lijnorganisatie vormen de basis voor de betrokkenheid van de lijnorganisatie en de mandatering. Dit maakt het ook mogelijk de sturing van de lijnorganisatie binnen de lijnorganisatie te beleggen.

Waarborg dat de lijnmanagers die de vernieuwingsactie meemaken er voldoende aandacht/tijd aan (kunnen en willen) besteden. De bestaande managementtafels zijn overvol en de kans is groot dat de privacybescherming onderaan het lijstje komt of van de tafel valt. Het benoemen van 'kampioenen' (champions, voorvechters) in de lijnorganisatie, die privacy als onderwerp in hun portefeuille hebben, helpt om het zichtbaar te houden. Een kampioen is een door management team aangestelde persoon *uit de lijnorganisatie* die de beoogde verandering begrijpt en steunt.

Een succesvolle samenwerking tussen de lijnorganisatie en het ACT-team is herkenbaar aan een negental kenmerken [19].

1. Het management investeert zichtbaar in samenwerking, bijvoorbeeld door uitingen op elektronische sociale ontmoetingsruimten.
2. De managers zijn rolmodellen; dit komt door het 'trickling down'-effect.
3. Er heerst een zogeheten 'gift culture', waarin managers een coachende rol spelen en ruimte wordt gegeven aan elkaars overwinningen.
4. Er zijn trainingen in relationele vaardigheden, zoals conflictmanagement en communicatie.
5. Er worden groepsactiviteiten georganiseerd om het gemeenschapsgevoel te versterken.
6. Het leiderschap is 'ambidextrous', leidinggevenden zijn zowel taak- als relatiegeoriënteerd.
7. Samenwerkingsverbanden worden samengesteld uit mensen die eerder met succes hebben samengewerkt.
8. De rolverdeling is niet alleen duidelijk, maar wordt ook gehanteerd en gerespecteerd.
9. Houd bij de samenstelling rekening met de verschillende mindsets, zodat de verschillende belangen en denkwijzen die binnen de organisatie spelen worden meegenomen.

> De eindverantwoordelijkheid voor privacybescherming ligt in de lijn;
> de verantwoordelijkheid voor de verandering ligt bij het ACT-team.

5.2.2 Ambities afgestemd op de organisatie

PriSa's en DPIA's kunnen aangeven waar de ambities voor het ACT-team moeten liggen. Dit is een rationeel proces. Het vermogen om de ambities waar te maken wordt echter bepaald door de effectiviteit om samen te werken met de lijnorganisatie. Belangrijk daarbij is te weten welke ambities gedragen worden in de organisatie en hoe een passende samenwerking ontstaat. Door de samenwerkingsvorm en de ambities af te stemmen op de organisatie ontstaan gezamenlijke ambities, draagvlak en duurzame relaties.

Het gaat daarbij dus om het verkrijgen van draagvlak voor ambities die gedeeld worden. Om dit te bereiken moet je kunnen bepalen waar je binnen de organisatie het beste kunt aanhaken en hoe sturing gegeven kan worden aan de verandering die moet plaatsvinden. Een aantal tips:

Meebewegen

- Weet wat voor jouw gesprekspartner een belangrijke ambitie is en welke ambities hij daarin ten aanzien van privacybescherming wil meenemen. Weet duidelijk te maken welke ambities van de organisatie daarmee gediend zijn.
- Streef ernaar dat de organisatie zelf in staat is de ambitie uit te dragen. Gebruik hiervoor de resultaten van de stakeholderanalyse (zie paragraaf 5.2.4).
- Besteed geen tijd aan het opnieuw verwoorden van beleid wanneer daarbij de boodschap is dat het beleid de ambitie is *omdat het nu eenmaal het beleid is*. Let steeds op de risico's en de belangen voor de organisatie. Let erop dat uitgangspunten elkaar niet tegenspreken.
- Let goed op het verschil tussen de ambitie van één persoon en een gezamenlijke ambitie. Relateer altijd aan haalbaarheid en draagvlak. Zo kan een inperking van de scope de haalbaarheid vergroten, maar kan het draagvlak binnen de organisatie voor een effectieve inzet binnen de organisatie ontbreken.
- Waardeer en respecteer de verschillen die de organisatie en het ACT-team hebben in de weging van het belang van het wegwerken van privacyrisico's. Beide gremia hebben nu eenmaal een andere rol en taakstelling. Focus hierbij niet op verschillen, maar neem de belangen mee in de afweging voor de keuzes die je maakt en waai niet mee met iedere uitspraak. Houd daarom wel rekening met de verschillen tussen persoonlijke doelen en bedrijfsdoelen.
- Stel je gerust kritisch op tegenover plannen van de organisatie, waarbij privacy niet voldoende is meegenomen. Voorkom dat je daarbij als drammer wordt gezien. Benut het verandermoment om ambities waar te maken en de principes van Privacy by Design mee te nemen.
- Weet wat 'verboden woorden' en no-go areas zijn en weet hoe je hiermee moet omgaan.
- Help de juiste mensen aan te haken bij de juiste activiteiten op de juiste plekken in de organisatie. Weet daarbij waar sponsoren zitten (stakeholderanalyse).
- Voorkom dat sturing plaatsvindt op basis van macht; probeer de sturing waar te maken op basis van gezag door het meegeven van visie en duidelijkheid, gebaseerd op de *gezamenlijke* ambities. Denk niet vanuit autonomie, maar committeer je aan gezamenlijke ambities.
- Neem eventuele ontevredenheid binnen de organisatie mee in de aanpak die je kiest.
- Overzie alle aspecten van de bedrijfsvoering en zorg ervoor dat je niet wordt gezien als 'die figuur die alleen op privacy let'.

Weet waar de beweging naar toe gaat:

- Onderzoek en begrijp hoe ingrijpend de ambitie van het ACT-team is en hoe je de mate van ingrijpen kunt beperken of hoe je de ambitie in behapbare stukken weet op te splitsen.
- Zorg ervoor dat iedereen weet waar de vernieuwing om gaat en waarom die nodig is.
- Verwacht niet dat iedereen precies weet wat jouw rol is. Zorg dat je zelf wel precies op de hoogte bent en dat jouw rol bekend is bij de direct betrokkenen.

- Hou er rekening mee dat het management vaak slecht op de hoogte is van de ambitie van het ACT-team. Zorg dat je zelf wel op de hoogte bent en weet hoe je beperkingen en obstakels beperkt kunt houden of weet om te zetten in kansen voor de organisatie.
- Zorg ervoor dat de betrokkenen het resultaat en het voorgestelde traject van de vernieuwing begrijpen.
- Voorkom dat jij en de betrokkenen in de val van een spraakverwarring trappen. Het gevaar is dan dat daardoor vertrouwen verloren gaat en binnen handbereik liggende goede oplossingen uit het gezichtsveld verdwijnen.
- Probeer de juiste 'maatvoering' te vinden: beperk de omvang en daarmee de impact op de bestaande bedrijfsvoering van de ambities. Knip ambities zonodig op in delen.
- Houd rekening met je eigen beperkingen om sturing te geven aan de veranderingen. Wees je daarbij bewust van je beperkte eigen kracht en verminder de inzet daarvan naar mate de organisatie weerstand biedt; voorkom krachtpatserij en escalatie, een clash resulteert vaak in stilstand.
- Zorg ervoor dat elke verbetergroep zich gesteund voelt: duidelijk beleid, voldoende middelen, acceptatie door lijnmanagement, opleidings- en begeleidingsmogelijkheden.
- Wordt jouw advies overgenomen, dan is het nog niet jouw taak om voor de uitvoering te zorgen. De primaire taken van het ACT-team zijn het adviseren over maatregelen en processen en de rapportage over voortgang van wegwerken en beheersbaar maken van de privacyrisico's.

Stel jezelf de volgende vragen:

- Kan de organisatie autonomie gedeeltelijk loslaten en om zich te committeren aan de doelstelling van het ACT-team?
- Beschikken de mensen binnen het ACT-team en de organisatie over de durf en diplomatieke vaardigheden om te kunnen functioneren in verschillende samenwerkingsverbanden?
- Zijn bedrijfsvoering en de verwerking van persoonsgegevens zodanig georganiseerd dat de organisatie zonder al te veel investeringen kan participeren in het ACT-team?
- Hoe kan iedereen beter zijn rol pakken?
- Welke no-go areas zijn er en hoe lopen we daar omheen?
- Is de doelstelling van één partij bepalend of gaan we volgens de logica van het netwerk op zoek naar gezamenlijke ambitie?

Het benutten van de kracht van de organisatie vraagt om alignment van de ambities van het ACT-team met die van de organisatie.

5.2.3 Communicatie van de ambitie

Ambities moeten verenigbaar zijn. Zo riep Martin Luther King: "I Have a Dream". Hij riep niet "I Have a Plan". Daar zou discussie over zijn gekomen als er niet eerst overeenstemming zou zijn over de droom die hij had. Zo geldt ook voor privacybescherming dat pas nadat er overeenstemming is over de gezamenlijke ambities ten aanzien van privacybescherming, de stap gemaakt kan worden naar implementatiestrategieën en uiteindelijk de implementatieplannen[19]. Dat betekent dat gedacht wordt vanuit de mensen en niet alleen vanuit de inhoud. Het gaat dus zowel om inhoudelijke argumenten als om persoonlijke overtuigingen en drijfveren. Plannen worden daarbij gevormd in een samenspel van mensen die komen tot gezamenlijke ambities, waarbij zij rekening houden met de krachten binnen de organisatie. Dit betekent dat ambities in elkaars verlengde moeten liggen, voordat planvorming kan plaatsvinden. Bij de planvorming wordt, kennende de organisatie en de beoogde veranderingen, de implementatiestrategie daarop afgestemd.

5.2.4 Stakeholderanalyse

Bij het opzetten van een passende aanpak door het ACT-team is een stakeholderanalyse een methode om de verhoudingen, relaties en gedragingen die van belang zijn binnen de organisatie in kaart te brengen. Met de stakeholderanalyse worden de personen herkenbaar, onderkend en hun belangen beoordeeld en wordt het effectief en efficiënt doorvoeren van de verandering mogelijk, doordat de veranderbehoefte, de oplossing en het draagvlak in elkaars verlengde komen te liggen. Het is als het zoeken naar een 'window of opportunity'. Hiervoor moet het volgende gebeuen:

1. *Breng de belangen in kaart*
   Je bent niet de enige die aandacht vraagt. Het is daarom belangrijk dat je de organisatie kent, wie de stakeholders zijn en wat de (andere) taken en verantwoordelijkheden zijn. Dit beeld is belangrijk om te kunnen bepalen wie sponsor is van de ambities en waar weerstand zit. Ben je ook bewust van belangen die van buiten de organisatie de belangen intern kunnen beïnvloeden.

   Denk na over wat voor iedere partner betekenisvol is, of dat voor de organisatie geldt of persoonlijk is en wat de gedeelde ambities zijn.

2. *Breng het speelveld in kaart*
   Niet iedereen is een stakeholder. Bepaalde personen staan op afstand van het onderwerp maar hebben wel veel invloed. Anderen staan dichtbij maar hebben geen invloed op de adoptie van de plannen. Breng dit krachtenveld in kaart. Neem het speelveld mee in het bereik van je ambitie. Hou daarbij rekening met ontwikkelingen, waardoor in een relatief korte periode spelers van plek kunnen veranderen en zelfs van het speelveld moeten verdwijnen. Benut daarbij de kennis van het management waaraan je rapporteert en de meer stabiele organisatieonderdelen.

3. *Kies het juiste tijdstip*
   De mogelijkheden die een organisatie heeft om te veranderen zijn afhankelijk van bestaande processen, zoals jaarplanning en de drukte op een bepaald moment in de bedrijfsvoering. Hou daarom bij het aanspreken van de organisatie rekening met de lopende zaken en toekomstige

[19] Een aanpak die helpt doelstellingen en ambities te vertalen naar inspanningen en activiteiten is bijvoorbeeld de VIP-behandeling zoals besproken in Koorman (2009) [8].

planning. Kies de momenten van interventies bewust en probeer aan te sluiten op de relevantie voor de stakeholders op dat moment.

Let er bij de analyse op dat de betrokkenen een objectief belang hebben bij de verandering. Bedenk daarbij dat de rationaliteiten niet altijd eenvoudig eenduidig zijn te duiden. Extra complicerend daarbij is dat de ratio, al dan niet terecht en bewust, een ondergeschikte rol speelt. Wanneer irrationele emoties een belangrijke rol spelen, schep daar dan ruimte voor en besteed er aandacht aan [16].

Weet welke krachten meewerken en waar weerstand zit.
Hier op de juiste manier rekening mee houden geeft verandervermogen.

5.2.5 Action learning

De planbaarheid en maakbaarheid van veranderingen in organisaties is beperkt. Daar komt bij dat managers en adviseurs op fundamenteel verschillende manieren naar veranderingen kunnen kijken. De organisatie moet daarom de mogelijkheid krijgen om te leren. Door stapsgewijs te verbeteren wordt van fouten geleerd en kunnen kansen worden benut.

Bij verbeteren gaat het erom dat iedereen voortdurend kleine verbeteringen invoert. Onder het motto: morgen weer beter doen wat vandaag goed is gegaan. Action learning is gebaseerd op de volgende stappen in de verbeteraanpak[20]:

1. Kies een privacyrisico.
2. Ga na wie de stakeholders zijn.
3. Benoem een verbetergroep.
4. Zorg ervoor dat de verbetergroep zich gesteund voelt door duidelijk beleid, voldoende middelen en acceptatie door lijnmanagement.
5. Zorg dat medewerkers de bekwaamheid hebben om verbeteracties uit te voeren: vergadervaardigheid en het kunnen volgen van een aanpak; bijvoorbeeld zoals in dit document beschreven.
6. Maak bij aanvang van de werkzaamheden van een verbetergroep afspraken over de opdracht ten behoeve van het te verbeteren proces.
7. Bespreek met elkaar hoe om te gaan met de spanning tussen de feitelijke situatie en de gewenste situatie.
8. Maak met betrokkenen procedureafspraken over onderwerpen als taakverdeling, wijze van besluitvorming, planning, rapportage e.d.
9. Maak een goede samenwerking in een verbeterteam mogelijk door aandacht te besteden aan teamrollen, vergadertechniek e.d.

[20] Selectie gebaseerd op meerdere bronnen; op internet is veel te vinden onder 'action learning'. De oplettende lezer herkent in deze lijst de grove blauwdruk van een groot deel van deze handleiding.

10. Doorloop de verbetercyclus: kies een proces, bepaal proces output (wat komt eruit), breng proces in kaart, inventariseer verspillingen, meet, doe voorstellen ter verbetering, voer verbeteringen in.
11. Hef na invoering van verbeteringen de verbetergroep op.

5.2.6 Privacybescherming: alleen omdat het moet?

Wie bezig is met privacybescherming, is gedreven. Wij zijn tenminste zo vrij om een zeker idealisme te veronderstellen bij de voorvechters van privacy, en gelukkig kunnen we dat ook daadwerkelijk waarnemen in de praktijk. Een ACT team moet uit gedreven, gemotiveerde mensen bestaan. Zij zien het belang voor de organisatie. Zij zien privacybescherming als noodzaak: als niet vanuit het oogpunt van mensenrechten, dan toch zeker als noodzakelijk voor het voortbestaan van de organisatie. Gedreven mensen die voor de implementatie verantwoordelijk zijn nemen daarom graag het initiatief. Hoe nobel ook, er kleven risico's aan: de privacymaatregelen en -processen moeten worden geïmplementeerd in een drukke omgeving en kosten in eerste instantie geld zonder dat er directe revenuen uit voortkomen. Let daarom scherp op de volgende risico's:

- *De maatregelen en processen worden het doel*
  De maatregelen en processen zijn niet een middel, waarmee de organisatie geholpen is, maar een te behalen 'objective' *omdat het moet*. Intrinsieke motivatie is dan geen of geen sterke drijfveer.
- *De implementatie wordt een krachtmeting*
  Het ACT-team neemt de implementatie op zich. Zij implementeren een maatregel en richten daarvoor alles in, om te komen tot het afdekken van risico's. De staande organisatie wordt via hiërarchische lijnen 'overtuigd' van de noodzaak.
- *De staande organisatie haakt af*
  De maatregelen en processen worden gezien als iets dat van het ACT-team is. Dat de maatregelen en processen de (hele) organisatie helpen in het realiseren van haar doelstellingen verdwijnt uit beeld.
- *Het ACT-team staat er alleen voor*
  Het ACT-team wil zijn doelen bereiken, terwijl de staande organisatie met andere zaken bezig is. Er wordt geen rekening meer met elkaar gehouden. Er zijn na de uitgebreide implementatie awareness programma's nodig om de maatregelen daadwerkelijk organisatiebreed toe te gaan passen.
- *De implementatie gaat lang duren*
  Doordat de maatregelen naast de staande organisatie van nul af moeten worden opgebouwd zijn er grote projecten nodig, waardoor doorlooptijden en kosten uit de hand lopen.

Sneller, met minder kosten, met meer plezier(!) en meer effect implementeren van de privacymaatregelen en -processen, dit alles vraagt om het onderkennen van deze risico's. Door in een samenwerking de bestaande organisatie te benutten verandert het gevecht van een implementatie in een beweging die meegaat in de kracht van de organisatie. Zo groeit ook het gemeenschappelijk besef van de noodzaak.

Door mee te bewegen met de organisatie en alleen daar waar nodig bij te sturen wordt de kracht van de organisatie benut.

5.2.7 Privacybescherming is geen overval op de organisatie

Het op orde brengen van de privacybescherming is geen vanzelfsprekendheid Of beter gezegd: het is een vanzelfsprekendheid, maar gaat niet vanzelf. Zeker niet als je beschouwt wat bij het inregelen van alle processen komt kijken. De activiteiten die voor inregelen van de Privacy Baseline op bijvoorbeeld een volwassenheidsniveau 3 nodig zijn, kunnen betekenen dat de lijnorganisatie wordt overvraagd. Niveau 3 en hoger vraagt namelijk een volwassen wordende organisatie, waarbij processen en verantwoordelijkheden aantoonbaar 'in place' worden gebracht.

Adviezen voor het ACT-team om de samenwerking met de staande organisatie te bereiken en te voorkomen dat de lijnorganisatie afhaakt zijn:

- Kom tot gezamenlijke ambities en laat die leidend zijn voor de activiteiten die worden opgepakt.
- Vertaal de privacyrisico's naar haalbare ambities en oplossingen. Geef aan hoe de impact op de organisatie beperkt wordt.
- Voorkom een overval met een veelheid aan op te pakken onderwerpen en verantwoordelijkheden op de vaak al overvolle agenda in de managementteamvergaderingen.
- Zorg ervoor dat de belangrijkste onderwerpen het eerst worden opgepakt. Gebruik hiervoor een prioritering op basis van risico's voor de organisatie: welke zwakke plek zorgt voor het grootste risico?
- Mensen hebben zo hun stokpaardjes. Voorkom dat onderwerpen, waarvan de risico's niet aantoonbaar zijn, prioriteit krijgen. Geef aan dat, als het risico daadwerkelijk gaat bestaan, het onderwerp alsnog prioriteit krijgt. Hiermee voorkom je dat de ambitie tijdens de implementatie wegvalt.
- Zorg ervoor dat de prioritering transparant is en wees helder over de onderwerpen die pas in een latere fase aan bod komen (geen "salamitactiek"), maar gebruik het Privacy Volwassenheidsmodel als fasering om de ambities waar te maken.
- Waarborg dat voldoende middelen beschikbaar gesteld worden voor de onderwerpen die prioriteit krijgen, in lijn met het belang van het onderwerp.
- Wees er zeker van dat voldoende sturing vanuit het ACT-team mogelijk is.

5.3 Het ACT-team en de organisatie als één team

5.3.1 Basisstructuur van een team

Bij het op orde brengen en houden van privacybescherming is een bonte verzameling aan samenwerkingsverbanden actief. Goed contact met de organisatie is een belangrijke voorwaarde om de organisatie mee te krijgen de juiste maatregelen te implementeren en op peil te houden. Het kan moeilijk zijn de organisatie mee te krijgen als slecht nieuws gebracht moet worden en je niet kunt refereren aan organisatiebrede ambities en vastgesteld beleid.

5.3.2 Privacybescherming is teamwork

Het verbeteren van privacybescherming is teamwork. De kern van het teamwork is het ACT-team. Het benutten van de kracht van de organisatie start met het neerzetten van dat team. De samenwerking van het team is echter niet beperkt tot alleen intern het team. Dat team werkt samen met de lijnorganisatie. Het kernteam kan samen met anderen in de organisatie ook weer een team vormen. Zeker als gebruik gemaakt wordt van kampioenen en campagneleiders, maken ook zij deel uit van het team.

Het teammodel van Lencioni (2009) [20] noemt vijf cruciale factoren voor het werken in een succesvol team, dwz: dat de juiste prestaties levert en goede resultaten behaalt. Het model wordt weergegeven in de vorm van een piramide.



Figuur 4: De piramide van Lencioni

De volgorde bij het opzetten van een succesvol team is van onder naar boven. Werken als team heeft onderling vertrouwen als basis. Door confrontaties en discussies te durven aangaan, commitment aan te gaan, verantwoordelijkheid te nemen kan de focus op resultaat ontstaan.

Voor het neerzetten van een succesvol team worden de volgende factoren genoemd:

- **Vertrouwen**: de basis van de piramide. Teamleden moeten vertrouwen hebben in elkaar. Vertrouwen staat voor de zekerheid van de teamleden dat de intenties van hun collega's goed zijn en dat er geen reden is om beschermend te zijn of bezorgd over de groep.

  Aanpak: vertrouwen ontstaat door het delen van ervaringen en persoonlijke geschiedenissen. Ook het benoemen van elkaars persoonlijke bijdrage in het team werkt bevorderend.

- **Confrontatie en discussie**: Volgens Lencioni is het belangrijk productieve confrontaties hun werk te laten doen. Deze teams kenmerken zich juist door hun gretigheid en door de bereidheid om het volgende belangrijke probleem aan te pakken.

  Aanpak: De eerste stap op deze weg is het erkennen dat conflicten en confrontaties productief zijn, dat maakt je als team sterker: als je er maar uitkomt.

- **Betrokkenheid**: Betrokkenheid van ieder teamlid gaat over duidelijkheid en steun bij het nemen van beslissingen, zonder dat men zich indekt. *Goed functionerende teams nemen duidelijke beslissingen en nemen ze tijdig*. Ze werken met complete instemming van alle teamleden, zelfs van diegenen die tegen het besluit hebben gestemd. Er is eenheid in het team.

  Aanpak: Beslissingen worden gezamenlijk genomen. De beslissingen zijn niet gebaseerd op het verlangen naar consensus, maar op het willen wegnemen van onzekerheid.

- **Verantwoordelijkheid**: Iedereen is bereid zijn verantwoordelijkheid te nemen. Het elkaar aanspreken op hun verantwoordelijkheden zorgt ervoor dat collega's die slecht presteren zich aangespoord voelen beter hun best te doen en zo beter bij te dragen aan het teamresultaat.

  Aanpak: Teamleden spreken elkaar aan op prestaties of gedragingen bij het realiseren van overeengekomen activiteiten. Lastige gesprekken worden daarbij niet vermeden. Op die manier

laten ze zien dat ze elkaar respecteren en hoge verwachtingen koesteren omtrent elkaars prestaties. Teambeloningen kunnen het nemen van verantwoordelijkheid bevorderen.

- **Resultaat**: Teams worden beoordeeld op prestaties. De focus van de teamleden ligt daarom op het bereiken van collectieve resultaten.

  Aanpak: Een duidelijke concentratie op specifieke doelstellingen en duidelijke omschreven resultaten, mede door het uitspreken van de gezamenlijk gedeelde resultaten en het uitspreken van de eigen steun.

Naast (en overlappend met) het teammodel van Lencioni kunnen de volgende tips voor het neerzetten van een team nuttig zijn:

- Zorg ervoor dat er in teams altijd een paar mensen zitten die elkaar al langer kennen.
  Dit bevordert coherentie en kennisdeling.
- Creëer een 'geefcultuur' van informele mentoring en coaching.
  In een geefcultuur geven mensen elkaar tijd, kennis, inzicht, support; tegenovergesteld aan een 'voor-wat-hoort-wat-cultuur'.
- Zorg voor de juiste capaciteiten bij mensen.
  Capaciteiten ook in de zin van relaties kunnen ontwikkelen, goed communiceren en creatief omgaan met conflicten.
- Zorg voor een sterk gemeenschapsgevoel. Gedeelde smart leidt tot emotionele binding onder medewerkers.
  Emotionele binding tussen medewerkers is de beste intrinsieke motivatie. Zoek naar commitment en filter niet gemotiveerde medewerkers eruit.
- Stel teamleiders aan die zowel taak- als relatiegeoriënteerd zijn.
  Beide oriëntaties zijn cruciaal voor teamsucces.
- Definieer scherp welke rol elk afzonderlijk teamlid heeft en geef het team tegelijkertijd speelruimte om te bepalen hoe de doelen worden bereikt.

5.3.3 Een effectief ACT-team

Onmisbaar onderdeel van de aanpak die de kracht van de organisatie benut is de actieve betrokkenheid van de staande organisatie in het ACT-team. De betrokkenheid is bij voorkeur niet beperkt tot alleen de deelname van het hoogste niveau van de lijnorganisatie in de stuurgroep: de gehele lijnorganisatie wordt betrokken bij het ACT-team. Belangrijk voor de deelname van de lijnorganisatie is de verandermanagementstijl, deze moet aansluiten bij die van het projectteam en gericht zijn op leren en verbeteren.

De lijnorganisatie blijft deel uitmaken van het ACT-team. Dit geldt ook voor na de projectfase, zodat de resultaten maximaal geborgd kunnen worden in de staande organisatie. Bij voorkeur is één van de managers van het hoogste niveau van de lijnorganisatie de voorzitter van het ACT-team.

Het ACT-team is (en blijft) verantwoordelijk voor het behalen én behouden van het volwassenheidsniveau.

5.3.4 De juiste houding

Het benutten van de kracht van de organisatie vraagt om de juiste houding van het ACT-team. Een juiste houding maakt het mogelijk mee te bewegen met de organisatie, waarbij rekening wordt gehouden met de bedrijfsbelangen. Afwegingen van het bedrijf worden meegenomen in de keuzes die nodig zijn voor een effectieve en efficiënte implementatie van de privacymaatregelen en -processen.

- **Open houding**: De privacymaatregelen en -processen kunnen tot in detail doordacht en beschreven worden, maar het is van belang dat zij aansluiten op behoefte van de organisatie. Voorstellen uit de organisatie maar ook weerstand kunnen gebruikt worden om de implementatie te versterken. Door te reageren op wat er zich in de organisatie afspeelt, ontstaat een open, ontspannen en krachtige relatie tussen de leden van het ACT-team en de organisatie.
- **Focus**: Privacybescherming vraagt om de implementatie van een palet maatregelen en processen. Implementatie van deze maatregelen kan door de organisatie als een overval worden ervaren, wat tot onrust kan leiden. Het creëren van overzicht en focus, onder andere door een op risico's gebaseerde prioritering, voorkomt dat conflicten ontstaan door het ontbreken van een (gedeelde) onderbouwing van het bedrijfsbelang.
- **'Verantwoord' verantwoordelijk**: Kennis van privacybescherming maakt het mogelijk de juiste maatregelen en processen te kiezen. Denken te weten wat goed is voor de organisatie mag echter niet verward worden met het dragen van de eindverantwoordelijkheid. De lijnorganisatie is en blijft eindverantwoordelijk voor de bedrijfsvoering. Het ACT-team is verantwoordelijk voor het aandragen van haalbare, passende en beheersbare maatregelen en processen en deze met de organisatie mogelijk te maken.
- **Enabler**: Door niet met de organisatie in gevecht te gaan en niet op eigen kracht de maatregelen en processen te implementeren, maar door op de bestaande bedrijfsprocessen aan te sluiten en uit te gaan van de bestaande middelen, voorkom je dat privacymaatregelen en -processen los van de bestaande bedrijfsinrichting worden doorgedrukt en ervaren worden als onwerkbaar of niet integreerbaar. Door wel de aansluiting te vinden op de bestaande bedrijfsprocessen en -middelen kunnen de leden van het ACT-team gezien worden als enabler van een verantwoorde bedrijfsvoering en niet als politieagent die de bestaande bedrijfsvoering verstoort.

De open houding van het ACT-team
maakt het mogelijk rekening te houden met de belangen van de organisatie.

5.3.5 De organisatie als partner

Iedere organisatie heeft haar eigen processen, dynamiek en belangen. Het kunnen doorvoeren van veranderingen is kansrijk wanneer de belangen van de organisatie en het ACT-team bekend zijn en de mensen met elkaar verbonden zijn. Pas dan is samenwerking mogelijk en is, rekening houdend met de dynamiek van de organisatie, een haalbaar ambitieniveau te bepalen. Het vraagt van de medewerkers

in het ACT-team - immers ook medewerkers in de organisatie - om een open houding om de dynamiek en de belangen van de organisatie te kunnen bepalen.

5.3.6 Analyse van de organisatie

In een SCOPAFIJTH analyse[21] wordt gekeken naar het effect van de ondersteunende processen op de verandering. Het in beeld brengen van de organisatie vraagt echter meer dan om een SCOPAFIJTH analyse. Juist de dynamiek en de belangen komen niet in beeld bij een SCOPAFIJTH analyse. Om de dynamiek en de belangen in beeld te krijgen is een gerichte analyse nodig. Een stakeholderanalyse of een krachtenveldanalyse geeft inzicht in waar stakeholders energie in willen steken. Die bereidheid is afhankelijk van de mate waarin zij bij het onderwerp betrokken zijn en vooral in de mate waarin zij hun verantwoordelijkheid ervaren. Echter ook als zij hun verantwoordelijkheid ervaren, kunnen hun eigen prioriteiten leiden tot een verminderde aandacht of zelf verzet tegen weer een verandering. Een eigen doelstelling en bijbehorende aanpak die rekening houdt met die verminderde aandacht of mogelijk verzet biedt kansen om de verandering door te voeren. Als daarbij rekening wordt gehouden met de bestaande processen en de impact beperkt blijft tot slechts het toevoegen van activiteiten aan bestaande processen zijn veranderingen met een beperkte impact door te voeren.

De aanpak van het ACT-team houdt rekening
met de krachten en weerstanden binnen de organisatie.

[21] SCOPAFIJTH staat voor de ondersteunende processen Security, Communicatie, Organisatie, Personeel, Administratieve organisatie, Financiën, Informatievoorziening, Juridisch, Technologie, Huisvesting.

Referenties

[1] **RICHTLIJN** (EU) 2016/680 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad; https://wetten.overheid.nl/EUR20160680?g=2020-07-15&z=2020-07-15.

<< terug naar pagina *5*; terug naar pagina *71*.

[2] **Wet** van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming); https://wetten.overheid.nl/BWBR0040940/2020-01-01.

<< terug naar pagina *5*; terug naar pagina *71*.

[3] **Privacy Baseline** v3.3 - CIP-publicatie in de reeks 'Grip op privacy'; https://cip-overheid.nl/productcategorieën-en-worshops/producten/privacy-bescherming/#privacy-baseline.

<< terug naar pagina *5*; terug naar pagina *69*.

[4] **Privacy Volwassenheidsmodel** - Model voor organisaties om te groeien in de omgang met privacy; CIP-publicatie in de reeks 'Grip op privacy'; https://www.cip-overheid.nl/productcategorieën-en-worshops/producten/privacy-bescherming/#handreiking-borging-van-privacy-en-volwassenheidsmodel.

<< terug naar pagina *6*; terug naar pagina *69*.

[5] **Privacy Selfassessment** (PriSa). Neem jezelf de maat, stel je een doel en zie wat je nog te doen staat bij het implementeren van privacyverantwoord handelen conform de AVG; CIP-product in de reeks 'Grip op privacy'; www.cip-overheid.nl/productcategorieën-en-worshops/producten/privacy-bescherming/#self-assessment-tool-privacy-volwassenheid-prisa–management-toelichting.

<< terug naar pagina *9*; terug naar pagina *69*.

[6] **ICO Wizard**. Met de ICO Wizard selecteer je eisenpakketten die passen bij de producten/diensten die je aanbesteedt en die je meegeeft aan de inschrijvers; CIP-product in het thema 'Veilig inkopen'; https://cip-overheid.nl/productcategorieën-en-worshops/producten/aanbesteden-en-inkopen/#ICO.

<< terug naar pagina *9*; terug naar pagina *42*.

[7] **DPIA**. Op het internet is veel te vinden over DPIA en er zijn heel wat modellen in omloop. Wij beperken hier de verwijzingen tot de AP, het model voor de 'RijksPIA' en een tweetal documenten in de de bibliotheek van CIP;

- Autoriteit Persoonsgegevens, diverse referenties: https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia;
- Model gegevensbeschermingseffectbeoordeling Rijksdienst: https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia;

- PIA-model voor ZBO's: https://www.cip-overheid.nl/productcategorieën-en-worshops/producten/privacy-bescherming/#privacy-impact-assessment-template;
- Quick Scan PIA: https://www.cip-overheid.nl/productcategorieën-en-worshops/producten/privacy-bescherming/#QS-PIA;

<< terug naar pagina *11*; terug naar pagina *42*.

[8] **Kooreman**, Martijn: Een VIP-Behandeling - Visualisatie van de InformatiePlanning bij UWV; Master of Science onderzoek BedrijfsInformatieTechnologie, Universiteit Twente, Augustus 2009; http://essay.utwente.nl/59794/1/MA_thesis_M_Kooreman.pdf.

<< terug naar pagina *14*; terug naar pagina *50*; terug naar pagina *57*.

[9] **COBIT** -Control Objectives for Information and Related Technologies; https://www.isaca.org/resources/cobit.

<< terug naar pagina *19*.

[10] **Het 7S model** (McKinsey). Het 7S-model van McKinsey beschrijft 7 factoren om een onderneming op een holistische en effectieve manier te organiseren; zie o.a.:

- http://7smodel.nl/.
- https://www.strategischmarketingplan.com/marketingmodellen/7s-model-mckinsey/.

<< terug naar pagina *21*.

[11] **Privacy by design** - Handleiding voor ontwerpers van Informatiesystemen; CIP-publicatie in de reeks 'Grip op privacy'; https://cip-overheid.nl/productcategorieën-en-worshops/producten/privacy-bescherming/#handleiding-privacy-by-design.

<< terug naar pagina *26*; terug naar pagina *42*; terug naar pagina *69*.

[12] **Wettelijke bewaartermijnen**:

- De fiscale bewaarplicht. Deze is neergelegd in artikel 52 van de Algemene Wet inzake Rijksbelastingen (AWR); https://wetten.overheid.nl/BWBR0002320/2018-01-01.
- De administratieplicht voor het bestuur van rechtspersonen, artikel 2:10 BW; https://maxius.nl/burgerlijk-wetboek-boek-2/artikel10/.
- De Archiefwet 1995 en de daaraan verbonden ministeriële regelingen. Hierin is is niet alleen bepaald hoe overheidsorganen hun archief moeten vormgeven en beheren, maar ook onder welke voorwaarden de bewaarde informatie mag worden verstrekt aan het publiek. https://wetten.overheid.nl/BWBR0007376/2020-01-01.

<< terug naar pagina *31*.

[13] **Testen met Persoonsgegevens** v2.0 (juni 2020); CIP-publicatie; https://cip-overheid.nl/productcategorieën-en-worshops/producten/privacy-bescherming/#testen-met-persoonsgegevens.

<< terug naar pagina *31*.

[14] **Gedragscode**: AVG art. 40, 41; zie ook:

- European Data Protection Board (EDPB): Guidelines 1/2019 on Codes of Conduct and Monitoring. Adopted on 12 February 2019; https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-20190219_guidelines_coc_public_consultation_version_en.pdf.
- AVG-gedragscode; https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/avg-gedragscode.

<< terug naar pagina *33*.

[15] **Padovani** M, Carvalho M M & Muscat A R N - Critical Gaps in Portfolio Management Implementation: A Brazilian Case Study. In Picmet 2006 proceedings. https://www.researchgate.net/profile/Marisa_Padovani/publication/224687152_Critical_Gaps_in_Portfolio_Management_Implementation_A_Brazilian_Case_Study/links/580bb50508ae74852b5a7191/Critical-Gaps-in-Portfolio-Management-Implementation-A-Brazilian-Case-Study.pdf.

<< terug naar pagina *48*.

[16] **Kaats**, Edwin & Opheij, Wilfrid - Leren samenwerken tussen organisaties; Kluwer, Deventer, 2012.

<< terug naar pagina *49*; terug naar pagina *58*.

[17] **Roadmap**. Gangbare term in de managementliteratuur voor een strategische planningstechniek die de doelen en belangrijke resultaten van een project (taken, mijlpalen) op een tijdlijn plaatst, allemaal gegroepeerd in een enkele visuele weergave of een afbeelding; https://www.officetimeline.com/nl/roadmap.

<< terug naar pagina *21*; terug naar pagina *50*.

[18] **Crawford**, L, & Pollack, J. - Hard and soft projects: a framework for analysis. International Journal of Project Management, 22 (2004), 645-653. https://opus.lib.uts.edu.au/bitstream/10453/4860/1/2004001481.pdf.

<< terug naar pagina *50*.

[19] **Acht factoren** bepalen de mate waarin teamleden succesvol samenwerken. Studie van de London Business School en het Concours Institute, vermeld in Managersonline, november 2006. http://www.managersonline.nl/nieuws/6441/acht-essentile-factoren-voor-succesvolle-samenwerking.html.

NB: de eerste 8 kenmerken zijn hieraan ontleend; wij hebben er een negende kenmerk aan toegevoegd.

<< terug naar pagina *54*.

[20] **Lencioni**, Patrick - De 5 frustraties van teamwork Hoe je ervoor zorgt dat het samenwerken leuk blijft (2009); https://www.managementboek.nl/boek/9789047001966/de_vijf_frustraties_van_teamwork-patrick_lencioni ; zie desgewenst ook:

- http://www.hays.nl/general-content/vijf-succesfactoren-voor-een-goede-teamprestatie-1164440.
- https://www.coachcenter.nl/is-er-binnen-jouw-team-ruimte-voor-conflict/.

<< terug naar pagina *61*.

Verder zijn geraadpleegd of is inspiratie gevonden in:

- Gardner, H. - Five minds for the future (paper, Januari 2008); https://howardgardner.com/five-minds-for-the-future/ en/of: https://duurzaamonderwijs.com/2015/01/03/5-minds-for-the-future-en-voor-het-onderwijs-van-vandaag/.
- Schermer B W, Wubben M, Falot N - Privacy Governance Handreiking Veiligheidshuizen (mei 2014); https://www.veiligheidshuizen.nl/publicaties/informatiepositie/privacy-governance-handreiking-veiligheidshuizen.
- 10 tips om conflicten op te lossen - https://www.managementsite.nl/10-tips-om-conflict-lossen.
- ZBC Kennisbank - MANAGEMENTRAPPORTAGE RISICOPROFIEL INFORMATIEBEVEILIGING ISO 27001 OF 27002; http://zbc.nu/security/aanpak-informatiebeveiliging-iso-27001-en-iso-27002/managementrapportage-risicoprofiel-informatiebeveiliging-iso-27002/.
- ZBC Kennisbank - HET OPZETTEN VAN EEN PRIVACY MANAGEMENTSYSTEEM; http://zbc.nu/security/privacy-officer-in-de-praktijk/het-opzetten-van-een-privacy-management-systeem/.

Bijlage 1: Grip op privacy

De Handleiding Privacy Governance is een publicatie in de reeks 'Grip op Privacy', het resultaat van een vraag uit het CIP-netwerk (anno 2016): schrijf eens zo eenvoudig mogelijk op hoe je als organisatie privacybescherming (volgens de wettelijke vereisten) kunt realiseren. Hieruit is een verzameling gerelateerde documenten ontstaan over de pragmatiek van privacy in organisaties. Het doel van deze documenten is praktische handvatten bieden aan organisaties die privacy in beleid en uitvoering controleerbaar willen implementeren, verbeteren en op orde houden.

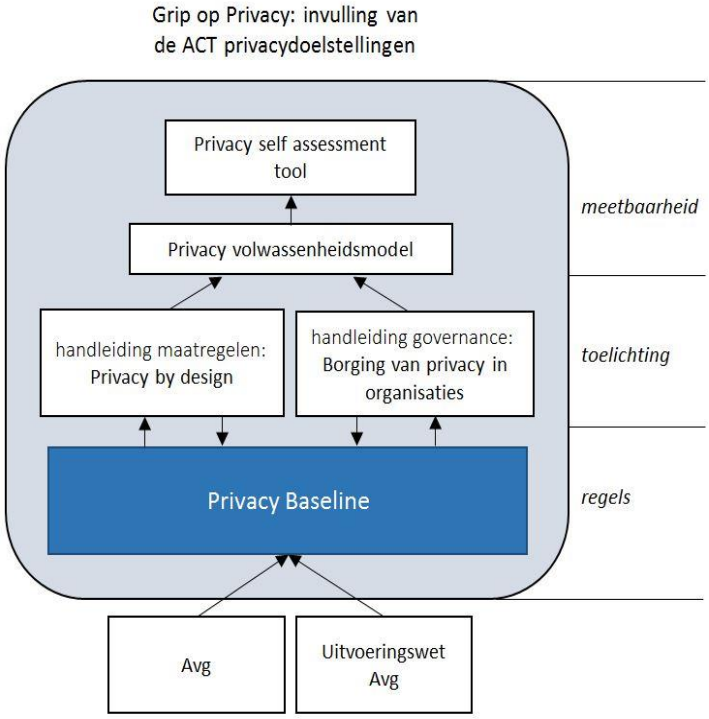
Het fundament van Grip op Privacy is de Privacy Baseline[3], de leidraad voor het voldoen aan de wettelijke vereisten voor het verwerken van persoonsgegevens. Maar het gaat niet om de wettelijke vereisten. Het gaat erom de ACT principes: Afscherming, Corrigeerbaarheid en Transparantie te realiseren en daarmee de betrokkene maximaal te respecteren in zijn privacy.

Maar hoe doe je dat en hoe hou je dat in stand? Als handreikingen c.q. hulpstukken daarbij zijn daarom, vanuit verschillende perspectieven, de volgende producten ontwikkeld. Zij zijn rechtstreeks geënt op de Privacy Baseline of georiënteerd op de bedrijfsmatige realisatie ervan:

- Privacy Governance ('Borging van privacy in organisaties')
- Privacy by Design[11]
- Privacy Volwassenheidsmodel[4]
- Privacy Self Assessment[5]

De eerste twee documenten zijn handreikingen voor het toepassen van de juiste maatregelen en het inrichten van de organisatie waarmee grip op privacy op de meest efficiënte en effectieve wijze kan worden bereikt. Het zijn toelichtende verhandelingen over:

- Hoe je kunt bewerkstelligen dat het aspect privacy niet achteraf nog eens moet worden 'bijgeplakt', maar van begin af aan in de ontwikkeling van programmatuur wordt meegenomen (privacy by design).
- Hoe je privacy in alle relevante bedrijfsprocessen implementeert, borgt, kunt onderhouden en verbeteren (governance).



Figuur 5: Grip op Privacy

Bij de Privacy Baseline hoort verder een speciaal daarop gebaseerd volwassenheidsmodel. Door privacy actief te hanteren als kwaliteitselement in de bedrijfsvoering kunnen organisaties naar een hoger niveau van volwassenheid groeien en privacy benutten om de dienstverlening aan klanten of ketenafnemers op een hoger peil te brengen. Dit aspect wordt ter hand genomen in het document 'Privacy

Volwassenheidsmodel', een praktische handleiding voor het vaststellen en vergroten van de organisatievolwassenheid in relatie tot de omgang met persoonsgegevens. Het model is afgeleid van gangbare 5-laagse volwassenheidsmodellen. Op basis van de mate waarin voldaan wordt aan de dertien criteria van de Privacy Baseline specificeert het model 5 niveaus langs het aspect van privacy.

Hoe volwassen gaat de organisatie met privacy om? Welk niveau wil de organisatie nastreven en wat is daarvoor nodig? Op deze vragen geeft het Privacy Self assessment (PriSa) antwoorden. Het assessmentrapport geeft aan wat nog te doen staat om het (zelf te kiezen) beoogde volwassenheidsniveau te bereiken. Op de website van het CIP (www.cip-overheid.nl) lees je er meer over. Daar vind je ook de overige hier aangehaalde Grip-op-privacy documenten.

Meer over de ACT-principes vind je in paragraaf 2.3 en in Bijlage 2.

Draagvlak door brede inbreng uit het CIP-netwerk

Alle documenten zijn tot stand gekomen in en vanuit de CIP-community. Het brede palet van organisaties dat daarbij betrokken is geweest geeft de auteurs het vertrouwen dat de methode 'Grip op privacy' draagvlak heeft voor een brede toepassing en verdere ontwikkeling.

Bijlage 2: De ACT-doelen

De volgende passages zijn overgenomen uit de Privacy Baseline versie 3.3, resp. uit de paragrafen 1.2 en 3.2.

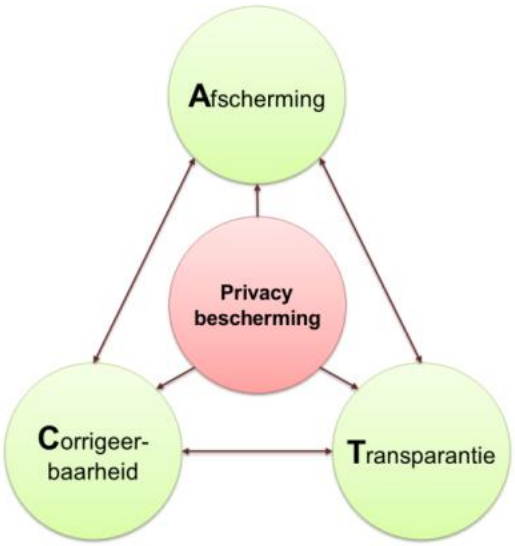
Voor organisaties die met persoonsgegevens werken bieden de AVG en de UAVG [1][2] een harde maatstaf om concreet, effectief en controleerbaar privacybeleid te voeren, volgens de drie doelstellingen *Afscherming*, *Corrigeerbaarheid* en *Transparantie* (ACT)[22].

ACT beoogt expliciet de betrokkene te beschermen. De AVG (art. 5) zegt met dezelfde bedoeling dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene "rechtmatig, behoorlijk en transparant" is. Vergeleken bij ACT is dat meer te beschouwen als een "juridische doelstelling"; ACT is een "functionele doelstelling" (overigens ook handig als richtlijn bij Privacy by Design).

Met enige lenigheid is deze trio's gemakkelijk met elkaar te verzoenen. In de (functionele) kern zijn het naar onze mening geen verschillende uitgangspunten c.q. doelstellingen. Het gaat per saldo niet om compliancy aan de wet, maar om deugdelijke privacybescherming.

De ACT-doelen zijn als volgt gedefinieerd:

- *Afscherming*: houdt in dat persoonsgegevens worden afgeschermd voor het gebruik voor andere doelen dan de doelen waarvoor ze mogen worden gebruikt.
- *Corrigeerbaarheid*: voor elke verwerking van persoonsgegevens is het mogelijk om de persoonsgegevens aan te passen of te vernietigen, indien de verwerking niet voldoet aan de eisen; bijvoorbeeld in geval van onjuiste informatie of als er geen noodzaak meer is om de informatie te bewaren.
- *Transparantie*: over elke verwerking van persoonsgegevens is de volgende informatie beschikbaar: de verantwoordelijken, de categorieën persoonsgegevens, categorieën van betrokkenen, categorieën van ontvangers, doelbinding, de wettelijke grondslag, de bewaartermijnen, de beveiligingsmaatregelen en de organisatorische en technische inrichting van verwerking van de persoonsgegevens.



Figuur 6: Privacybescherming als resultante van ACT.

[22] De ACT-privacydoelstellingen zijn gebaseerd de Privacy Protection Goals van ENISA: Unlinkability, Transparency, Intervenability; ENISA dec 2014, Privacy and data protection by design. From policy to engineering.

In de volgende tabellen staan per ACT-doel de privacyprincipes beschreven. Per privacyprincipe wordt aangegeven welke criteria leidend zijn om aan het privacyprincipe te kunnen voldoen. De ondersteunende criteria zijn randvoorwaardelijk voor een effectieve invulling van de leidende criteria.

Tabel 3: Afscherming

Afscherming		
Privacyprincipe 1: Doelbinding		
Persoonsgegevens worden slechts verzameld en verwerkt voor vooraf welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en worden niet verder verwerkt voor doelen die hiermee onverenigbaar zijn.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	U.01 Doelbinding gegevensverwerking U.05 Informatieverstrekking aan betrokkene bij verzameling persoonsgegevens	B.01, U.02
Privacyprincipe 2: Doelbinding		
De verzameling en verwerking van persoonsgegevens is toegespitst op een gespecificeerd doel met een wettelijke grondslag. De persoonsgegevens zijn daartoe toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	U.01 Doelbinding gegevensverwerking	U.02, B.03
Privacyprincipe 3: Bewaren		
Persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	U.06 Bewaren van persoonsgegevens	U.02
Privacyprincipe 4: Beveiliging		
Passende technische en organisatorische maatregelen, zoals pseudonimisering van persoonsgegevens, zijn op een dusdanige manier getroffen dat een passende beveiliging van de verwerking en de persoonsgegevens gewaarborgd is en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	U.04 Beveiligen van de verwerking van persoonsgegevens	B.03, C.03
Privacyprincipe 5: Doorgifte naar derden		
Persoonsgegevens worden slechts doorgegeven wanneer formeel afdoende garanties zijn vastgelegd, zodat aangetoond kan worden dat ook bij doorgifte aan de AVG wordt voldaan.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	U.07 Doorgifte persoonsgegevens	B.02, U.02

Tabel 4: Corrigeerbaarheid

Corrigeerbaarheid		
Privacyprincipe 6: Kwaliteit		
De persoonsgegevens en de verwerking ervan voldoen aan vooraf vastgestelde kwaliteitseisen, zodat ze juist zijn en zo nodig worden geactualiseerd en waarbij alle redelijke maatregelen moeten zijn genomen om de persoonsgegevens, die gelet op de doeleinden waarvoor zij worden verwerkt onjuist zijn, onverwijld te wissen of te rectificeren.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	U.03 Kwaliteitsmanagement	C.02

Tabel 5: Transparantie

Transparantie		
Privacyprincipe 7: Verantwoording (accountability)		
Verantwoordelijken hebben aantoonbaar maatregelen genomen, zodat de wijze van verwerken ten aanzien van de betrokkene behoorlijk is, waarbij de risico's zijn geëlimineerd of gemitigeerd door het toepassen van Privacy by Design, het uitvoeren van gegevensbeschermingseffectbeoordelingen (DPIA's) en het gebruik van standaardinstellingen.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	B.03 Risicomanagement, Privacy by Design en de DPIA C.01 Intern toezicht	B.02, U.02
Privacyprincipe 8: Recht op transparantie		
De wijze waarop de persoonsgegevens worden verwerkt is voor het publiek en de betrokkene transparant en maakt het de betrokkene mogelijk zijn rechten uit te oefenen. Hierbij is specifiek aandacht voor de bescherming van kinderen. Bij een inbreuk in verband met persoonsgegevens (datalek, 'personal data breach') worden de betrokkenen en de AP geïnformeerd als deze inbreuk waarschijnlijk een risico inhoudt voor de rechten en/of vrijheden van natuurlijke personen.		
Criteria Privacy Baseline	*Leidende criteria*	*Ondersteunende criteria*
	B.01 Privacybeleid C.02 Toegang gegevensverwerking voor betrokkenen C.03 Meldplicht Datalekken	B.02, U.02, U.05

De ACT-doelen zijn gebaseerd op de privacywetgeving en geven daarnaast invulling aan de actuele privacyprincipes, zoals beschreven door de Organisation for Economic Cooperation and Development (OECD - http://oecdprivacy.org/).