Informatiebeveiliging en privacy beleid

mboRijnland

Versiebeheer

Versie	Status	Datum	Auteur	Omschrijving
0.1	Concept	3-7-2019	Ludo Cuijpers	1e Draft
0.2	Concept	5-7-2019	Vincent Reijnen en Ludo Cuijpers	Aanpassen aan functies en processen mboRijnland
0.3	Concept	8-7-2019	Vincent Reijnen en Ludo Cuijpers	2e Draft
0.4	Concept	17-7-2019	Jaco Opschoor, Vincent Reijnen en Ludo Cuijpers	3e Draft
0.8	Concept	19-7-2019	Vincent Reijnen en Ludo Cuijpers	Eind draft Besluit 30, Calamiteitenplan ICT toegevoegd
0.9	Concept	6-8-2019	Niels Dutij en Ludo Cuijpers	Bijlage 2 nader bekeken
0.91	Concept	12-8-2019	Niels Dutij en Ludo Cuijpers	Bijlage 2 afgerond
0.92	Concept	19-8-2019	Niels Dutij, Vincent Reijnen en Ludo Cuijpers	Slotversie
0.93	Concept	25-9-2019	Jaco Opschoor, Vincent Reijnen en Ludo Cuijpers	FD gewijzigd in FD (hoofdstuk 3)
0.94	Concept	26-9-2019	Vincent Reijnen	Paragraaf 2.8.Logging en monitoring aangepast
0.95	Concept	02-10-2019	Niels Dutij, Vincent Reijnen en Ludo Cuijpers	Opmerkingen van Frans Noordman verwerkt
0.96	Concept	4-10-2019	Vincent Reijnen	Opmerkingen van Gydo van Dorland verwerkt.

Vastgesteld door mboRijnland:

Versie	Datum	Naam	Functie
1.0	29-10-2019	CvB	CvB

1. Verantwoording en richtlijnen

1.1. Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan, met name ook van minderjarigen[1]. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

1.2. Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.
Informatiebeveiliging richt zich op de volgende aspecten:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten volledig, juist en actueel zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades, boetes en imagoverlies.

1.3. Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:
Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens[2].

1.4. Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één geheel: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis om informatiebeveiliging en privacy binnen mboRijnland te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

1.5. Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen van wie mboRijnland persoonsgegevens verwerkt, waaronder studenten, hun ouders/verzorgers en medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a.

[1] Groene woorden worden in bijlage 3 (Verklarende woordenlijst) toegelicht

[2] Bewerkt artikel 2, lid 2 van de AVG.

medewerkers, studenten en hun ouders/verzorgers) wordt gerespecteerd en mboRijnland voldoet aan relevante wet- en regelgeving.

1.6. Reikwijdte

- Het IBP-beleid binnen mboRijnland geldt voor alle betrokkenen, te weten: medewerkers, studenten, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing).

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van mboRijnland. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken (b.v. uitspraken van medewerkers, op (persoonlijke pagina's van) websites en of social media.). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.

- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van mboRijnland evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- IBP-beleid heeft binnen mboRijnland raakvlakken met:
  - *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen.
  - *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.
  - *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen
  - *Medezeggenschap* van studenten, hun ouders/verzorgers en medewerkers.

1.7. Concretisering[3]

mboRijnland hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het **College van Bestuur** van mboRijnland neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de **verwerkingsverantwoordelijke**.

2. mboRijnland voldoet aan alle **relevante wet- en regelgeving**.

3. Bij mboRijnland is de verwerking van persoonsgegevens altijd gekoppeld aan een **specifiek doel** en gebaseerd op één van de **wettelijke grondslagen**. Een goede balans tussen het belang van mboRijnland om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming in- en herzien.

4. mboRijnland zal alle **betrokkenen helder en actief informeren** over de verwerkingen van hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, aanvullen, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit, afscherming en profilering van hun persoonsgegevens.

5. mboRijnland legt alle **verwerkingen van persoonsgegevens** vast in een **dataregister** en zal deze up-to-date houden. mboRijnland voldoet hiermee aan de documentatieplicht, zoals benoemd in de AVG.

6. Binnen mboRijnland is het **veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van**

[3] Deze uitgangspunten zijn operationeel uitgewerkt en toegelicht in bijlage 1.

eenieder. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.

7. mboRijnland is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het **eigendom** (auteursrecht) **toebehoort aan derden**. Medewerkers en studenten worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. mboRijnland **classificeert informatie en informatiesystemen**. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.

9. mboRijnland sluit met **alle leveranciers van digitale onderwijsmiddelen** (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken.

10. mboRijnland verwacht van alle **medewerkers, studenten, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen** met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. mboRijnland heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. **Informatiebeveiliging en privacy is bij mboRijnland een continu kwaliteitsproces**, waarbij regelmatig (minimaal jaarlijks) wordt ge-audit of een self assessment wordt uitgevoerd en wordt gekeken of een aanpassing gewenst dan wel noodzakelijk is.

12. mboRijnland kijkt bij **wijzigingen** (denk ook aan uitfasering) in de infrastructuur of de **aanschaf van nieuwe (informatie)systemen** vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

13. mboRijnland neemt **passende organisatorische of technische (beveiligings-)maatregelen** om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.

14. mboRijnland zal alle **beveiligingsincidenten en datalekken** vastleggen, volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

15. mboRijnland kiest ten aanzien van informatiebeveiliging (**autorisatie en authenticatie**) voor de vooronderstelling "Alles is in principe verboden tenzij het uitdrukkelijk is toegelaten"[4] in plaats van de zwakkere regel "Alles is in principe toegelaten tenzij het uitdrukkelijk is verboden".

[4] Op basis van functie/rollen worden rechten door de leidinggevende toegekend. Een functioneel beheerder kent de rechten feitelijk toe. Bijvoorbeeld: een HR adviseur mag alleen de dossiers van de aan hem/haar toegewezen medewerkers inzien, als dat noodzakelijk is vanwege de opgedragen werkzaamheden.

2. Compliance

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

2.1. Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet Educatie en Beroepsvorming (WEB)
- Branche code Goed Bestuur MBO, MBO Raad
- Wet Inspectietoezicht
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Archiefwet
- Auteurswet
- Wetboek van Strafrecht
- Koppelingswet

De internationale normenkader voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.
mboRijnland hanteert het Toetsingskader Informatiebeveiliging en Privacy dat ontwikkeld is door MBO-Raad (saMBO-ICT). Ook hanteert mboRijnland het NBA (Nederlandse Beroepsvereniging van Accountants) toetsingskader als self assessment tool.

2.2. Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens te weten:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld, inclusief de bewaartermijnen. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.
3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie**: de school legt aan betrokkenen (studenten, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast informatie, inzage, verbetering, aanvullen, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit, afscherming en profilering van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens volledig, juist en actueel zijn.

2.3. Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende documenten. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

2.4. Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd op basis van het ROSA model. Het niveau van de te nemen beveiligingsmaatregelen is

afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitscriteria die van belang zijn.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden middels een centraal ingeregeld DPIA (Data Protection Impact Assessment). Vanaf de start van nieuwe (ICT)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

2.5. Incidenten en datalekken

Alle medewerkers die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings-)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings-)incidenten kunnen worden gemeld bij het IPCP (Informatiebeveiliging en Privacy Crisis Team) middels TOPdesk.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.
Studenten en externen kunnen kwetsbaarheden melden bij privacy@mborijnland.nl.

2.6. Planning en controle

Dit IBP-beleid wordt jaarlijks gereviewed en eventueel bijgesteld door het bestuur. Hierbij wordt rekening gehouden met:

- de status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
- de actuele geinventariseerde risico's;
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan.

Daarnaast kent mboRijnland een jaarlijkse verbeterplan voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het IBP-beleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen. Een en ander leidt tot een jaarplan IBP.

2.7. Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Naleving van ons IBP-beleid is een primaire verantwoordelijkheid van alle medewerkers binnen mboRijnland. Daar boven nemen de leidinggevenden en proceseigenaren hun verantwoordelijkheid om hun medewerkers aan te spreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, d.m.v. een instelling brede gedragscode, d.m.v. periodieke bewustwordingscampagnes, et cetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.
Mocht de naleving van dit beleid ernstig tekort schieten, dan kan mboRijnland de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

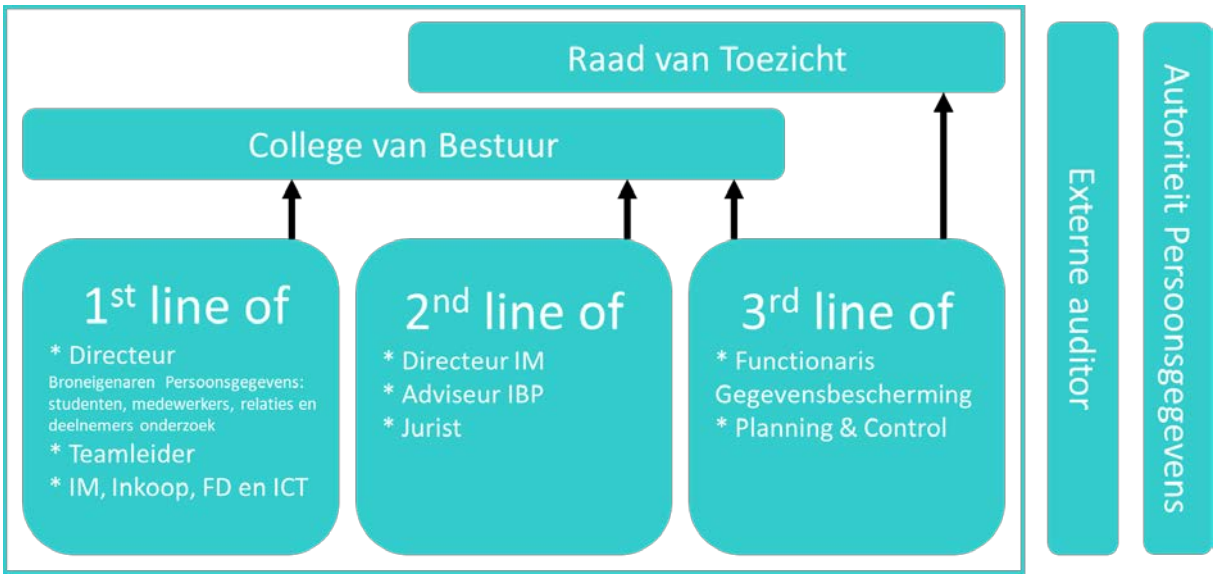
2.8. Logging en monitoring

Logging en monitoring door het team ICT en applicatie eigenaar zorgt er voor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk. mboRijnland zal deze logging regelmatig beoordelen.

3. Governance

3.1. Rollen en verantwoordelijkheden

mboRijnland hanteert het three lines of defense model. De eerste lijn binnen dit model is cruciaal, immers de directeuren en teamleiders moeten er op toezien dat de AVG wordt nageleefd. Daartoe zijn alle leidinggevenden geschoold en zij zien erop toe dat al hun teamleden handelen volgens het vastgesteld IBP-beleid. Schematisch als volgt weergegeven.



3.2. De first line of defense: directeur, teamleider, IM, Inkoop, FD en ICT

De eerste lijn bewaakt het privacybeleid binnen hun eigen organisatorische onderdeel (bijvoorbeeld onderwijs). Directeuren, teamleiders, IM, Inkoop, FD en ICT vormen de first line of defense als het gaat om de bescherming van persoonsgegevens. Directeuren, teamleiders, IM, Inkoop, FD en ICT voeren de daarbij horende operationele taken uit, zoals:

- toetsen dat geen andere verwerkingen plaatsvinden als vastgelegd in de dataregisters voor studenten, medewerkers en relaties,
- toetsen dat een Verwerkersovereenkomst of een Gezamenlijk Verantwoordelijkenovereenkomst wordt afgesloten als persoonsgegevens worden overgedragen aan externe partijen,
- beoordelen van incidenten rond persoonsgegevens en het intern melden daarvan als het vermoeden bestaat dat het gaat om een datalek.

Directeuren en teamleiders voeren bovendien de volgende operationele taken uit:

- toetsen dat hun medewerkers voldoende geschoold zijn in het kader van de AVG,
- vastleggen van de extra taken en rollen van medewerkers en de daarbij behorende rechten binnen de bijbehorende systemen/processen.

3.3. De second line of defense: directeur IM en adviseur IBP van mboRijnland

Experts op het gebied van informatiebeveiliging en privacybescherming werken samen binnen de stafdienst Informatiemanagement. De stafdienst Informatiemanagement monitort de toepassing en naleving van het informatiebeveiligings- en privacybeleid, adviseert, gevraagd en ongevraagd, over informatiebeveiliging en privacybescherming en ondersteunt de first line. De stafdienst Informatiemanagement ontwikkelt waar nodig beleid op het gebied van informatiebeveiliging en privacy, het College van Bestuur stelt dit voorgenomen beleid vast.
De stafdienst Informatiemanagement wordt geleid door de directeur Informatiemanagement. Hij geeft leiding aan de werkzaamheden van de stafdienst Informatiemanagement. De stafdienst Informatiemanagement vormt de second line of defense als het gaat om de bescherming van persoonsgegevens.

3.4. De third line of defense: de Functionaris voor Gegevensbescherming en Planning & Control

a) de Functionaris voor gegevensbescherming

mboRijnland heeft een interne toezichthouder op de verwerking van persoonsgegevens aangesteld. Deze toezichthouder wordt functionaris voor gegevensbescherming genoemd (hierna: "FG"). De FG zal door mboRijnland tijdig worden betrokken bij alle aangelegenheden waar persoonsgegevens bij komen kijken. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie binnen mboRijnland. mboRijnland heeft de FG aangemeld bij de nationale toezichthoudende autoriteit, de zogenaamde Autoriteit Persoonsgegevens.

De taken van de FG houden in:

- het informeren en adviseren van alle betrokken partijen over hun verplichtingen onder de AVG,
- het toezien op de naleving van de AVG en andere relevante privacywetgeving,
- het toezien op de naleving van dit IBP beleid door mboRijnland,
- het toezien op een Data Protection Impact Assessment,
- het behandelen van klachten over de toepassing van het privacyreglement,
- fungeren als eerste aanspreekpunt voor en samenwerken met de Autoriteit Persoonsgegevens.

b) Planning & Control

Externe controles worden uitgevoerd door onafhankelijke accountants. Deze worden gepland en geformuleerd door de afdeling Planning & Control van mboRijnland.

3.5. De taken van de medewerkers

Onderwerp	1st line of defence	2nd line of defence	3rd line of defence
Autorisaties	Management[5] brengt autorisaties in kaart (SOLL) en toetst dit bij de Functioneel beheerders (IST). ❶ (stap 1)	De stafdienst Informatiemanagement controleert of het SOLL en IST autorisatie vergelijk is uitgevoerd. ❷ (stap 2)	De FG'er controleert of de autorisaties zijn ingericht op basis van *need-to-know* en *least privilege*. ❸ (stap 3)
Beleidsdocumenten	Directeur, teamleider, IM, Inkoop, FD en ICT zien er op toe dat de goedgekeurde kaders en richtlijnen uit de beleidsdocumenten worden uitgevoerd. ❷	De stafdienst Informatiemanagement schrijft en evalueert de beleidsdocumenten en bespreekt deze met alle stakeholders en de FG'er en dient ze in bij het CvB ter goedkeuring. ❶	De FG'er toetst de kwaliteit van het beleid en de werking van het door het CvB goedgekeurde beleid. ❸
Bewaartermijn	Directeur, teamleider en FD zijn verantwoordelijk voor het handhaven van de bewaartermijnen conform het Documentair StructuurPlan (DSP). ❶	De stafdienst Informatiemanagement adviseert aan de hand van de het Documentair StructuurPlan (DSP) de 1st line over de geldende bewaartermijnen. ❷	De FG'er ziet er op toe dat de bewaartermijnen worden nageleefd. ❸
Bewustwording	Management voert het opleidingsplan van de stafdienst Informatiemanagement uit of stelt een afgeleid opleidingsplan vast. ❶	De stafdienst Informatiemanagement stelt een opleidingsplan op voor IBP-scholings- en awareness plannen en faciliteert ook centrale trainingen. ❷	De FG'er toetst het gewenste kennisniveau aan de scholings- en awareness plannen en komt eventueel met aanbevelingen. ❸
DPIA's	• Directeur, teamleider, IM, Inkoop, FD, ICT en projectleiders voeren een pré DPIA uit bij ieder nieuw ICT project. ❶ • Directeur, teamleider, IM, FD, ICT en projectleider voeren een DPIA uit op in opdracht van de FG. ❹	De stafdienst Informatiemanagement komt op basis van de pré DPIA, uitgevoerd door de 1st line, tot een voorstel om al dan niet een DPIA uit te voeren en wordt betrokken bij de uitvoering van de DPIA. ❷	De FG'er besluit op basis van het voorstel van de stafdienst Informatiemanagement of er een DPIA moet worden uitgevoerd en adviseert gevraagd of ongevraagd over de DPIA. ❸ De DPIA wordt slechts vastgesteld na goedkeuring van de FG. ❺

[5] Met management worden directeuren en teamleiders bedoeld.

Datalekken	Medewerkers melden zelf intern een datalek via TopDesk. Het management draagt zorg voor bekendheid van de meldprocedure en scholing van haar medewerkers. 1	De FG'er informeert de stafdienst Informatiemanagement over de gemelde datalekken. 3	De FG'er besluit, na overleg met het CvB, om al dan niet het datalek bij de AP en/of de betrokkenen te melden. 2
Dataregisters centraal	De in § 3.7 aangewezen verantwoordelijke directeuren (broneigenaren) voor de Dataregisters bewaken de actualiteit van het dataregister. 1	De stafdienst Informatiemanagement adviseert en controleert op volledigheid, juistheid en actualiteit van de Dataregisters. 2	De FG toetst of het dataregister voldoet aan wet- en regelgeving. 3
Door het management aangewezen uitvoerders	Het management wijst de deelprocesuitvoerders aan (bijv. examinering, roostering, stage, etc.). 1	De stafdienst Informatiemanagement toetst het toegewezen eigenaarschap aan de autorisatie. 2	De FG 'er toetst of het eigenaarschap beschreven is. 3
Rechten van de betrokkenen	Het management ontvangt het verzoek van de FG'er en neemt deze in behandeling (controle door afdeling Studentzaken of afdeling Personele Zaken). 2	De FG'er informeert de stafdienst Informatiemanagement over het aantal verzoeken. 3	De FG'er is het eerste aanspreekpunt en volgt de vastgestelde procedure. 1
Verwerkersovereenkomsten	De betrokken directeur, teamleider, Inkoop, FD en ICT zorgt dat er altijd een verwerkersovereenkomst is opgesteld en kan de stafdienst Informatiemanagement hiervoor advies vragen. De directeur, teamleider, Inkoop, FD en ICT stuurt de verwerkersovereenkomst ter goedkeuring aan de FG. 1	De stafdienst Informatiemanagement adviseert bij verwerkersovereenkomsten op verzoek van de first line. 2	De FG'er toetst de verwerkersovereenkomst op rechtmatigheid en volledigheid. Het College van Bestuur tekent na akkoord van de FG'er. 3
Vragen van medewerkers betreffende IBP gerelateerde onderwerpen	Het management is het eerste aanspreekpunt voor vragen inzake privacy en security, medewerkers kunnen de stafdienst Informatiemanagement ook zelf benaderen. 1	De stafdienst Informatiemanagement adviseert de manager en/of medewerker. 2	De FG'er controleert de gestelde vragen en de oplossingen. 3

3.6. Implementatie beleid

Het College van Bestuur is verantwoordelijk voor de verwerkingen van persoonsgegevens binnen mboRijnland. Het College van Bestuur wordt aangemerkt als de verwerkingsverantwoordelijke in de zin van de wet AVG. De verantwoordelijkheid houdt kort samengevat in:

- dat de persoonsgegevens verwerkt worden in overeenstemming met de vastgestelde doelen van de verwerking, dat die doelen gerechtvaardigd zijn en dat de verwerking zorgvuldig gebeurt,
- dat hierover verantwoording kan worden afgelegd aan de Autoriteit Persoonsgegevens.

De feitelijke verwerking van persoonsgegevens wordt echter op allerlei lagen van mboRijnland uitgevoerd. Het is niet één instituut of dienst die effectief verantwoordelijk kan zijn voor alle persoonsgegevens die mboRijnland verwerkt. Er is een onderscheid tussen centrale verwerkingen, waarvoor de Shared Service Centra (SSC) of stafdiensten verantwoordelijk zijn, en, aanvullend daarop, decentrale verwerkingen, waarvoor het onderwijsteam of individuele SSC zelf verantwoordelijk is.

3.7. Verdeling van de verantwoordelijkheden

mboRijnland onderscheidt een viertal soorten verwerkingen van persoonsgegevens met daarbij benoemde broneigenaren:

- het SSC Administraties (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle mensen die bij mboRijnland onderwijs volgen. Het SSC Administraties is verantwoordelijk voor het Dataregister met studentgegevens,
- het SSC Administraties (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle mensen die in opdracht van mboRijnland, zowel centraal als decentraal, werk verrichten. Het SSC Administraties is verantwoordelijk voor het Dataregister van medewerkers,
- de dienst Marketing en Communicatie (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle mensen waarmee mboRijnland centraal een relatie onderhoudt, zoals belangstellenden, sollicitanten, oud-werknemers, contactpersonen van de stageverlenende organisaties en leveranciers, potentials en alumni. Deze dienst is verantwoordelijk voor het Dataregister van deze relaties,
- de opdrachtgever van onderzoek (broneigenaar) dat mboRijnland uitvoert, zowel centraal als decentraal, is verantwoordelijk voor de verwerkingen van persoonsgegevens in het kader van dat onderzoek. Een onderzoeksvoorstel wordt altijd voorgelegd aan de stafdienst Informatiemanagement.

Deze toewijzing van verantwoordelijkheden houdt ook in dat elke manager die buiten de genoemde broneigenaren om, eigen persoonsgegevens verwerkt of verrijkt, zélf verantwoordelijk is voor die aanvullende persoonsgegevens. Zij dienen deze verwerkingen te melden bij de functionaris voor gegevensbescherming en te documenteren.

3.8. Inpassing in de instellingsgovernance en afstemming met aanpalende beleidsterreinen

Om de samenhang in de organisatie met betrekking tot gegevensbescherming goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van verwerking van persoonsgegevens binnen de verschillende onderdelen op elkaar af te stemmen, is het belangrijk om gestructureerd overleg te voeren over het onderwerp privacy op verschillende niveaus.
Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van privacyaspecten. Het strategisch niveau wordt voorbereid door de stafdienst Informatiemanagement.
Op tactisch niveau wordt de strategie vertaald naar plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering. Het tactisch niveau wordt ingevuld door de stafdienst Informatiemanagement.
Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan. Het operationeel niveau wordt ingevuld door de directeur, teamleider, IM, Inkoop, FD en ICT, zowel op centraal als decentraal niveau.

3.9. Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Noodzakelijk is het om het bewustzijn voortdurend aan te scherpen, zodat bij mboRijnland kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordings-campagnes voor medewerkers, studenten en relaties. Verhoging van het bewustzijn is de verantwoordelijkheid van elke leidinggevende en wordt gefaciliteerd door het de stafdienst Informatiemanagement.

3.10. Controle en naleving

Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert gezamenlijk met de 2nd line en Planning & Control de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens.
Eventuele externe controles worden uitgevoerd door onafhankelijke accountants. Deze externe controles worden gepland en geformuleerd in een nauwe samenspraak met Planning & Control van mboRijnland.
Mocht de naleving op de bescherming van data- en privacygegevens ernstig tekortschieten, dan kan mboRijnland de betrokken verantwoordelijke medewerkers een maatregel opleggen, binnen de kaders cao-mbo en de wettelijke mogelijkheden.
Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten mboRijnland maken het noodzakelijk om periodiek te bezien of men nog voldoende op koers zit met het beleid.

Bijlage 1: Ondersteunende documenten

Deze bijlage bevat een aantal aanvullende documenten. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

	IBP beleid 1.7 Concretisering:	mboRijnland document:	Bron:
1	College van Bestuur, verwerkingsverantwoordelijke	IBP-beleid mboRijnland, hoofdstuk 3	MBO-Raad, Kennisnet
2	Relevante wet- en regelgeving	IBP-beleid mboRijnland, hoofdstuk 2	MBO-Raad, Kennisnet
3	Specifiek doel en wettelijke grondslag	• Dataregisters • Toestemmingsverklaring	• MBO-Raad • Eigen versie
4	Betrokkenen helder en actief informeren	Privacy verklaring voor medewerkers en studenten	MBO-Raad, Kennisnet
5	Verwerkingen van persoonsgegevens (dataregisters)	• Dataregister medewerkers • Dataregister studenten • Dataregister relaties	MBO-Raad, Kennisnet
6	Veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van eenieder	• Privacyreglement medewerkers • Privacyreglement studenten	• Goedgekeurd door OR • Goedgekeurd studentenraad
7	Eigendom toebehoort aan derden	Auteursrecht	MBO-Raad, Kennisnet
8	Classificeren informatie en informatiesystemen	BIV classificatie	MBO-Raad, Kennisnet
9	Leveranciers van digitale onderwijsmiddelen	Model verwerkersovereenkomsten mboRijnland	MBO-Raad, Kennisnet
10	Medewerkers, studenten, (geregistreerde) bezoekers en externe relaties gedragen zich ‘fatsoenlijk’	• 10 grondregels mboRijnland • Handboek AVG voor medewerkers • Reglement verantwoord gebruik ICT-faciliteiten door medewerkers van mboRijnland	• ROC Nijmegen • Eigen versie • Bewerkte versie saMBO-ICT
11	Informatiebeveiliging en privacy is een continu kwaliteitsproces	Self assessment op basis van ISO27001/2	MBO-Raad, Kennisnet
12	Wijzigingen en aanschaf van nieuwe (informatie)systemen	• Privacy by design/default • DPIA • OTAP beleid	• Fontys Hogescholen • Rijksoverheid en NOREA • Eigen versie
13	Passende organisatorische of technische (beveiligings-)maatregelen	DPIA, deel 2	Rijksoverheid en Norea
14	Beveiligingsincidenten en datalekken	Beleid datalekken mboRijnland	Eigen versie
15	Autorisatie en authenticatie	• Autorisatie- en authenticatiebeleid mboRijnland • Boek 9 (Autorisatie)	• Eigen versie • Eigen versie

Bijlage 2: Besluitenlijst

Besluit 20: Mobiele apparatuur.
Voor mobiele apparatuur geldt de 3 Treden regeling:
Trede 1 - Gebruik de applicatie

Persoonsgegevens worden zoveel als mogelijk opgeslagen in de applicaties.
Toelichting: persoonsgegevens in applicaties zijn in het algemeen goed beveiligd door toekenning van rollen en rechten en een persoonlijke account.

Trede 2 - Gebruik het mboRijnland opslag aanbod (bijvoorbeeld: SharePoint, Teams, OneDrive)

Het kan noodzakelijk zijn om persoonsgegevens verder te verwerken, terwijl dat niet in de hiertoe aangewezen applicatie kan. Voor de opslagen van dergelijke verder verwerkte gegevens kan het netwerk gebruikt worden.

Trede 3 - Gebruik encryptie

Is het lokaal opslaan van persoonsgegevens op eigen apparatuur (zoals de BYOD-apparatuur) onvermijdelijk dan geldt: gebruik wachtwoordbeveiliging en encryptie als je gegevens op bijvoorbeeld je eigen device of een USB-stick of een externe harde schijf plaatst.

Samenvattend:
- Persoonsgegevens worden opgeslagen in centrale versleutelde databases, indien dit niet mogelijk is dan encrypted opslaan op een device (bijv. usb).
- mboRijnland maakt gebruik van een versleutelprogramma (bijv. Bitlocker).
- Sleutels worden opgeslagen bij ICT.

Besluit 21: Classificatiemodel.
mboRijnland hanteert het ROSA classificatiemodel en de uitkomsten van de classificatie worden openomen in het dataregister.

Besluit 22: Bewaartermijnen.
mboRijnland hanteert het DSP (Documentair Structuur Plan) van de MBO Raad.

Besluit 23: Lidmaatschap IBP-netwerk, SCIRT en SCIPR.
mboRijnland is actief lid van communities op gebied van IBP, bijvoorbeeld saMBO-ICT, IBP-Netwerk saMBO-ICT, SCIPR en SCIRT.

Besluit 24: Thuiswerken.
Medewerkers mogen thuis alleen applicaties ontsluiten, die gegevens bevatten met de vertrouwelijkheid “Hoog”, als zij gebruik maken van multi factor authenticatie.

Besluit 25: Responsible disclosure procedure.
Hackers kunnen (op ethisch verantwoorde wijze) kwetsbaarheden ontdekken in onze beveiliging. Daar kunnen we van leren en mogelijke schade voorkomen. Hier het beleid hoe mboRijnland hiermee omgaat (communicatie, eventuele beloning) en wat de spelregels zijn voor de melder.
Als een ethische hacker aan deze regels voldoet, zullen wij geen aangifte bij de politie doen.

Wat wij van de hacker eisen:
- *Geen openbaarmaking of wijziging van onze gegevens;*
- *Onze gegevens en/of de kwetsbaarheid niet delen met anderen;*
- *Ons zo snel mogelijk (maar uiterlijk binnen 24 uur) en zo volledig mogelijk informeren op privacy@mborijnland.nl;*
- *Geen gebruik te maken van deze gegevens door bijvoorbeeld extracties te maken van de database of andere handelingen met de gegevens uit te voeren;*

- *dat de hacker de gegevens zo spoedig mogelijk en volledig verwijderd van zijn/haar systemen inclusief back-up voorzieningen;*
- *mboRijnland inzicht te geven in de wijze van hacken;*
- *mboRijnland inzicht te geven in de details van de gehackte informatie.*

Wat wij de hacker beloven:
- *We ondernemen geen juridische stappen;*
- *We reageren binnen 5 werkdagen;*
- *We handelen dit vertrouwelijk af;*
- *We houden hem/haar op de hoogte.*

Dit beleid is gepubliceerd op de openbare website van mboRijnland.

Besluit 26: Clear desk, Clear screen.

Clear Screen:
Medewerkers dienen hun laptop, computers of andere device te vergrendelen, zodra zij hun device achterlaten. Medewerkers dienen dit bijvoorbeeld te doen als zij een kop koffie gaan halen, naar het toilet gaan etc. Een device mag niet onvergrendeld toegankelijk zijn voor studenten en collega's of andere derden.

Technisch afdwingen:
SSC FD & ICT is verplicht om apparatuur die in beheer is van mboRijnland automatisch na maximaal 15 minuten inactiviteit te vergrendelen. De directeur SSC FD & ICT kan deze termijn verkorten als hij dat noodzakelijk acht voor de veiligheid. Van een BYOD-apparaat is het technisch afdwingen niet mogelijk, maar medewerkers hebben de plicht om zelfstandig hun scherm te vergrendelen als het apparaat niet wordt gebruikt door de medewerker.

Clean desk:
Medewerkers zijn verplicht om privacygevoelige informatie en bedrijfskritische informatie in een afgesloten omgeving op te slaan. Medewerkers mogen dit niet op hun bureau onbeheerd laten liggen. Medewerkers zijn verplicht de aangewezen kasten te gebruiken voor de opslag van hun fysieke documenten en dienen deze kasten ook telkens af te sluiten.

De leidinggevende is verantwoordelijk voor een goede uitvoering van het clean-desk beleid. De locatie-directeur is verantwoordelijk en aanspreekpunt voor het (laten) plaatsen van voldoende afsluitbare kasten en omgevingen.

Papierversnipperaar en beveiligde containers:
Iedere locatie dient in het bezit gesteld te worden van papierversnipperaars of beveiligde containers voor de afvoer van vertrouwelijke informatie. Medewerkers zijn verplicht om privacygevoelige informatie en bedrijfskritische informatie in deze papierversnipperaars of beveiligde containers te doen als papier wordt weggegooid.
SSC FD & ICT is verantwoordelijk voor een goede uitvoering van dit beleid.

Besluit 27: Back-up van informatie.
mboRijnland heeft als back-up beleid het uitgangspunt dat de default-instellingen van de leverancier worden overgenomen. Voor de kernsystemen van mboRijnland geldt aanvullend:
- Een verplichting om afspraken vast te leggen in een Service Level Agreement;
- Een verplichting aan de zijde van de leverancier om tenminste 1 keer per dag een back-up te maken;
- De Recovery Point Objective is maximaal 1 uur;
- Viermaal per jaar dient leverancier een restore test uit te voeren;
- Afspraken van de leverancier dienen gecontroleerd te kunnen worden.

Besluit 28: Logging.
mboRijnland logt in ieder geval de werking en het gebruik van de top 10 aan kernsystemen. Logging wordt toegepast met de volgende doelstellingen:
- Ontdekken van fouten in soft- en hardware (security, IBP gerelateerd);
- Ontdekken van fouten door menselijk handelen (misbruik gerelateerd);
- Ontdekken van indringers (niet realtime, maar na analyse van logs);

- Ondersteunen bij forensisch onderzoek.

Algemeen
Het raadplegen van de technische logbestanden kan alleen door het team ICT en applicatie eigenaar. Bij het toepassen van logging gelden de volgende regels:

- Het toepassen van logging is in ieder geval verplicht op onze kernsystemen.
- Het actief zijn van de logging-services wordt gemonitord.
- Logbestanden worden maximaal 3 maanden bewaard, tenzij een incident het noodzaakt om logging langer te bewaren. Specifieke logbestanden kunnen langer bewaard blijven bijv. t.b.v. een forensisch onderzoek.
- Er is een automatische en tijdige signalering van het vollopen van log-opslagruimte.
- Het handmatig verwijderen en wijzigen van logbestanden wordt gelogd.
- Er is geen logging van gegevens waarmee beveiliging kan worden doorbroken (wachtwoorden).
- Leveranciers moeten mogelijkheden bieden om logging te kunnen (laten) controleren.
- Logging van de kernsystemen wordt op basis van een deelwaarneming en regelmatig gecontroleerd op onregelmatigheden door de bron-eigenaar conform het informatiebeveiligings- en privacy beleid.
- Tenminste eenmaal per maand zal een deelwaarneming worden uitgevoerd, waarbij onregelmatigheden worden opgespoord.

Te loggen gegevens
De volgende gegevens worden in ieder geval gelogd binnen de kernsystemen:
- het inloggen/uitloggen van een gebruiker;
- autorisatie-wijzigingen;
- het raadplegen/wijzigen van gevoelige gegevens, waarbij gegevens met een categorie Hoog op het dataregister van toepassing is.

Besluit 29: Calamiteitenplan ICT
- Het calamiteitenplan sluit aan bij het wettelijke calamiteitenplan van mboRijnland.
- Bij een ICT calamiteit is er een crisisteam beschikbaar tenminste bestaande uit: CvB, directeur Informatiemanagement, directeur FD & ICT, teamleider ICT, FG, één directeur onderwijs en directeur M&C.
- Voor datalekken geldt het beleid c.q. procedure datalekken.

Besluit 99: Dit besluit (BOEK9) is gebaseerd op hoofdstuk 9 van ISO27002, Toegangsbeveiliging.

Bijlage 3: Verklarende woordenlijst

AVG:	Algemene Verordening Gegevensbescherming.
Beleid:	Beleid met betrekking tot het verwerken van persoonsgegevens door mboRijnland.
Betrokkene:	Een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft.
Broneigenaar:	Aangewezen directeur die verantwoordelijk is voor persoonsgegevens van één of meerdere categorieën van Betrokkenen. De Broneigenaar voert de persoonsgegevens in en zorgt voor de vernietiging. In de tussentijd leent hij ze uit aan de organisatorische eenheden binnen mboRijnland. De organisatorische eenheden mogen dan de persoonsgegevens verrijken.
Datalek:	Een inbreuk in verband met persoonsgegevens, die leidt tot enige ongeoorloofde verwerking daarvan. Hier vallen zowel opzettelijke als onopzettelijke inbreuken onder.
Dataportabiliteit:	Het recht om persoonsgegevens en informatie over te dragen aan een nieuwe verwerker zonder technische problemen.
Dataregister:	De AVG spreekt van het Register van Verwerkingsactiviteiten, dit is een overzicht van de persoonsgegevens die verwerkt worden, met informatie over het doel daarvan, de grondslag daarvoor, de bewaartermijnen van de gegevens en bron of ontvanger van de gegevens. mboRijnland heeft drie centrale registers: dat voor studentgegevens, voor medewerker gegevens en voor relatiegegevens. Het dataregister is het Register van Verwerkingsactiviteiten aangevuld met de BIV-classificatie en de autorisatie matrix op hoofdlijnen.
DPIA:	Data Protection Impact Assessment (Gegevensbeschermingseffectbeoordeling): een beoordeling die helpt bij het identificeren van privacy risico's en de handvaten levert om deze risico's te verkleinen tot een acceptabel niveau. Soms ook wordt de term PIA gebruikt, Privacy Impact Assessment.
Functionaris voor Gegevensbescherming:	Interne toezichthouder en privacy adviseur aangesteld door het College van Bestuur, op grond van artikel 37 van de AVG, ook wel aangeduid als FG.
Kernsystemen:	De hoofdsystemen voor: SIS, HR, Financiën, Rooster, ELO, MIS, CRM, IDM, Office en ARBO.
Minderjarige:	Voor de AVG geldt iedere persoon die de leeftijd van 16 jaar nog niet heeft bereikt. Buiten de AVG geldt uiteraard jonger als 18 jaar.
Niet-geautomatiseerde verwerking:	Voorbeelden: aangetekende stukken, pasjes die zichtbaar gedragen worden, klassenlijsten met foto's (smoelenboek), etc.
Persoonsgegeven:	Elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon.
Privacy by Default:	Een gegevensverwerking waarbij de standaardinstellingen van producten en diensten zo zijn ingesteld dat de privacy van betrokkenen maximaal wordt gewaarborgd. Dit betekent onder meer dat er zo min mogelijk gegevens worden gevraagd en verwerkt.
Privacy by Design:	Al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) wordt ten eerste aandacht besteed aan privacy verhogende maatregelen. Ten tweede wordt rekening gehouden met dataminimalisatie: er worden zo min mogelijk persoonsgegevens verwerkt, alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.
Verwerker:	een door mboRijnland ingeschakelde (derde) partij die ten behoeve van mboRijnland, en op basis van haar schriftelijke instructies, persoonsgegevens verwerkt, e.e.a. vastgelegd in een verwerkersovereenkomst.
Verwerking:	elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, afschermen, wissen of vernietigen van gegevens.
Verwerkingsverantwoordelijke:	College van Bestuur van mboRijnland dat het doel en de middelen van de verwerking van persoonsgegevens vaststelt.