Handreiking PDCA-cyclus

Een hulpmiddel voor organisaties om een PDCA-cyclus in te richten voor privacy en informatiebeveiliging

Classificatie	Extern voor klanten
Status	Definitief
Auteurs	Susan Ashworth en Mitchell Hendriks
Opsteldatum	25 mei 2021

Lumen Group B.V.
Reactorweg 301
3542 AD UTRECHT

T +31 (0)30 889 6575
E info@lumengroup.nl
www.lumengroup.nl

IBAN: NL74 INGB 0007 8585 98
KvK: 68906803
BTW nr: 8576.42.467.B01

Versiebeheer

Versie	Datum	Door	Opmerking
V0.1	8 januari 2021	Lumen Group B.V. – Mitchell Hendriks	Eerste opzet en uitwerking.
V0.2	1 maart 2021	Lumen Group B.V. – Mitchell Hendriks	Doorontwikkeling van de eerste opzet.
V0.3	20 april 2021	Lumen Group B.V. – Susan Ashworth	Aanpassing en toevoeging n.a.v. klantfeedback.
V1.0	25 mei 2021	Lumen Group B.V. – Susan Ashworth en Mitchell Hendriks	Finalisering van de handreiking.

LUMEN GROUP privacy & data

Inhoud

1. Over deze handreiking

1.1 Inleiding

Een goed opgezette PDCA-cyclus is een belangrijk onderdeel van de implementatie en naleving van de Algemene Verordening Gegevensbescherming (AVG). Deze zorgt er onder andere voor dat periodieke controles en evaluaties plaatsvinden. Lumen Group constateert in toenemende mate dat veel klanten behoefte hebben aan handvatten voor het inrichten van een PDCA-cyclus. In dat kader hebben wij deze handreiking opgesteld, inclusief handige **voorbeeldstuurvragen** en een **voorbeeld van een AVG-checkplan**.

1.2 Voor wie is deze handreiking bedoeld?

Deze handreiking is bedoeld voor privacy-coördinatoren of andere personen die operationeel verantwoordelijk zijn voor privacy en gegevensbescherming (eerste lijn). Een functionaris gegevensbescherming (tweede lijn) kan hierbij adviseren en bovendien gebruik maken en onderdeel zijn van het toezichtskader, wat door een goede PDCA-cyclus voor haar/hem beschikbaar is.

1.3 Hoe moet je deze handreiking gebruiken?

Aangezien het inrichten van een goed werkende PDCA-cyclus geen simpel afvinklijstje is, bevat deze handreiking de benodigde achtergrondinformatie om de juiste afwegingen te maken bij de opzet en uitvoering. Hoewel implementatie van de AVG-vereisten initieel onderdeel uitmaakt van een PDCA-cyclus, ligt het zwaartepunt in de handreiking op de ‘check’-fase.

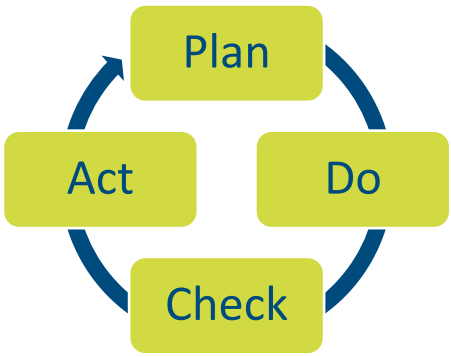
Eerst wordt uitgelegd wat een PDCA-cyclus inhoudt en waarom de PDCA-cyclus van belang is (hoofdstuk 2). Daarna is aangegeven hoe de reikwijdte en omvang van de PDCA-cyclus wordt bepaald (hoofdstuk 3). Vervolgens wordt er een beeld geschetst hoe een PDCA-cyclus er daadwerkelijk uit ziet en uit welke onderdelen deze bestaat (hoofdstuk 4). Tot slot worden er praktische handvatten gegeven middels voorbeeldstuurvragen en een voorbeeld van een AVG-checkplan (bijlagen). In bijlage C vind je op één pagina nog overzichtelijk deze handreiking in een notendop.

2. Over de PDCA-cyclus

2.1 Wat is een PDCA-cyclus?

De PDCA-cyclus staat voor: *Plan-Do-Check-Act*-Cyclus, maar wordt ook wel *Deming cycle* genoemd. De PDCA-cyclus is wereldwijd een toonaangevende methode die organisaties gebruiken om de controle en voortdurende verbetering van processen, diensten en producten te waarborgen. Het is niet de enige methode hiervoor. Het staat organisaties dan ook vrij een andere methode te hanteren. Wij richten ons op de methode van de PDCA-cyclus, vanwege de brede inzetbaarheid en de positieve ervaringen die wij hiermee hebben.

Bij een goed ingerichte PDCA-cyclus wordt de operationele werkelijkheid bewaakt aan de hand van vier fasen: *Plan*, *Do*, *Check* en *Act*. Kernonderdelen in de cyclus zijn inzicht in de stand van zaken, checks op tijd en kwaliteit, betrokkenheid en (bij)sturing op diverse (bestuurs)niveaus binnen de organisatie, verantwoording en transparantie.



Figuur 1 - PDCA-cyclus

2.2 Waarom is de PDCA-cyclus van belang?

Een centraal onderdeel van de AVG is de *verantwoordingsplicht*. Deze plicht houdt in dat organisaties verantwoordelijk zijn voor naleving van de AVG en ook daadwerkelijk moeten kunnen aantonen dat deze zich houden aan de privacyregelgeving. Bovendien betekent verantwoording ook dat organisaties de genomen maatregelen regelmatig evalueren en, indien nodig, actualiseren. Dat kan door het inrichten van een PDCA-cyclus. Deze cyclus resulteert in een gestructureerd beleid en beheersmaatregelen. Vervolgens herhaalt de cyclus zich steeds en wordt zodoende de werking van het beleid en de beheersmaatregelen regelmatig getoetst en eventueel aangepast.

Artikel 24, lid 1, AVG:

Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. ***Die maatregelen worden geëvalueerd en indien nodig geactualiseerd.***

3. Reikwijdte en omvang van de PDCA-cyclus

In dit hoofdstuk geven wij aan uit welke fasen de PDCA-cyclus is opgebouwd, welke controleraamwerken gebruikt worden en hoe de reikwijdte (scope) van de cyclus bepaald wordt.[1]

3.1 Welke fasen kent de PDCA-cyclus en wat houden deze in?

Aan de hand van de PDCA-cyclus wordt de operationele (privacy)werkelijkheid bewaakt. Dit gebeurt aan de hand van vier fasen: *Plan*, *Do*, *Check* en *Act*. Hieronder is aangeven wat deze fasen inhouden en welke centrale vragen er per fase gelden.

3.2 Hoe ziet het controleraamwerk er uit?

Binnen een PDCA-cyclus is het van belang dat er een duidelijk controleraamwerk is, waarin alle onderwerpen die van belang zijn voor een passend privacybeleid zijn opgenomen. Daar hoort ook bij dat vastligt wanneer deze controles worden uitgevoerd en vervolgens gecheckt/geëvalueerd en wanneer aanpassingen worden gemaakt. Een dergelijk controleraamwerk bestaat uit twee onderdelen: het toezicht op de inspanningen en resultaten (4.1) en het verkrijgen van informatie (4.2).

3.3 Wat is de reikwijdte van de PDCA-cyclus?

De AVG is risicogebaseerde regelgeving, waardoor ook de implementatie en naleving van de AVG op risicogebaseerde wijze kan plaatsvinden. Voor het inrichten van de PDCA-cyclus betekent dit, dat de reikwijdte ervan door het risico van de verwerkingen van de persoonsgegevens binnen de organisatie wordt bepaald. Hoe hoger het risico van de verwerkingen is, hoe

[1] Soms hebben organisaties al een bestaande PDCA-cyclus (of AO/IC) ten aanzien van andere organisatieaspecten, zoals algemeen kwaliteitsmanagement of financieel management. Mocht dat het geval zijn, dan raden wij aan om privacy en de AVG te integreren in de bestaande PDCA-cyclus (of AO/IC).

intensiever/diepgaander en vaker controle en evaluatie moet plaatsvinden en aantoonbaar gemaakt moet worden.

De onderdelen die de hoogte van het risico bepalen zijn:

- Categorieën van betrokkenen
- Hoeveelheid betrokkenen
- Soorten persoonsgegevens
- Hoeveelheid persoonsgegevens
- Context van de verwerkingen
- Hoeveelheid/omvang van de verwerkingen
- Doeleinden van de verwerking

Als is vastgesteld hoe hoog het algemene risico (bijv. door een risicoanalyse op organisatieniveau) en dus wat de reikwijdte van de PDCA-cyclus is, kan de verdere invulling van de twee onderdelen binnen de PDCA-cyclus, het toezicht en het verkrijgen van informatie, opgepakt worden.

4. Inrichting en inhoud van de PDCA-cyclus

In dit hoofdstuk worden het controleraamwerk en de reikwijdte van de PDCA-cyclus geconcretiseerd. Per fase is aangegeven welke acties er moeten worden ondernomen, hoe dit gebeurt en met welk doel. De twee onderdelen, *Toezicht op inspanning en resultaten* (PDCA-1) en *Verkrijgen van informatie* (PDCA-2), zijn twee parallel lopende onderdelen, die samen de PDCA-cyclus omvatten. Er wordt ook ingegaan op stuurvragen in de check-fase en op een passende inrichting van de (privacy)organisatie, wat essentieel is voor een goed werkende PDCA-cyclus.

4.1 PDCA-1: Toezicht op inspanningen en resultaten

Het controleraamwerk om toezicht te houden op de wijze waarop de organisatie inspanningen doet en op de resultaten die de organisatie boekt om te voldoen aan de AVG, is hieronder uitgewerkt.

Fase	Wat en hoe?	Met welk doel?
PLAN	AVG-compliant worden/blijven (de resultaten): – Bepalen wat *compliant* zijn inhoudt en doelstellingen (KPI's) op SMART-wijze vaststellen – Privacybeleid opstellen – AVG-jaarplan opstellen – Onderliggende protocollen, procedures, procesbeschrijvingen opstellen – Gegevensverwerkingen inventariseren – Risicoanalyse(s) en DPIA('s) uitvoeren	Wat is er noodzakelijk om de doelen te behalen?
DO	Acties: – Privacybeleid operationaliseren – Jaarplanacties opvolgen – Protocollen bekend maken en procedures en processen inrichten – Beheersmaatregelen n.a.v. risicoanalyse(s) en DPIA('s) implementeren – Gegevensverwerkingen in lijn brengen met art. 5 AVG – Systemen, netwerken, apparaten en applicaties/programma's configureren	Welke concrete acties moeten er worden verricht om de doelen te behalen?
CHECK	Monitoren: – (Risico-gebaseerde) zelfassessments, interne controles, audits verrichten op de uitgevoerde acties (structureel én ad hoc) – Resultaten van de controles afzetten tegen doelstellingen (KPI's)	Zijn de doelen behaald?

	– (Management)rapportages opstellen met bevindingen en aanbevelingen	
ACT	Bijstellen, wanneer nodig: – Bij niet of onvoldoende compliant zijn (hoogste) management informeren en stimuleren om aanpassingen in gang te zetten – Opstellen van een duidelijk verbeterplan naar aanleiding van de *check*-fase, dat als input dient voor de (volgende) *plan*-fase.	Moet er aanpassing plaatsvinden om de doelen te behalen?

4.2 PDCA-2: Verkrijgen van informatie

Het controleraamwerk om de informatie te verkrijgen die nodig is om goed invulling te geven aan de toezichthoudende taak en om de taken rond advisering en het geven van informatie aan de organisatie gericht te kunnen uitvoeren, is hieronder uitgewerkt.

Fase	Wat en hoe?	Met welk doel?
PLAN	Compliant worden/blijven (informatie verkrijgen): – Bepalen welke informatie nodig is om *compliancy* te toetsen en doelstellingen (KPI's) op SMART-wijze vaststellen – Jaarlijkse rapportagecyclus van afdelingshoofden of proceseigenaren instellen – Procedures, instructies, protocollen voor de registers van verwerkingen, registers datalekken, contacten inzake rechten van betrokkenen, DPIA's e.d., opstellen	Wat is er noodzakelijk om de doelen te behalen?
DO	Acties: – Op eigen initiatief of op uitnodiging op regelmatige basis aansluiten bij MT-, directie en-medewerkersoverleggen, waar besluitvorming of werkzaamheden plaatsvindt rond privacy en gegevensbescherming – Interviews houden op werkplek en informatie opvragen binnen de organisatie over het maken van verwerkingsregisters, DPIA's en over de afwikkeling van datalekken – Nieuwe ontwikkelingen op gebied van de bescherming van persoonsgegevens (o.a.	Welke concrete acties moeten er worden verricht om de doelen te behalen?

	wetgeving, IT, informatiebeveiliging) delen binnen de organisatie – Bereikbaar en zichtbaar zijn voor betrokkenen	
CHECK	Monitoren: – Opvragen en/of verrichten van (risico-gebaseerde) zelfassessments, interne controles, audits op de uitgevoerde acties (structureel én ad hoc) – Gebruik maken van (trend)analyses, besprekingsverslagen, incident-beoordelingen – Controle op de uitvoering van vastgestelde verbetermaatregelen – Resultaten controles afzetten tegen doelstellingen (KPI's) – (Management)rapportages opstellen met bevindingen en aanbevelingen	Zijn de doelen behaald?
ACT	Bijstellen, wanneer nodig: – Bij niet of onvoldoende compliant zijn, eerst de verantwoordelijke teamleider, afdelingshoofd e.d. informeren en stimuleren om aanpassingen in gang te zetten. Lukt dit niet of onvoldoende: dan escaleren naar volgend niveau – Opstellen van een duidelijk verbeterplan naar aanleiding van de *check*-fase, dat als input dient voor de (volgende) *plan*-fase.	Moet er aanpassing plaatsvinden om de doelen te behalen?

4.3 Stuurvragen voor *Check*-fase

De *Check*-fase is essentieel om vast te stellen (in welke mate) de gewenste doelen voor het compliant zijn/blijven inzake AVG-vereisten zijn behaald. Daarbij dienen de volgende vragen als uitgangspunten:

- Wat wordt er gemeten?
- Wat is het doel van de meting?
- Hoe wordt er gemeten en met welke frequentie?
- Wie voert de meting uit?
- Wie documenteert dat de meting is uitgevoerd en gerapporteerd?
- Zijn er wijzigingen die er voor zorgen dat een KPI moet worden aangepast?

In bijlage A van deze handreiking zijn voor de belangrijkste privacyonderwerpen stuurvragen opgenomen. Deze stuurvragen kunnen worden gebruikt voor het inrichten van de *checks* (en daarmee bij het opstellen van het AVG-checkplan, zoals is opgenomen verder op in deze handreiking).

4.4 Organisatiestructuur in lijn brengen

Voor een goed werkende PDCA-cyclus is het essentieel om de organisatiestructuur in lijn te brengen met de onderdelen zoals hierboven omschreven, zodat de acties zijn belegd en iedereen weet wat er van hem/haar verwacht wordt en wanneer. De privacycoördinator of persoon die verantwoordelijk is voor de operationele uitvoering van privacyzaken (of een ander persoon die jouw organisatie aanwijst) heeft de algehele coördinatie van de PDCA-cyclus in handen. Zorg er daarnaast voor dat er duidelijkheid is over wie de actie-eigenaren zijn met betrekking tot onderstaande:

- Wie is verantwoordelijk voor welke actie?
- Waarvoor is iemand verantwoordelijk (wat houdt de actie concreet in)?
- Wanneer worden de acties uitgevoerd (incl. realistische deadlines)?
- Hoe en wanneer wordt gerapporteerd (incl. minimale rapportagevereisten en de vorm hiervan)?

4.5 AVG-checkplan maken

Tot slot is het van belang om een checkplan (of breder actieplan) per jaar op te stellen. Hierdoor is het duidelijk voor de actie-eigenaren wat zij moeten controleren, wat het doel hiervan is, hoe en hoe vaak zij moeten controleren, wie de controle verricht, wie de uitvoering en uitkomsten van de controle rapporteert en hoe de eerder gestelde KPI's moeten worden aangepast.

In bijlage B van deze handreiking is een voorbeeld AVG-checkplan opgesteld voor de belangrijkste privacyonderwerpen. Dit voorbeeld kan gebruikt worden als basis voor een eigen checkplan. Hierbij is de focus gelegd op de *Check*-fase. Immers, de *Plan*- en *Do*-fase zijn bij de implementatie van de AVG-zaken over het algemeen al doorlopen. De *Check*-fase is nu het belangrijkste om de cyclus in te richten en zo aantoonbaar te maken dat wordt voldaan aan de AVG vereisten.

Bijlage A – Voorbeeld stuurvragen

De antwoorden op deze vragen helpen bij het opstellen van het AVG-checkplan (bijlage B).

1. Verantwoordingsplicht (IBP-beleid en register van verwerkingsactiviteiten)

- Is er een (vastgesteld) privacy- en informatiebeveiligingsbeleid?
- Zijn er wijzigingen in wet- en regelgeving, jurisprudentie, richtlijnen van de EDPB/AP, normen, standaarden en best practices die aanpassingen vereisen?
- Is er inzicht in gewijzigde of nieuwe processen, werkwijzen, applicaties en systemen binnen de organisatie die aanpassingen in beleid en register vereisen?
- Hoe recent is het beleid, van wanneer is de laatste update van het beleid?
- Is er een register van verwerkingsactiviteiten?
- Zijn de gegevensverwerkingen in lijn met het opgestelde beleid?
- Is het register nog compleet en actueel**,** worden de wijzigingen in het register goed bijgehouden?
- Zijn de opgenomen verwerkingen in lijn met de gesloten verwerkersovereenkomsten?
- Wordt (aantoonbaar) gebruik gemaakt van een AVG-Jaarplanning?
- Is er een Gedragscode veilig gebruik ict-middelen en persoonsgegevens?
- Is er een Social Media Protocol?
- Zijn het beleid en de protocollen/werkprocedures bekendgemaakt en (goed) vindbaar voor medewerkers?
- Worden (of zijn) er DPIA's (Data Protection Impact Assessments) verricht?
- Heeft er een risicoanalyse met betrekking tot privacy en informatiebeveiliging plaatsgevonden?
- Zijn de beheersmaatregelen naar aanleiding van risicoanalyses en DPIA's (aantoonbaar) genomen?
- Passen de genomen beheersmaatregelen nog bij de geïdentificeerde risico's?
- Worden de genomen privacy- en informatiebeveiligingsmaatregelen aantoonbaar getoetst d.m.v. (technische) audits?

2. Informatieplicht (privacyverklaring)

- Klopt de informatie in de privacyverklaring nog, is deze nog in lijn met de persoonsgegevens die verwerkt worden en zijn de contactgegevens correct?
- Is er getoetst of de privacyverklaring voor iedereen goed leesbaar en begrijpelijk is?

3. Verwerkers en verwerkersovereenkomsten

- Is er een overzicht van verwerkersovereenkomsten, incl. looptijd?
- Komen de verwerkers en -overeenkomsten nog overeen met het verwerkingsregister?
- Is er een proces van controle en beoordeling van de diensten, rapporten en registraties van verwerkers? (bijv. door middel van PEN-testen en auditverklaringen)

4. Bewaartermijnen en vernietiging van persoonsgegevens

- Is er een vastgesteld beleid Bewaartermijnen?
- Zijn de niet-wettelijke bewaartermijnen onderbouwd?
- Zijn alle werknemers op de hoogte van de bewaartermijnen en de procedures?
- Zijn de bewaartermijnen – voor zover mogelijk – ingeregeld in systemen en applicaties?
- Worden de gegevens binnen de termijnen daadwerkelijk en aantoonbaar vernietigd?

5. Rechten van betrokkenen

- Is er een protocol voor de uitoefening van de rechten van betrokkenen?
- Is het protocol Rechten van betrokkenen bekendgemaakt en vindbaar voor alle betrokkenen, dus ook de medewerkers?
- Is er een register waarin uitoefeningsverzoeken betrokkenen worden geregistreerd?
- Worden verzoeken binnen de aangegeven tijd afgehandeld?
- Zijn werknemers goed op de hoogte van het proces voor verzoeken?

6. Datalekken en -incidenten

- Is er een datalekken en -incidentenprotocol?
- Is er een register waarin datalekken en -incidenten worden geregistreerd?
- Wordt het protocol naar medewerkers bekend gemaakt? (bijv. flyers, presentaties, etc.)
- Is er getest of het protocol werkt?
- Is er een trend in de hoeveelheid beveiligingsincidenten?
- Worden phishingmails door medewerkers (goed) herkend?
- Wat is de gemiddelde tijdsduur tussen een geconstateerd incident en de opvolging?
- Wat is de gemiddelde tijdsduur tussen een geconstateerd incident en de melding naar de AP?
- Wat is de (geschatte) schade van de beveiligingsincidenten geweest sinds de laatste rapportage?

7. Bewustwording, kennis en training

- Wordt er regelmatig aandacht besteedt aan privacy en informatiebeveiliging onder de medewerkers?
- Wordt gebruik gemaakt van een programma/planning met betrekking tot kennis en bewustwording?
- Is het bewustwordingsprogramma aantoonbaar uitgevoerd?
- Is er aandacht voor soft controls?
- Is aantoonbaar hoeveel mensen hebben deelgenomen aan (onderdelen van) het bewustwordingsprogramma?
- Worden er nieuwe onderwerpen geïnventariseerd die in het volgende programma moeten worden opgenomen?

8. Technische en organisatorische maatregelen

- Is er een overzicht van de IT-/ICT-infrastructuur waarin alle applicaties en programma's zijn opgenomen, incl. bijbehorende autorisatieniveaus?
- Worden rollen en rechten (autorisaties) per applicatie/programma toegekend op basis van een autorisatiematrix? Zijn deze nog actueel?
- Is er een toegangs- en toekenningsprocedure voor autorisaties?
- Hebben er incidenten plaatsgevonden met het huidige autorisatiesysteem?
- Op welke wijze wordt de logging gecontroleerd? Is er een data leakage prevention-systeem?
- Wordt er gebruik gemaakt van USB-sticks?
- Zijn de gegevensdragers versleuteld (bijv. Bitlocker/FireVault)?
- Is er een wachtwoordenbeleid?
- Worden persoonsgegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?
- Welke bescherming is er tegen malware?
- Worden beveiligingsupdates en -patches tijdig uitgevoerd?
- Worden er back-ups gemaakt, en hoe?
- Welke (sterke) authenticatie-methoden worden gehanteerd?
- Op welke wijze is het netwerk beveiligd?
- Wordt er gebruik gemaakt van een Virtual Private Networks (VPN)
- Worden er geheimhoudingsverklaringen met medewerkers en overige personen die onder de verantwoordelijkheid van de organisatie persoonsgegevens verwerken afgesloten?
- Worden bijzondere persoonsgegevens via een versleutelde e-mail of ander communicatiekanaal gedeeld?
- Wordt de downloadmap en prullenbak op de computer automatisch geleegd?
- Worden computers vergrendeld als medewerkers weglopen van hun computer?
- Is sprake van een clean desk policy?
- Worden papieren documenten bewaard in afsluitbare kasten?

Bijlage B – Voorbeeld AVG-checkplan per jaar

Algemene uitgangspunten bij AVG-checkplan

- Het plan hieronder is nadrukkelijk bedoeld als een voorbeeld. Hierin is bijvoorbeeld gekozen voor een maandelijkse check op de technische en organisatorische maatregelen, omdat (bijvoorbeeld) is gebleken dat er veel met bijzondere persoonsgegevens van een kwetsbare groep personen wordt gewerkt en deze optimaal beschermd moeten zijn. Maar iedere organisatie moet voor zichzelf bepalen welke checks en acties nodig zijn.
- Gebruik voor het uitvoeren van de checks en de invulling van de acties de stuurvragen uit bijlage A.
- Elke *check* leidt tot een *act*. Toets daarom altijd of de genomen beheersmaatregel *genomen* is en of deze beheersmaatregel *effectief* is in de volgende ronde van de cyclus.
- Stem het plan af met de Functionaris Gegevensbescherming en neem diens checks en acties (bijvoorbeeld het afnemen van een AVG-Steekproef) ook op in het AVG-checkplan.

Periode	Check	Actie
Januari	1. Verantwoordingsplicht	– IBP-beleid, gedragsregels en werkprocedures controleren – Register van verwerkingsactiviteiten controleren – DPIA('s) controleren (1x per 3 jaar)
	4. Bewaartermijnen en vernietiging van persoonsgegevens	– Bewaartermijnen controleren – Naleving bewaartermijnen controleren
	8. Technische en organisatorische maatregelen	– Naleving en effectiviteit van genomen beheers-/beveiligingsmaatregelen controleren
Februari	2. Informatieplicht	– Privacyverklaring(en) controleren
	7. Bewustwording, kennis en training	– Naleving bewustwordingsplan/-planning controleren
	8. Technische en organisatorische maatregelen	– Naleving en effectiviteit van genomen beheers-/beveiligingsmaatregelen controleren

Maart	3. Verwerkers en (verwerkers)overeenkomsten	– Overzicht van verwerkers controleren – Verwerkersovereenkomsten controleren – Diensten, rapporten en registraties van verwerkers controleren
	6. Datalekken en -incidenten	– Afhandeling van datalekken en -incidenten controleren – Verbetermaatregelen controleren
	8. Technische en organisatorische maatregelen	– Naleving en effectiviteit van genomen beheers-/beveiligingsmaatregelen controleren
April	7. Bewustwording, kennis en training	– Naleving bewustwordingsplan/-planning controleren
	8. Technische en organisatorische maatregelen	– Naleving en effectiviteit van genomen beheers-/beveiligingsmaatregelen controleren
Mei	5. Rechten van betrokkenen	– Afhandeling rechtsverzoeken van betrokkenen controleren
	8. Technische en organisatorische maatregelen	– Naleving en effectiviteit van genomen beheers-/beveiligingsmaatregelen controleren
Juni	8. Technische en organisatorische maatregelen	– Naleving en effectiviteit van genomen beheers-/beveiligingsmaatregelen controleren
Juli	4. Bewaartermijnen en vernietiging van persoonsgegevens	– Bewaartermijnen controleren – Naleving bewaartermijnen controleren
	6. Datalekken en -incidenten	– Afhandeling van datalekken en -incidenten controleren – Verbetermaatregelen controleren
	8. Technische en organisatorische maatregelen	– Naleving en effectiviteit van genomen beheers-/beveiligingsmaatregelen controleren
Augustus	7. Bewustwording, kennis en training	– Naleving bewustwordingsplan/-planning controleren
	8. Technische en organisatorische maatregelen	– Naleving en effectiviteit van genomen beheers-/beveiligingsmaatregelen controleren

September	6. Datalekken en -incidenten	– Afhandeling van datalekken en -incidenten controleren – Verbetermaatregelen controleren
	8. Technische en organisatorische maatregelen	– Naleving en effectiviteit van genomen beheers-/beveiligingsmaatregelen controleren
Oktober	8. Technische en organisatorische maatregelen	– Naleving en effectiviteit van genomen beheers-/beveiligingsmaatregelen controleren
November	7. Bewustwording, kennis en training	– Naleving bewustwordingsplan/-planning controleren
	8. Technische en organisatorische maatregelen	– Naleving en effectiviteit van genomen beheers-/beveiligingsmaatregelen controleren
December	6. Datalekken en -incidenten	– Afhandeling van datalekken en -incidenten controleren – Verbetermaatregelen controleren
	8. Technische en organisatorische maatregelen	– Naleving en effectiviteit van genomen beheers-/beveiligingsmaatregelen controleren
Overig	Jaarlijkse rapportage Functionaris Gegevensbescherming	– (laten) uitvoeren van een steekproef om de werking van de cyclus en het voldoen aan de AVG vereisten onafhankelijk te laten toetsen.

Bijlage C – De Handreiking PDCA-cyclus in een notendop