G02 Beleid

De Kempel

Vastgesteld door De Kempel:

Versie	Datum	Naam	Functie
1.04	14-01-2026	R. Verbruggen	Voorzitter CvB

Verantwoording en richtlijnen

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 en de komst van AI. 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.

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.

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].

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, is de basis voor informatiebeveiliging en privacy binnen De Kempel te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en een bijdrage leveren aan de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen van wie De Kempel persoonsgegevens verwerkt, waaronder studenten, samenwerkingspartners en medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen

[1] Groene woorden worden in bijlage 1 (Verklarende woordenlijst) toegelicht
[2] Bewerkt artikel 2, lid 2 van de AVG.

privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkenen (o.a. medewerkers en studenten) wordt gerespecteerd en De Kempel voldoet aan relevante wet- en regelgeving.

Reikwijdte

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

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van De Kempel. 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 en studenten in discussies, op (persoonlijke pagina's van) websites en of social media.). Onder dit beleid[3] 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 De Kempel 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 De Kempel raakvlakken met:

- *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement (Integrale veiligheid), huisvesting en ongevallen.
- *Personeels- en organisatiebeleid;* met als aandachtspunten in-, door- en uitstroom van medewerkers, taak-wisselingen, functiescheiding en vertrouwensfuncties.
- *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen
- *Medezeggenschap;* van studenten en medewerkers.

Concretisering

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

1. Het **College van Bestuur** van De Kempel 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. De Kempel voldoet aan alle **relevante wet- en regelgeving**.

3. Bij De Kempel 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 De Kempel 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 allen tijde hun toestemming in- en herzien.

4. De Kempel 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. De Kempel legt alle **verwerkingen van persoonsgegevens** vast in een **dataregister** (register van verwerkingen) en zal deze up-to-date houden. De Kempel voldoet hiermee aan de documentatieplicht,

[3] Dit beleid wordt nader uitgewerkt in een reglement.

zoals benoemd in de AVG.

6. Binnen De Kempel is het **veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van 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. De Kempel 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. De Kempel **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. De Kempel sluit met **alle leveranciers van digitale onderwijsmiddelen** (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken.

10. De Kempel 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. De Kempel heeft hiervoor een privacyreglement (en privacyverklaring) geformuleerd, vastgesteld en geïmplementeerd.

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

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

15. De Kempel 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.

Compliance

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

Relevante wet- en regelgeving

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

- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)[5]
- Archiefwet
- Auteurswet
- Branche code Goed Bestuur Hogescholen – Vereniging Hogescholen
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Wet onderwijstoezicht
- Wet op het Hoger Onderwijs

Het NBA (Nederlandse Beroepsvereniging van Accountants) toetsingskader is leidend voor de te nemen beveiligingsmaatregelen. De Kempel hanteert het Toetsingskader NBA en Privacy dat ontwikkeld is door SURF.

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[5]:
    a. Er is toestemming van de persoon om wie het gaat.
    b. Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren.
    c. Het is noodzakelijk om gegevens te verwerken omdat dit wettelijk verplicht is.
    d. Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen.
    e. Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefen.
    f. Het is noodzakelijk om gegevens te verwerken om een gerechtvaardigd belang te behartigen.
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 heeft de betrokkene recht op informatie, inzage, verbetering, aanvullen, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens ten behoeve van automatische profilering.
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens volledig, juist en actueel zijn.

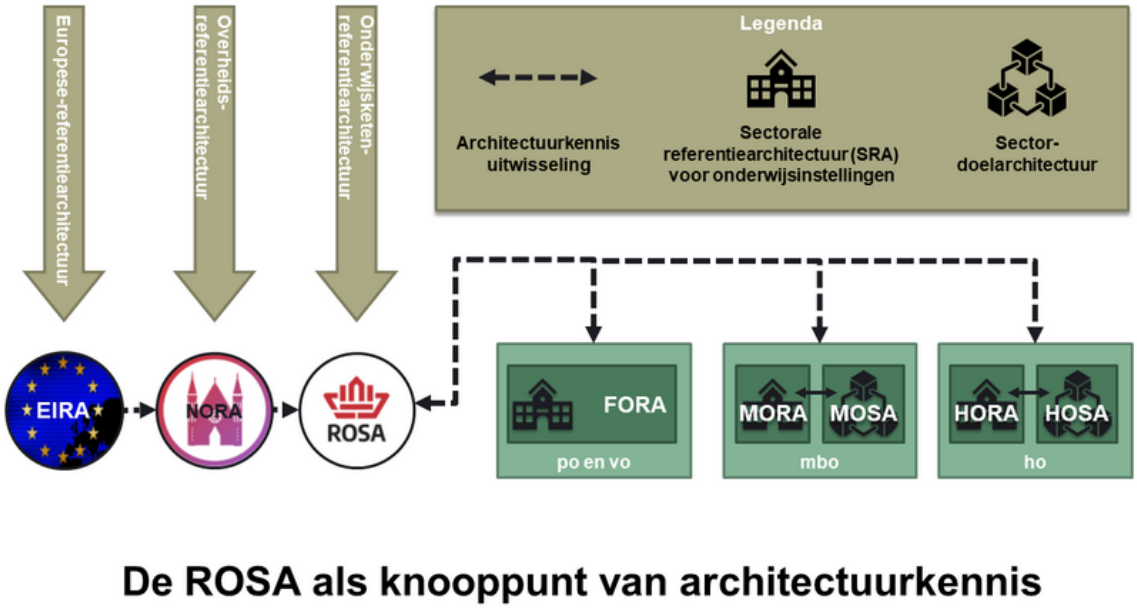
[5] AVG, Artikel 6.1 (https://www.privacy-regulation.eu/nl/artikel-6-rechtmatigheid-van-de-verwerking-EU-AVG.htm)

Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in dataregisters.

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 (zie Figuur 1). 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.
De Kempel conformeert zich aan de MORA (document G03 Architectuur), deze architectuur maakt gebruik van de ROSA als classificatie architectuur.



Figuur 1: Samenhang ROSA binnen de verschillende modellen

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.

Gezien de geopolitieke situatie hanteert De Kempel, bij gelijke geschiktheid, een beleid waarbij Europese leveranciers de voorkeur genieten.

Beveiligingsincidenten 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 de Helpdesk middels e-mail aan helpdesk@kempel.nl. Registratie vindt altijd plaats in Topdesk.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden. Beveiligingsincidenten met een grote impact zullen terstond worden besproken en opgepakt.
Studenten en externen kunnen kwetsbaarheden melden bij helpdesk@kempel.nl.

Planning en controle

Dit IBP-beleid wordt jaarlijks gereviewed en eventueel bijgesteld in opdracht van het bestuur. Het toezicht hierop berust bij de afdeling ICT. Hierbij wordt rekening gehouden met:

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

Daarnaast kent De Kempel een jaarlijkse verbeterplan voor privacy. Informatiebeveiliging wordt meegenomen in de kwartaalrapportages. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het IBP-beleid wordt opgenomen in de PDCA cyclus van De Kempel. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving etcetera meegenomen. Een en ander leidt tot een jaarlijkse roadmap.

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 De Kempel. Leidinggevenden en proceseigenaren zijn 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, etcetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het bestuur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.
Mocht de naleving van dit beleid ernstig tekortschieten, dan kan De Kempel de betrokken verantwoordelijke medewerker(s) een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

Logging en monitoring

Logging en monitoring door het team ICT zorgt ervoor 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 (zogenaamd SOC SIEM).

Governance

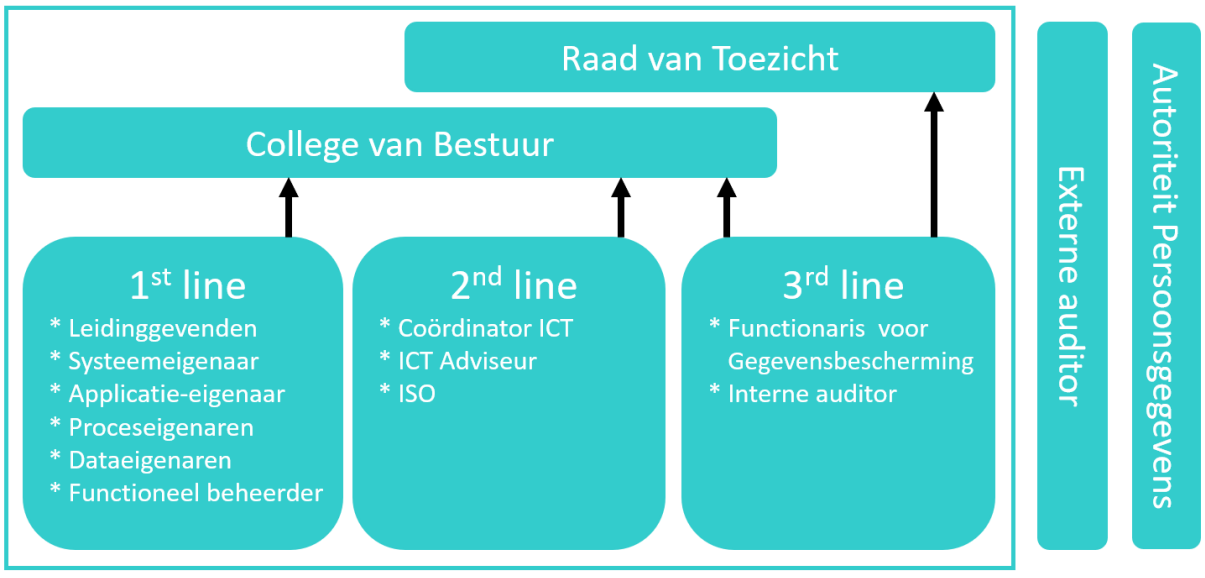
Rollen en verantwoordelijkheden

De Kempel hanteert het three lines model. De eerste lijn binnen dit model is cruciaal, immers de leidinggevenden moeten erop toezien dat het IBP beleid (InformatieBeveiliging en Privacy beleid) wordt nageleefd. Daartoe zijn alle managers geschoold en zij zien erop toe dat al hun teamleden handelen volgens het vastgesteld beleid. Schematisch als volgt weergegeven.

Het IBP-loket binnen de Kempel wordt gevormd door:

- Voorzitter CvB
- IT-manager
- IT-adviseur
- HRM adviseur
- Systeembeheerder
- Data Engineer
- Interne auditor
- Externe FG

Hogeschool de Kempel is een betrekkelijk kleine organisatie waardoor het lastig is een strikte scheiding aan te brengen tussen de drie lijnen. De IT manager is leidinggevende, systeemeigenaar en is daarnaast verantwoordelijk voor het IBP-loket (2de lijn). Om belangenverstrengeling (zoveel mogelijk) te voorkomen neemt de Information Security Officer (ISO) ook zitting in dit IPB-loket. Binnen de 3de lijn neemt de externe FG ook plaats in het IBP-loket. Naast de FG zit er Internal auditor in de derde lijn. Deze auditor zit niet in de andere lijnen waardoor het voorkomen van belangenverstrengeling is geborgd.



Toelichting: De 1e, 2e en 3e line moeten afzonderlijk van elkaar (op verzoek) verantwoording afleggen aan het CvB.

De first line of defense: Leidinggevenden, Systeemeigenaar, Applicatie eigenaar, Proceseigenaren en Dataeigenaar

Leidinggevenden (Cruciale rol 1e lijn)

De eerste lijn is verantwoordelijk voor de volgende onderwerpen:

1. Scholing leidinggevende (1e lijn).
2. Scholing medewerkers (inclusief awareness).
3. Naleving afspraken (voorkomen schaduwadministraties).
4. Registreren toegekende extra autorisaties.
5. Toezien op verwerkersovereenkomsten van decentrale applicaties die gebruikt worden binnen hun organisatorische eenheid.

De leidinggevende is verantwoordelijk voor de uitgifte van rollen en rechten van haar medewerkers. De leidinggevende dient periodiek (eens per zes maanden) te controleren of de uitgegeven rollen/rechten nog actueel zijn, de systeem-eigenaar faciliteert hiervoor een proces.
Leidinggevenden dragen verantwoordelijkheid voor het correct naleven van het privacybeleid binnen hun eigen lijnmanagement, oftewel in de processen waar zij eindverantwoordelijk voor zijn.

Systeemeigenaar

De systeemeigenaar is eigenaar van alle componenten in het ICT-netwerk. Het functioneel beheer en de scholing van de medewerkers in de applicaties valt niet onder de verantwoording van de systeemeigenaar. Het functioneel beheer valt onder de applicatie-eigenaar van de desbetreffende applicatie. De systeemeigenaar faciliteert het technische proces, maar is niet verantwoordelijk voor de inhoud of het beheer van een applicatie.

Applicatie-eigenaar

De applicatie-eigenaar is de eigenaar van de desbetreffende applicatie die hem/haar is toegewezen. De applicatie-eigenaar is verantwoordelijk voor:

1. Inrichten van de applicatie conform de eisen van het IBP-beleid;
2. Vaststellen van een autorisatiematrix en een passende toegangsverleningsprocedure;
3. In samenspraak met de proceseigenaar vaststellen van de rollen en rechten van medewerkers;
4. Toezien op leveranciersmanagement, waaronder het jaarlijks beoordelen van de verwerkersovereenkomst en beveiligingsaspecten, ondersteund door voorzitter CvB (vanuit de rol inkoop);
5. Periodiek laten uitvoeren van een data protection impact assessment (DPIA), indien dit noodzakelijk is conform wetgeving.

Proceseigenaren

De proceseigenaren worden door het College van Bestuur benoemd. De proceseigenaar zal in overleg met de applicatie-eigenaren[6] de processen inrichten, doorgaans met behulp van applicaties waarvan hij de functionaliteit mee heeft bepaald.
De proceseigenaar is daardoor ook verantwoordelijk voor bijvoorbeeld de inrichting van het systeem op basis van de principes uit dit beleid. Dit betekent bijvoorbeeld concreet dat de proceseigenaar verantwoordelijk is voor het vaststellen van rollen en rechten en de toetsing op need-to-know en dataminimalisatie binnen zijn proces en de bijbehorende applicaties.
De processen zoals opgenomen in de MORA zijn leidend.

Dataeigenaar

De 1e lijn eigenaar welke verantwoordelijke is voor alle data in de applicatie.

De functioneel beheerder (geen onderdeel van 1e lijn)

[6] Doorgaans is de applicatie eigenaar ook de proceseigenaar (HRM of financiën). Uitzondering is het Leerling informatiesysteem / Studenten informatiesysteem of Management Informatiesysteem.

Bundelt de rechten in een systeem tot een systeemrol en volgt procedures conform het inrichting- of beheerdocument voor die applicatie. De rechten op functionaliteiten en specifieke data worden vastgelegd in de autorisatiematrix en samenwerking met de applicatie-eigenaar. Op verzoek van leidinggevenden worden deze rollen aan specifieke medewerkers toegekend.
De functioneel beheerder van een applicatie zorgt voor actuele autorisatiematrix, waarin is opgenomen welke rollen en rechten er zijn binnen de desbetreffende applicatie.

Samenhang tussen de rollen binnen het IBP beleidsplan van het De Kempel.

Rol	Toewijzing	Invulling
Systeemeigenaar	IT-manager	Aanbesteding en kostenplaatseigenaar en contracteigenaar van systemen (hardware en applicaties)
Applicatie eigenaar	Data engineer HRM adviseur Coördinator Financiële administratie Systeembeheerder Manager Professionalisering	Applicaties
Proceseigenaar	Hoofden benoemd op basis van de MORA	Datamangement

De second line of defense: IT manager, ICT-adviseur en ISO

Experts op het gebied van informatiebeveiliging en privacybescherming werken samen binnen het IBP-loket (onderdeel 2de lijn). Het IBP-loket monitort de toepassing en naleving van het informatiebeveiligings- en privacybeleid, adviseert over informatiebeveiliging en privacybescherming en ondersteunt de leidinggevenden. Het IBP-loket ontwikkelt waar nodig beleid op het gebied van informatiebeveiliging en privacy, het College van Bestuur stelt dit voorgenomen beleid vast.
Het IBP-loket wordt aangestuurd door de IT manager. Hij geeft sturing aan de werkzaamheden van het IBP-loket. Het IBP-loket vormt de second line of defense als het gaat om de bescherming van persoonsgegevens.

De third line of defense: de Functionaris voor Gegevensbescherming en interne auditor

a) Functionaris voor gegevensbescherming

De Kempel heeft een externe toezichthouder op de verwerking van persoonsgegevens aangesteld. Deze toezichthouder wordt functionaris voor gegevensbescherming genoemd (hierna: “FG”). De FG zal door De Kempel 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 bij De Kempel. De Kempel 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 privacybeleid door De Kempel.
- Het toezien op een Privacy Impact Assessment.
- Het behandelen van klachten over de toepassing van het privacyreglement.
- Fungeren als eerste aanspreekpunt voor en samenwerken met de Autoriteit Persoonsgegevens.

b) de interne auditor

Externe controles worden uitgevoerd door onafhankelijke accountants. Deze worden voorbereid, gepland en geformuleerd door de interne auditor van De Kempel. Deze voert ook jaarlijkse interne audits.

Implementatie beleid

Het College van Bestuur van De Kempel is verantwoordelijk voor verwerkingen van persoonsgegevens waarvoor het doel en de middelen vaststelt. Het 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 De Kempel uitgevoerd. Het is niet één instituut of dienst die effectief verantwoordelijk kan zijn voor alle persoonsgegevens die De Kempel verwerkt. Er is een onderscheid tussen centrale verwerkingen, waarvoor de diensten verantwoordelijk zijn, en -aanvullend daarop- decentrale verwerkingen, waarvoor de opleidingen of individuele diensten zelf verantwoordelijk zijn.

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 ingevuld door de leidinggevenden uit onderwijs en bedrijfsvoering (Information Board).
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 IT manager en ICT-adviseur.
Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan. Het operationeel niveau wordt ingevuld door het management, ICT, HRM, financiën, administratie en facilitair.

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 De Kempel kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende scholingen voor medewerkers en bewustwordings-campagnes voor medewerkers, studenten en relaties. Deze campagnes sluiten bij voorkeur aan bij landelijke campagnes in het mbo/hoger onderwijs, zo mogelijk in afstemming met andere of integrale beveiligingscampagnes. Verhoging van het bewustzijn is de verantwoordelijkheid van elke leidinggevende en wordt gefaciliteerd door de ISO.

Controle en naleving

Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert gezamenlijk met de ISO en de interne auditor 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 de interne auditor van De Kempel, al dan niet mede gefinancierd en georganiseerd door SURF.

Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten De Kempel maken het noodzakelijk om periodiek te bezien of men nog voldoende op koers zit met het beleid.

Bijlage 1: Verklarende woordenlijst

AVG:	Algemene Verordening Gegevensbescherming.
Beleid:	Beleid met betrekking tot het verwerken van persoonsgegevens door De Kempel.
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 De Kempel. 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. De Kempel 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.
IBP-Beleid:	Informatie Beveleiging en Privacy Beleid.
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 De Kempel ingeschakelde (derde) partij die ten behoeve van De Kempel, 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 De Kempel dat het doel en de middelen van de verwerking van persoonsgegevens vaststelt.