# Werken aan het IBP Normenkader met Myndr

Hieronder vind je een lijst met alle normen uit het IBP Normenkader die betrekking hebben op de samenwerking met Myndr. We noemen de punten uit de volwassenheidsniveaus waarbij wij ter sprake *kunnen* komen en welke standaarden van toepassing zijn.

1. **Informatiebeveiliging**

   **Domein 4: Bewustwording en informatiebeveiliging. NORM HR.06 Veiligheidsbewustzijn.**
   *Omschrijving uit volwassenheidsniveaus:*
   Er is een bewustwordingsprogramma opgenomen in het informatiebeveiligingsplan en dit wordt organisatiebreed uitgevoerd.

   *Op onze website kun je informatie vinden over veilig internetten in de vorm van blogs en artikelen. Deze kunnen ondersteunend zijn in de bewustwording.*

   **Domein 8: Informatiebeveiliging.**
   **NORM SD.01 Methodiek voor veilige softwareontwikkeling en -implementatie**
   *Omschrijving uit volwassenheidsniveaus:*
   Voor elke nieuwe ontwikkeling of aanschaf is goedkeuring nodig van het juiste niveau van het school- of it-management.
   De methodiek voor toetsing van softwarekwaliteit bevat verplichte ‘mijlpalen voor informatiebeveiliging’ (met inbegrip van risicobeoordeling, broncodebeoordeling en tests) die niet kunnen worden omzeild. Deze worden gedocumenteerd.

   Van toepassing: *AVG, ROSA, PEN-test*

**Domein 9: Datamanagement. NORM DM.03 Beveiligingseisen voor datamanagement.**

*Omschrijving uit volwassenheidsniveaus:*

Er is een beleid bepaald, geïmplementeerd en gecommuniceerd om gevoelige data te beschermen tegen ongeautoriseerde toegang en incorrecte uitwisseling.

Van toepassing: *AVG, ROSA*

**Domein 11: Securitymanagement. NORM SM.03 Mobiele apparaten en telewerken**

*Omschrijving uit volwassenheidsniveaus:*

Informatiebeveiliging wordt geborgd bij het gebruik van mobiele apparaten en telewerkfaciliteiten. Mobile device management, versleuteling en bescherming tegen malware zijn aanwezig om de risico's te beperken.

Van toepassing: *Myndr blokkeert alle malware voor leerlingen*

**Domein 11: Securitymanagement. NORM SM.12  Beheersing van malware-aanvallen**

*Omschrijving uit volwassenheidsniveaus:*

Er is anti-malwarebeleid gedefinieerd, gedocumenteerd en gecommuniceerd.
Geautomatiseerde antivirussoftware is in gebruik en formeel vastgelegd.
Er zijn maatregelen genomen om het verspreiden van malware te beperken.

Van toepassing: *Myndr blokkeert alle malware voor leerlingen, ROSA*

**Domein 15: Ketenbeheer. NORM SC.01 Service Level Agreement**

*Omschrijving uit volwassenheidsniveaus:*

IT-services die aan de organisatie worden geleverd, worden gedefinieerd in het contract en bijhorende SLA. Checklist Eisen aan leveranciers en de IT-eisen uit ROSA.

Van toepassing: *SLA, ROSA*

**Domein 15: Ketenbeheer. NORM SC.02 Service Level Management**
*Omschrijving uit volwassenheidsniveaus:*
De performance van de services worden periodiek gerapporteerd in een service level rapport (SLR), en indien nodig besproken met de leverancier.

Van toepassing: *je ontvangt wekelijkse rapportages en kunt resultaten monitoren in je dashboard*

**Domein 15: Ketenbeheer NORM SC.03 Leveranciersrisicomanagement.**
*Omschrijving uit volwassenheidsniveaus:*
Contracten zijn volgens algemene bedrijfsstandaarden en voldoen aan wet- en regelgeving (bijvoorbeeld dataprivacy).
Voordat de contracten worden ondertekend wordt een toetsing verkregen, die aantoont dat de levering van diensten voldoet aan wet- en regelgeving en aan het eigen (beveiligings)beleid.

Van toepassing: *verwerkersovereenkomst volgens PCO-04*

**Domein 15: Ketenbeheer NORM SC.04 Interne beheersing bij derden**
*Omschrijving uit volwassenheidsniveaus:*
De status van de interne beheersmaatregelen van de externe dienstverleners wordt periodiek geëvalueerd.
Er zijn procedures om te garanderen dat externe dienstverleners zich aan de contractuele verplichtingen houden.

Van toepassing: *verwerkersovereenkomst volgens PCO-04, Ethisch hacken*

## 2. Privacy

**Domein 2: Processen NORM PR.04 en DPIA'S NORM PR.05 Identificatie risico's gegevensverwerking met behulp van pre-DPIA's**
*Omschrijving uit volwassenheidsniveaus:*
Er is een methode/procedure vastgesteld om voor alle nieuwe en gewijzigde verwerkingen te bepalen of deze mogelijkerwijs een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.

Van toepassing: *verwerkersovereenkomst volgens PCO-04, DPIA*

### Domein 2: Processen NORM PR.06 Gegevensbescherming door privacy by design en privacy by default

*Omschrijving uit volwassenheidsniveaus:*
Voorafgaand aan de inkoop of de ontwikkeling van toepassingen, diensten en producten vindt systematisch een beoordeling plaats van de privacyrisico's. Hierbij worden de benodigde maatregelen vastgesteld om de privacybeginselen van art. 5 lid 1 AVG na te leven.

Van toepassing: *AVG, ROSA, verwerkersovereenkomst volgens PCO-04, DPIA, PEN-test*

### Domein 3: Organisatorische inbedding NORM OI-04 Bewustwording bescherming persoonsgegevens

*Omschrijving uit volwassenheidsniveaus:*
Medewerkers zijn goed geïnformeerd over hun verantwoordelijkheden met betrekking tot privacy en de bescherming van persoonsgegevens en handelen daarnaar.
Leerlingen worden op een planmatige manier geïnformeerd over het belang van privacy en de bescherming van persoonsgegevens.

*Op onze website kun je informatie vinden over veilig internetten in de vorm van blogs en artikelen. Deze kunnen ondersteunend zijn in de bewustwording.*

### Domein 5: Samenwerking. NORM SW.01 AVG-rollen

*Omschrijving uit volwassenheidsniveaus:*
De organisatie heeft de AVG-rollen van de organisatie en die van externe partijen duidelijk en inzichtelijk gemaakt en medewerkers zijn zich bewust van het belang om AVG–rollen te onderscheiden.
Er worden consistent afspraken gemaakt met verwerkers, gezamenlijke verwerkingsverantwoordelijken en eventueel zelfstandig verwerkingsverantwoordelijken.

Van toepassing: *AVG, ROSA, verwerkersovereenkomst PCO*

**Disclaimer:**
Aan dit artikel kunnen geen rechten worden ontleend. Scholen zijn zelf verantwoordelijk voor het voldoen aan het Normenkader IBP. Myndr wil met dit artikel ondersteunend zijn in het implementeren van het Normenkader, maar kan niet aansprakelijk gesteld worden indien niet aan alle normen wordt voldaan. In geval van onjuistheden of onvolledigheden worden wij graag op de hoogte gebracht.