

FG-jaarverslag 2024

Informatiebeveiliging en Privacy

PCBO Leeuwarden e.o.



Bestemd voor bestuur van: PBCO Leeuwarden	Door: Evelyn de Graaf Functionaris Gegevensbescherming Datum: 10-02-2025
Datum vastgesteld:	

Inhoudsopgave

Inleiding	3
Toezicht	3
Doel jaarverslag	3
Status Informatiebeveiliging en Privacy (IBP)	3
<i>Compliance</i>	3
NORMENKADER	6
<i>Normenkader geen afvinklijstje</i>	6
<i>Principe Comply or Explain</i>	6
<i>Governance</i>	6
<i>Groeipad en Roadmap</i>	7
Actiepunten 2024	8
<i>DPIA</i>	8
<i>Risicomanagement</i>	8
<i>Bedrijfscontinuïteit</i>	8
<i>Incidenten en datalekken</i>	8
<i>Documentbeheer</i>	9
<i>Verwerkingsregister</i>	9
<i>Bewaartermijnen</i>	10
<i>Verwerkersovereenkomsten</i>	10
<i>Toegangsbeleid en autorisatiematrix</i>	10
<i>Register rechten betrokkenen</i>	10
<i>Indienst/uitdienst</i>	10
<i>ICT: netwerk en back-up</i>	10
<i>Bewustwording</i>	11
<i>PDCA-cyclus</i>	11
MIDDELEN	11
CONCLUSIES EN AANBEVELINGEN	11
<i>Maatregelen (aanbevolen) voor 2025</i>	11
BIJLAGEN	12
<i>Bijlage 1 Roadmap</i>	12
<i>Bijlage 2 Verwerkingsregister 31-12-2024</i>	12
FORMELE VASTSTELLING	12

Inleiding

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. Met de toenemende digitalisering in het onderwijs, nemen de dreigingen en privacyrisico's toe. Het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hebben hun krachten gebundeld en het normenkader laten opstellen als onderdeel van hun programma Digitaal Veilig Onderwijs. Sinds april 2023 is het Normenkader deel Informatiebeveiliging vastgesteld en gepubliceerd, in juni 2024 gevolgd door het deel Privacy. Het Normenkader heeft als doel veilig digitaal onderwijs. Het beschrijft de normen voor digitale veiligheid en biedt voorbeeldmaatregelen voor schoolorganisaties om zich zo goed mogelijk te beschermen tegen digitale dreigingen als datalekken en cyberaanvallen. Voldoen aan het Normenkader helpt om technische problemen te voorkomen en daarmee verstoringen van bijvoorbeeld lessen en toetsen.

Het Normenkader is geen vervanging van de AVG maar door de maatregelen te implementeren die (met name) voortkomen uit de privacynormen, voldoet een organisatie wel aan een aantal verplichtingen van de Algemene Verordening Gegevensbescherming (AGV). Daarnaast blijven de principes vanuit de AVG van toepassing zoals rechtmatigheid van de verwerking van persoonsgegevens, doelbinding en dataminimalisatie. In dit jaarverslag wordt de status met betrekking tot zowel de AVG als het Normenkader Funderend Onderwijs beschreven.

Toezicht

Dit verslag is opgesteld door Evelyn de Graaf, Functionaris Gegevensbescherming (FG) van PCBO Leeuwarden. De FG ziet toe op de naleving van de AVG en voorts ook op de inrichting van het Normenkader Funderend Onderwijs. Daarnaast geeft de FG advies aan het bestuur omtrent het beleid Informatie Beveiliging en Privacy (IBP). Het bestuur is als verwerkingsverantwoordelijke zowel eindverantwoordelijk voor de naleving AVG als de inrichting van het Normenkader.

Doel jaarverslag

Doel van het jaarverslag is het Bestuur en de Raad van Toezicht op de hoogte te stellen van de huidige status van de implementatie van het IBP-beleid en het geven van advies.

Status Informatiebeveiliging en Privacy (IBP)

Hieronder wordt beschreven wat de huidige status van het managementsysteem voor Informatiebeveiliging en Privacy (AVG en Normenkader Funderend Onderwijs) is binnen PCBO Leeuwarden.

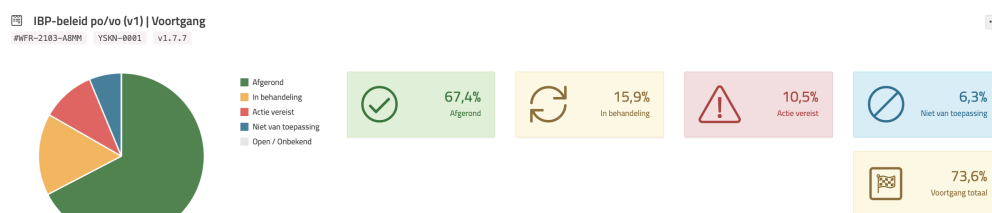
Compliance

PCBO Leeuwarden gebruikt de AVG-tooling van YourSafetynet voor het beheren van het managementsysteem voor Informatiebeveiliging en Privacy. Deze GRC-tool (Governance Risk Compliance) wordt als verantwoordingsmiddel richting stakeholders en Autoriteit Persoonsgegevens (AP) gebruikt. Met de komst van het Normenkader is er een nieuwe workflow Normenkader IBP ontwikkeld die gaandeweg de 'oude' IBP-workflow zal vervangen.

IBP Workflow

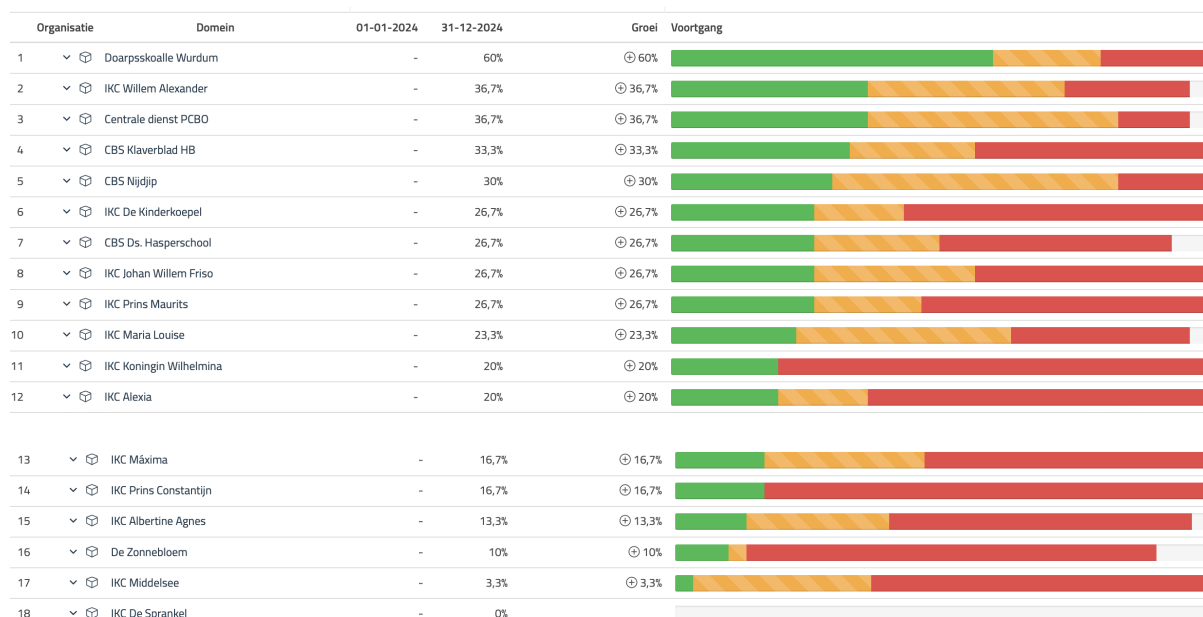
In 2024 is er verder gewerkt aan de AVG-compliance. Eind 2023 stond PCBO Leeuwarden in de IBP-workflow op 70,7 % AVG-compliance, eind 2024 op 73,6%. Dit is weer een kleine stap vooruit.

Grafiek AVG-compliance overkoepelend niveau



De workflow voor de locaties is in het najaar van 2024 uitgerold, daarmee is de bewustwording op de scholen verder vergroot. De ontwikkeling hierbij zal bovenschools worden gemonitord.

Grafiek AVG-compliance op schoolniveau



Normenkader

Het Normenkader Informatiebeveiliging en Privacy (IBP) bestaat uit de volgende domeinen:

IB (Informatiebeveiliging: 15 domeinen met 69 normen):

1. Bestuur (Governance)
2. Organisatie
3. Risicomanagement
4. Personeelsbeheer
5. Configuratiemanagement
6. Incident- en probleemmanagement
7. Changemanagement
8. Systeemontwikkeling
9. Datamanagement
10. Identity & Access Management
11. Securitymanagement
12. Fysieke beveiliging
13. IT-operatie
14. Bedrijfscontinuïteitsmanagement
15. Ketenbeheer

P (Privacy 7 domeinen met 25 normen):

1. Beleid
2. Processen
3. Organisatorische inbedding
4. Rechten van betrokkenen
5. Samenwerking
6. Beveiliging
7. Verantwoording

YourSafetynet (YSN) heeft naast de workflow IBP ook een workflow Normenkader ontwikkeld. Op 18 oktober 2024 is de nulmeting door het IBP-team afgerond in aanwezigheid van de FG. In de workflow Normenkader zijn de scores per norm ingevuld op basis van het volwassenheidsmodel (maturity model). Door de volwassenheid van het Normenkader binnen een organisatie te meten ontstaat een goed beeld van mogelijke verbeterpunten, prioriteiten en risico's. Hierdoor wordt structureel gewerkt aan de wettelijke plicht om te verbeteren.

Kleurcodes per norm op basis volwassenheidsniveau:



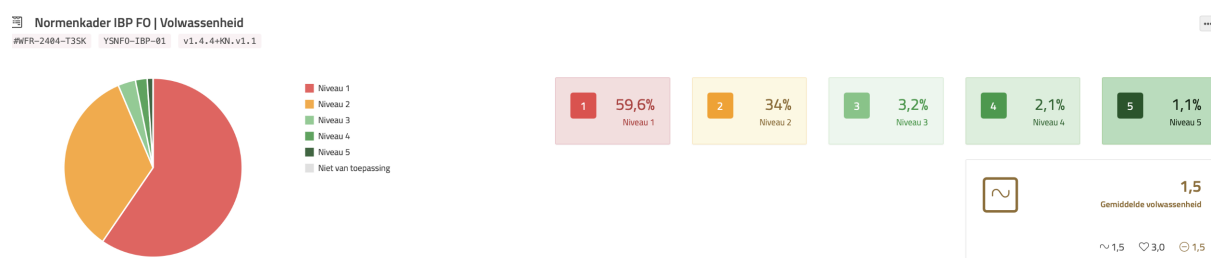
Volwassenheidsmodel (Maturity Model):

Het volwassenheidsmodel kent 5 niveaus. Het streven vanuit de overheid is dat het funderend onderwijs begin 2027 alle nomen uit het Normenkader minimaal op volwassenheidsniveau 3 heeft bereikt.

Volwassenheidsmodel: 5 niveaus

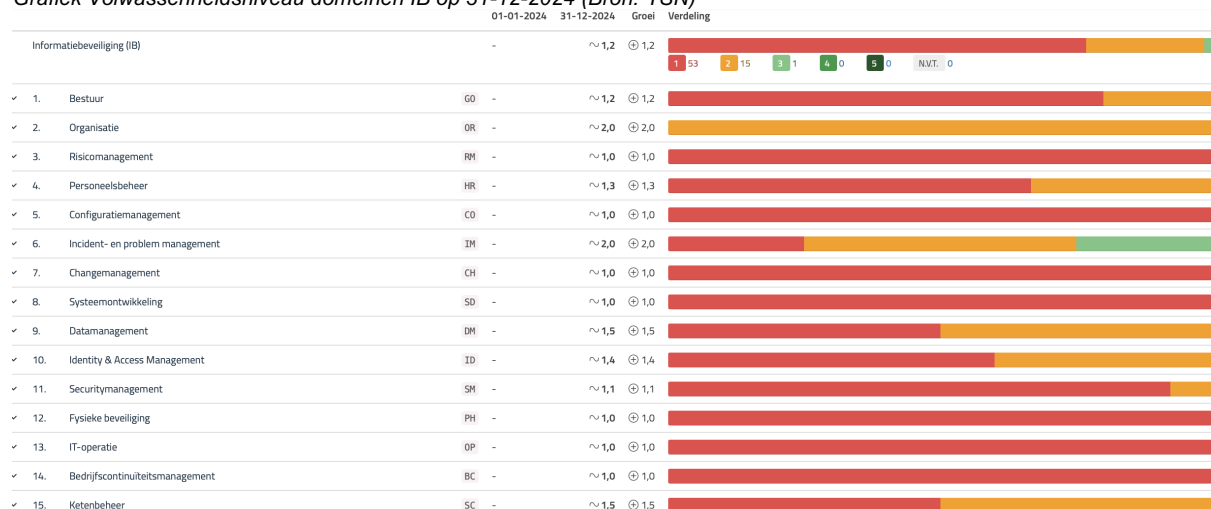
1. Ad hoc: geen maatregelen of ad hoc (reactief)
2. Herhaalbaar: informele procedures / basismaatregelen
3. **Bepaald**: beleid vastgesteld, gedocumenteerd en geïmplementeerd
4. Beheerst: geëvalueerd (gemeten, vergeleken met branche: PDCA)
5. Continu verbeteren: verbetercyclus als integraal onderdeel van bedrijfsstrategie

Grafiek volwassenheidsniveau Normenkader op 31-12-2024 (Bron: dashboard YourSafetynet)

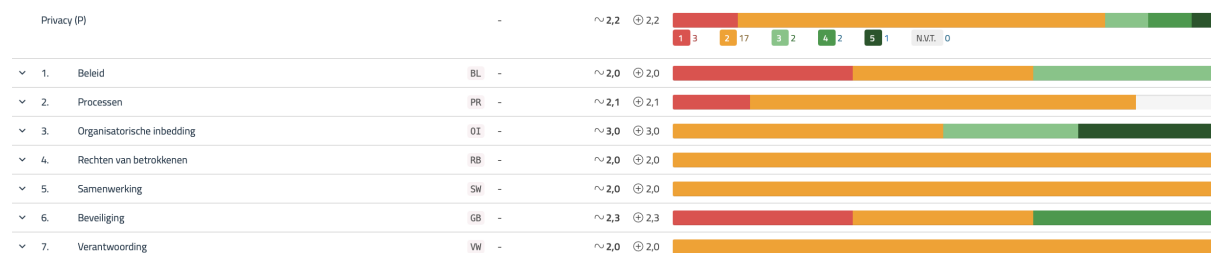


De scores laten zien dat er nog werk te doen is om begin 2027 alle normen op 'groen' te krijgen (minimaal volwassenheidsniveau 3 op 'afgerond').

Grafiek Volwassenheidsniveau domeinen IB op 31-12-2024 (Bron: YSN)



Grafiek Volwassenheidsniveau domeinen Privacy op 31-12-2024



Hoe is het grote verschil te verklaren met de 73,6% compliancy in de 'oude' IBP-workflow?

De IBP-workflow is met name gericht op de eisen vanuit de AVG. Deze eisen komen voor een deel terug in het Normenkader (deel Privacy). Het deel Informatiebeveiliging (IB) in het Normenkader is grotendeels nieuw en veel uitgebreider. In de grafieken hierboven is te zien dat het deel IB nog redelijk veel normen op

volwassenheidsniveau 1 (rood) heeft staan terwijl in het deel Privacy al veel normen op volwassenheidsniveau 3 (groen) staan en nog een aantal normen op niveau 2 (oranje). Vanuit de 'oude' workflow zou je verwachten dat er al meer privacynormen op niveau 3 'afgerond' (groen) zouden staan. Dit kan verklaard worden vanuit het feit dat het Normenkader aanvullende eisen stelt waar nog aan gewerkt moet worden.

In het totaal staat 6,4% van de normen op volwassenheidsniveau 3 of hoger (groen) en 34% op volwassenheidsniveau 2 (oranje). Niveau 2 wil zeggen dat er al informele procedures zijn of maatregelen zijn genomen maar deze zijn niet formeel vastgesteld en geïmplementeerd. Een aantal van deze normen is betrekkelijk eenvoudig naar volwassenheidsniveau 3 te brengen. Al met al een heel aardige score als startpunt om aan de slag te gaan met het Normenkader.

Het meeste werk zal gaan zitten in de 59,6% van de normen die nog op volwassenheidsniveau 1 staan (rood: nog niet of ad hoc geregeld).

NORMENKADER

Normenkader geen afvinklijstje

Met de nulmeting is de status met betrekking tot het Normenkader in kaart gebracht. De laatste openstaande onderdelen vanuit de 'oude' IBP-workflow komen terug in het Normenkader. Vanaf het najaar 2024 richt PCBO Leeuwarden zich dus volledig op de workflow Normenkader IBP. Het Normenkader vraagt om een duidelijke structuur van informatiebeveiliging en privacy. Het is geen afvinklijstje van losse normen maar betreft een samenhangend geheel van eisen waarop maatregelen moeten worden genomen (managementsysteem). Daarbij wordt gekeken naar de risico's, dat wil zeggen waar de organisatie een hoog risico loopt zullen meer maatregelen getroffen moeten worden.

In het document Roadmap (zie bijlage 1 tabblad 'Nulmeting NK') zijn de scores (volwassenheidsniveaus) voor alle normen van het Normenkader ingevuld.

Principe Comply or Explain

Bij de inrichting van het Normenkader wordt gebruik gemaakt van het principe **Comply** of **Explain**. Dit wil zeggen dat PCBO Leeuwarden het volwassenheidsniveau van een norm op 'afgehandeld' (groen) kan zetten in YSN op basis van **het voldoen aan** alle eisen (taken) OF dat de organisatie **uitlegt** op welke wijze invulling wordt gegeven aan een bepaald volwassenheidsniveau en daarmee vindt dat de organisatie voldoet. Zowel comply als explain dient onderbouwd te worden, bijvoorbeeld met beleidsprocedures, protocollen, formuleren, notulen etc.).

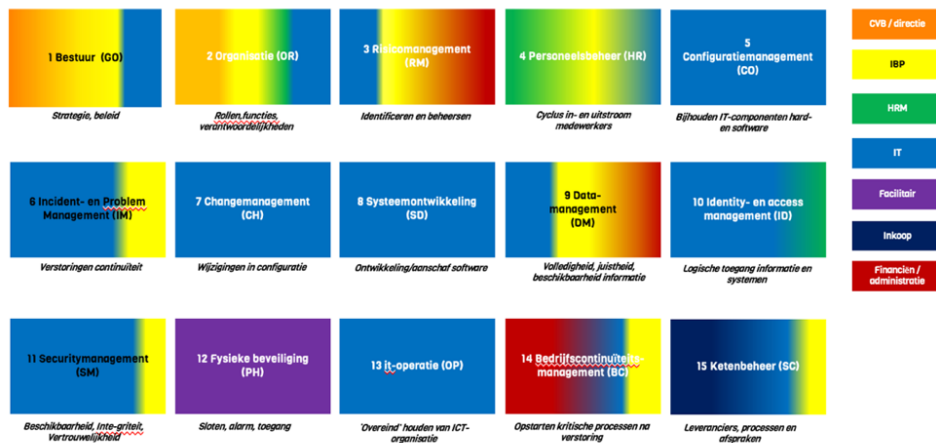
Governance

Bij PCBO Leeuwarden is er een heldere governance structuur IBP aanwezig. In het Informatiebeveiliging en Privacy-beleid (IBP-beleid) worden de missie en visie op het gebied van IBP beschreven en wordt vastgelegd welke uitgangspunten de organisatie hanteert bij het beveiligen van informatie en het garanderen van privacy van medewerkers en leerlingen. Daaruit voort vloeien de bijbehorende maatregelen, procedures en afspraken. In het IBP-beleid wordt ook vastgelegd wie verantwoordelijk is voor de uitvoering van IBP binnen de organisatie. Wie houden zich met IBP bezig en wie is daarbij eigenaar van welke processen. Binnen PCBO Leeuwarden is de huidige rolverdeling beschreven in het IBP-beleid. Er zijn nog geen proceseigenaren aangewezen. Het IBP-team binnen PCBO Leeuwarden bestaat op dit moment uit de Privacy Officer, de bovenschouls ICT-coördinator en de secretaresse. Het IBP-team heeft één keer per 4-6 weken overleg met de FG om de voortgang met betrekking tot compliance en overige privacy gerelateerde zaken te bespreken en hier een prioriteitsindicatie aan te hangen. De onderlinge relaties en verantwoordelijkheden zijn beschreven en vastgelegd in het IBP-beleid. Let op: inmiddels is er een nieuwe template IBP-beleid beschikbaar vanuit Kennisnet. PCBO Leeuwarden zal haar huidige IBP-beleid hierop actualiseren tijdens de eerstvolgende review.

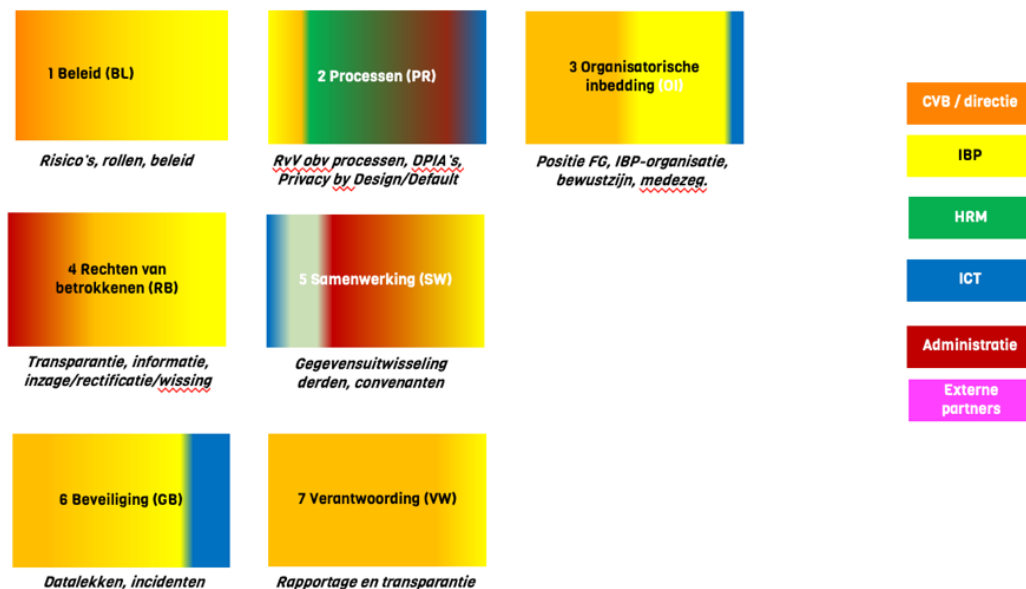
Het IBP-team is niet verantwoordelijk voor de uitvoering van het hele Normenkader en het IBP-beleid. Vanuit het IBP-team wordt de regie op het Normenkader gevoerd. Het IBP-team betreft vervolgens de diverse afdelingen bij de behandeling van de betreffende normen. Hierbij worden proceseigenaren aangewezen. De bestuurder blijft eindverantwoordelijk voor het IBP-beleid.

Bij de inrichting van het Normenkader is het daarom belangrijk om te bepalen waar de domeinen met bijbehorende normen zich bevinden in de organisatie en wie zich bezig gaan houden met de invulling van deze normen. Alhoewel vaak gedacht is het Normenkader niet (alleen) een ICT-aangelegenheid! Het Normenkader betreft de hele organisatie, zoals hieronder te zien in de overzichten IB-normen en Privacy-normen. Het is dus nodig om de juiste afdelingen te betrekken bij de verschillende normen.

Overzicht IB-normen in organisatie



Overzicht Privacy-normen in organisatie



Maatregelen:

- Actualiseren IBP-beleid
- Bepaal welke afdelingen binnen PCBO Leeuwarden betrokken moeten worden bij het Normenkader vanuit de normen Informatiebeveiliging en Privacy
- Aanwijzen proceseigenaren

Groeipad en Roadmap

Als bekend is wie zich bezig gaan houden met IBP moet er een planning gemaakt worden om in de juiste volgorde invulling te geven aan de maatregelen uit het Normenkader. Kennisnet heeft hiervoor het Groeipad ontwikkeld en adviseert het Normenkader aan de hand van dit Groeipad aan te pakken. Het Groeipad bestaat uit 5 fasen met deelprojecten die een bepaalde volgorde hebben. Het advies is dus om te starten met fase 1 en dan vervolgens naar fase 2 etc. Sommige normen komen in meerdere fasen terug en worden dan verder uitgediept.

Fase 1

Bestaat uit 8 deelprojecten met 16 normen waarbij het fundament wordt gelegd (scheppen randvoorwaarden) om de normen uit het Normenkader toe te kunnen passen (strategie en visie, rolverdeling, inventarisatie en classificatie data).

Fase 2

Bestaat uit 12 deelprojecten met 36 normen waarbij de normen in een bepaalde volgorde worden behandeld waarbij de normen die de grootste risico's afdekken als eerste worden behandeld.

Fase 3 en 4

Fase 3 bestaat uit 8 deelprojecten met 24 normen en Fase 4 bestaat uit 19 normen, waarbij net als in fase 2 de volgorde en risico's leidend zijn.

Fase 5

Bestaat uit 10 deelprojecten met 16 normen. In deze fase worden de puntjes op de i gezet waarbij de processen worden verfijnd en geoptimaliseerd.

Per norm worden de eisen bij de verschillende volwassenheidsniveaus aangegeven (in de vorm van voor gedefinieerde taken). Een volwassenheidsniveau wordt op afgerond (groen) gezet als alle bijbehorende taken zijn uitgevoerd en afgevinkt. De stappen die genomen moeten worden zijn daarmee bekend vanuit het Groeipad en daarmee is de inhoud van de roadmap (wat te doen en in welke volgorde) op hoofdlijnen bepaald. Resteert om hier een tijdlijn aan te hangen.

Vanuit de nulmeting zijn alle gescoorde volwassenheidsniveaus ingevuld in het document Roadmap (zie bijlage 1, tabblad 'Nulmeting NK'). In het tabblad 'Roadmap planning' is de planning opgenomen van de te behandelen normen.

Het streven vanuit de landelijke onderwijspartijen is dat begin 2027 alle 94 normen op volwassenheidsniveau 3 staan binnen het PO/VO-onderwijs. Dit betekent dat gemiddeld iedere week één norm afgehandeld moet worden. Ondanks dat dit redelijk ambitieus is wil PCBO Leeuwarden trachten deze planning aan te houden. Deze planning wordt besproken met de bestuurder en vastgesteld.

Maatregelen:

- *Bespreken en vaststellen Roadmap en planning*

Actiepunten 2024

DPIA

De DPIA op ParnasSys is in maart 2023 afgerond maar niet officieel vastgesteld. Inmiddels zijn echter een aantal actiepunten opgepakt en daarmee zijn de meeste risico's gemitigeerd.

Vanuit het Normenkader zal gekeken worden of er nog aanvullende maatregelen nodig zijn.

De DPIA cameratoezicht is bijna afgerond, momenteel wordt de laatste hand gelegd aan de DPIA-rapportage.

Risicomanagement

Het Normenkader stelt dat er een beleid voor risicomanagement moet zijn. Dit wordt in Fase 2 van het Groeipad opgepakt.

Bedrijfscontinuïteit

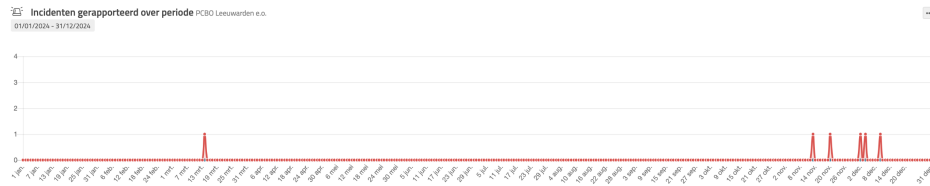
In het kader van de bedrijfscontinuïteit heeft PCBO Leeuwarden een eerste opzet voor een crisiscommunicatieplan gemaakt, inclusief bellijst.

Het Normenkader stelt ook eisen aan een Disaster Recovery Plan (DRP). De bedrijfscontinuïteit wordt vanuit het Groeipad opgepakt in fase 2 en 3.

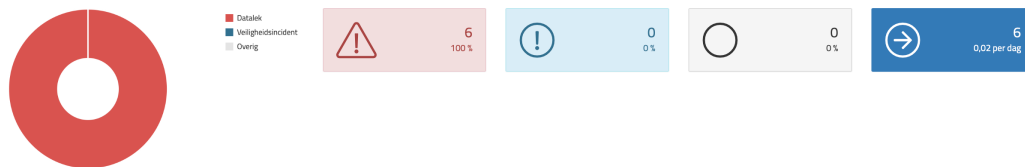
Incidenten en datalekken

In 2024 zijn zes incidenten gemeld en geregistreerd. Alle incidenten zijn gekwalificeerd als datalek, waarvan één incident is besproken met de Functionaris Gegevensbescherming (FG). Alle incidenten zijn opgenomen in het incidentregister in YSN. Er is geen melding bij de Autoriteit Persoonsgegevens gedaan omdat ingeschat is dat er door snel en correct handelen geen hoge risico's zijn ontstaan voor de betrokkenen. De FG heeft de incidenten achteraf alsnog beoordeeld. In 2025 zal de FG vaker in een eerder stadium betrokken worden bij incidenten die gekwalificeerd worden als datalek.

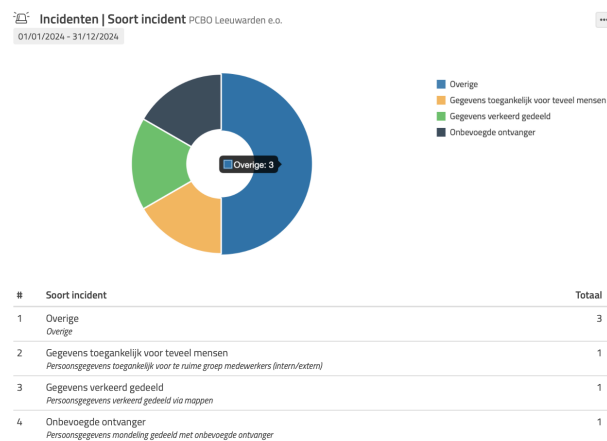
Grafiek incidenten over 2024



Grafiek verdeling datalek en incidenten over 2024



Grafiek soort incident over 2024



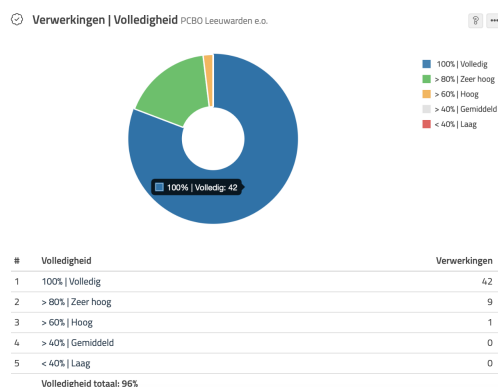
Documentbeheer

In 2024 is een aantal ontbrekende documenten opgesteld. De rest van de documenten wordt vanuit het Normenkader opgepakt.

Verwerkingsregister

Het verwerkingsregister wordt op continue basis geactualiseerd en is in 2024 gecontroleerd door de FG (zie bijlage 2).

Grafiek volledigheid verwerkingsregister



De geregistreerde verwerkingen zijn op dit moment voor 96% volledig ingevuld.
De verplichte DPIA's op de hoog risicoverwerkingen zijn uitgevoerd.

Grafiek top-risico verwerkingen



Bewaartermijnen

In 2024 is een conceptprocedure bewaartermijnen opgesteld, deze moet nog worden vastgesteld.
De gegevens van de medewerkers zijn inmiddels opgeschoond, het opschonen van de gegevens van de leerlingen vindt momenteel plaats.

Verwerkersovereenkomsten

Alle verwerkersovereenkomsten zijn gecontroleerd. PCBO Leeuwarden maakt gebruik van het convenantmodel verwerkersovereenkomst en is aangesloten bij de Dienst Kennisnet Verwerkersovereenkomsten., Versiewijzigingen van de convenantmodellen zijn daarmee beheerst. Afwijkende modellen en nieuwe verwerkersovereenkomsten worden gecontroleerd door de FG. De geactualiseerde verwerkersovereenkomsten zijn opgenomen in de bibliotheek van YSN en gekoppeld aan het digitale register van verwerkingen.

Toegangsbeleid en autorisatiematrix

De autorisatiematrix is inmiddels opgesteld maar moet nog worden gecontroleerd.
Controle op de ingestelde rechten heeft nog niet plaats gevonden. Vanuit het Normenkader wordt verdere invulling gegeven aan het toegangsbeleid en autorisatiematrix.

Register rechten betrokkenen

Het register rechten betrokkenen is geïmplementeerd maar er zijn nog geen inzageverzoeken geregistreerd.
Het is niet duidelijk of deze er niet zijn geweest of dat ze nog niet worden geregistreerd. In het kader van de bewustwording zal het melden van verzoeken in 2025 onder de aandacht gebracht moeten worden.

Indienst/uitdienst

Er is een procedure indienst/uitdienst opgesteld maar omdat er vanuit het Normenkader aanvullende eisen worden gesteld aan onder andere de werving van nieuwe medewerkers, het opleiden en de onboardingsprocedure wordt de procedure verder vanuit fase 1 van het Groeipad Normenkader opgepakt.

ICT: netwerk en back-up

Het in kaart brengen van de benodigde back-up procedures is met de komst van het Normenkader doorgeschoven en zal in Fase 2 van het Groeipad 2025 opgepakt worden.

Bewustwording

In 2024 is er veel aandacht geschonken aan de bewustwording binnen de organisatie. De workflow IBP voor scholen is uitgerold, er zijn diverse nieuwsbrieven verstuurd waarin aandacht is besteed aan IBP en de Functionaris Gegevensbescherming heeft een presentatie gegeven.

Vanuit het Normenkader wordt in fase 2 aandacht besteed aan het opstellen van een bewustwordingsprogramma.

PDCA-cyclus

De openstaande actiepunten zijn opgenomen in het IBP-jaarplan en afgehandeld of met redenen doorgeschoven omdat ze vanuit het Normenkader opgepakt zullen worden (Roadmap). Alhoewel PCBO Leeuwarden de PDCA-cyclus al toepast bij de actualisatie van de registers en de diverse IBP-documenten wordt de PDCA-cyclus vanuit het Normenkader bij volwassenheidsniveau 4 opgepakt.

MIDDELEN

Op dit moment wordt er intern gekeken naar de inzet van extra uren op het gebied van Normenkader IBP.

CONCLUSIES EN AANBEVELINGEN

PCBO Leeuwarden heeft de basis voor het managementsysteem voor Informatiebeveiliging en Privacy (IBP) staan, inclusief de verplichte registers en een protocol voor het melden van incidenten en datalekken.

Met de komst van het Normenkader worden nog aanvullende eisen gesteld waar PCBO Leeuwarden invulling aan zal moeten geven om Veilig Digitaal Onderwijs verder op de kaart te zetten.

Het Normenkader kent in totaal 94 normen waarop maatregelen getroffen dienen te worden.

Hieronder worden de maatregelen zoals hierboven benoemd en de nog openstaande actiepunten uit 2024 op een rijtje gezet. De overige maatregelen komen aan bod vanuit de aanpak Normenkader op basis van de 5 fasen van het Groeipad in 2025-2026.

Maatregelen (aanbevolen) voor 2025

- Governance (IB domein 1 GO.01-02 en Privacy domein 1 BL.01-03)
 - Actualiseren IBP-beleid bij review
 - Bepaal welke afdelingen binnen PCBO Leeuwarden betrokken moeten worden bij welke domeinen/normen
 - Aanwijzen proceseigenaren
- Roadmap Fase 1 Groeipad
 - Opstellen Roadmap Normenkader + planning
 - Bespreken Roadmap + planning met bestuurder
- Bewaartermijnen:
 - Vaststellen procedure bewaartermijnen
- Toegangsbeleid en autorisatiematrix (Domein 10 IB ID 01-02):
 - Checken autorisatiematrix
 - Controle op ingestelde rechten
- Rechten betrokkenen (IB domein 4 RB.01-04)
 - Registreren verzoeken in register rechten betrokkenen (inzageverzoeken)
- Personeelsbeheer (IB domein 4 HR.01-06)
 - Opstellen procedure personeelsbeheer (werving, opleiding, onboarding/wijziging etc.)
- Bewustwording (IB domein 4 HR.06 en Privacy domein 3 OI.04)
 - Opstellen bewustwordingsprogramma 2025: oa blijvende aandacht voor het melden en registreren van incidenten/datalekken, rechten betrokkenen en phishing

BIJLAGEN

Bijlage 1 Roadmap

Bijlage 2 Verwerkingsregister 31-12-2024

FORMELE VASTSTELLING

Het Bestuur stelt het FG-jaarverslag formeel vast.

Ondertekening Bestuur

Naam:

Handtekening:

Datum: