

Informatiebeveiligings- en privacybeleid

Zadkine

Op basis van ISO 27001 en 27002 en alle van toepassing zijnde relevante wet- en regelgeving



Versiebeheer

Versie	Status	Datum	Auteur(s)	Omschrijving
1.5	Concept	3-3-2020	Martijn Bijleveld, Richard de Koning	Ter beoordeling voorgelegd aan FG
			Marieke Lunter	Review door Audit & Control
1.9	Concept	7-4-2020	Richard de Koning	Besproken in FG-CvB overleg, ter vaststelling naar CvB
1.99	Finaal Concept	9-4-2020	Richard de Koning	Verduidelijkingen n.a.v. review Audit & Control
2.0	Definitief	21-4-2020	Richard de Koning	Vastgesteld door College van Bestuur

Vastgesteld

Versie	Datum	Naam	Functie
2.0	17-4-2020	Philippe Raets	Voorzitter College van Bestuur Zadkine

INFORMATIEBEVEILIGINGS- EN PRIVACYBELEID ZADKINE	1
1 VERANTWOORDING EN RICHTLIJNEN	3
1.1 HET BELANG VAN INFORMATIEBEVEILIGING EN PRIVACY.....	3
1.2 TOELICHTING INFORMATIEBEVEILIGING	3
1.3 TOELICHTING PRIVACY	3
1.4 VERVLECHTING INFORMATIEBEVEILIGING EN PRIVACY	3
1.5 DOEL	3
1.6 REIKWIJDTE.....	4
1.7 CONCRETISERING	4
2 COMPLIANCE	6
2.1 RELEVANTE WET- EN REGELGEVING	6
2.2 BASISREGELS BIJ HET OMGAAN MET PERSOONSGEGEVENS.....	6
2.3 ONDERSTEUNENDE RICHTLIJNEN EN PROCEDURES	6
2.4 VOORLICHTING EN BEWUSTZIJN.....	6
2.5 CLASSIFICATIE EN RISICOANALYSE.....	7
2.6 INCIDENTEN EN DATALEKKEN	7
2.7 PLANNING EN CONTROLE	7
2.8 NALEVING EN SANCTIES	7
2.9 LOGGING EN MONITORING	7
3 GOVERNANCE.....	8
3.1 ROLLEN EN VERANTWOORDELIJKHEDEN	8
3.2 DE FIRST LINE OF DEFENSE: DIRECTEUR, TEAMLEIDER, IM, INKOOP, FB EN ICT	8
3.3 DE SECOND LINE OF DEFENSE: DE IVP-ORGANISATIE VAN ZADKINE	9
3.4 DE THIRD LINE OF DEFENSE: DE FG EN DE (INTERNE) AUDITFUNCTIE.....	9
3.5 DE TAKEN VAN DE MEDEWERKERS.....	10
3.6 IMPLEMENTATIE BELEID	11
3.7 VERDELING VAN DE VERANTWOORDELIJKHEDEN	11
3.8 INPASSING IN DE GOVERNANCE EN AFSTEMMING MET AANPALENDE BELEIDSTERREINEN.....	11
3.9 BEWUSTWORDING EN TRAINING.....	11
3.10 CONTROLE EN NALEVING.....	12
BIJLAGE 1: ONDERSTEUNENDE DOCUMENTEN EN RICHTLIJNEN.....	13
A. RICHTLIJNEN INFORMATIEBEVEILIGING	14
B. RICHTLIJNEN PRIVACY	17

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. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging / informatieveiligheid en privacy (afgekort tot IBP/IVP) in een IBP/IVP-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 Zadkine. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imago-verlies.

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.

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 proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis op informatiebeveiliging en privacy binnen Zadkine 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 de dienstverlening van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen van wie Zadkine 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. medewerkers, studenten en hun ouders/verzorgers) wordt gerespecteerd en Zadkine voldoet aan relevante wet- en regelgeving.

1.6 Reikwijdte

- Het IBP-beleid binnen de MBO Raad 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 Zadkine. 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 sociale media). Onder dit beleid vallen ook alle devices (mobiele telefoon, laptop, tablet, etc.) 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 MBO Raad 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 Zadkine 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

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

1. Het College van Bestuur van Zadkine 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 verwerkingsverantwoordelijke¹.
2. Zadkine voldoet aan alle relevante wet- en regelgeving.
3. Bij Zadkine 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 Zadkine 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 herzien.
4. Zadkine zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.
5. Zadkine legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Zadkine voldoet hiermee aan de documentatieplicht.
6. Binnen Zadkine 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

¹ De verwerkingsverantwoordelijke bepaalt de doeleinden waarvoor en de middelen waarmee persoonsgegevens worden verwerkt.

de daarin opgeslagen informatie, maar ook van papieren documenten.

7. Zadkine is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert Zadkine informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en studenten worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
8. Zadkine 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. Zadkine sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken.
10. Zadkine verwacht van alle medewerkers, studenten, (geregistreeerde) 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 imagooverlies. Zadkine heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
11. Informatiebeveiliging en privacy is bij Zadkine een continu kwaliteitsproces, waarbij regelmatig (minimaal jaarlijks) wordt beoordeeld (via audit en/of self assessment met peer review) of aanpassing gewenst is.
12. Zadkine kijkt bij wijzigingen 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. Zadkine neemt passende organisatorische en/of technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs en de bedrijfsvoering of de bescherming van de privacy van betrokkenen kunnen verstoren.
14. Zadkine zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en zo nodig melden bij de Autoriteit Persoonsgegevens en zo nodig aan de betrokkenen.
15. Zadkine kiest ten aanzien van informatiebeveiliging (autorisatie en authenticatie) voor de vooronderstelling "Alles is in principe verboden tenzij het uitdrukkelijk is toegelaten" in plaats van het zwakkere uitgangspunt "Alles is in principe toegelaten tenzij het uitdrukkelijk is verboden".

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
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Auteurswet
- Wetboek van Strafrecht
- Koppelingswet

Het internationale normenkader voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2017) is leidend voor de te nemen beveiligingsmaatregelen. Zadkine hanteert het Toetsingskader² Informatiebeveiliging en Privacy dat ontwikkeld is door saMBO-ICT en Kennisnet onder verantwoordelijkheid van de regiegroep IBP in het mbo.

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 beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

2.4 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt

² Zie www.sambo-ict.nl/ibpdoc40

aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP-manager, de FG, en/of de Security- en Privacy Officer(s) met het College van Bestuur als eindverantwoordelijke.

2.5 Classificatie en risicoanalyse

Alle gegevens en informatiesystemen waarop dit beleid van toepassing is worden geclassificeerd. 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. Hiervoor worden DPIA's uitgevoerd (Data Protection Impact Assessment; gegevensbeschermingseffectbeoordeling). Vanaf de start van nieuwe (ICT)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

2.6 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 een door Zadkine bepaald contactpunt: de Servicedesk (IVP)

Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

Ook aan studenten en externen is gecommuniceerd op welke manier zij kwetsbaarheden en incidenten dienen te melden.

2.7 Planning en controle

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

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

Daarnaast kent Zadkine een jaarlijks 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. Eén en ander leidt tot een jaarplan IBP.

2.8 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 onze instelling. Daarboven nemen de leidinggevend en proceseigenaren hun verantwoordelijkheid om hun medewerkers aan te spreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP-zaken 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 het College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan de school de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

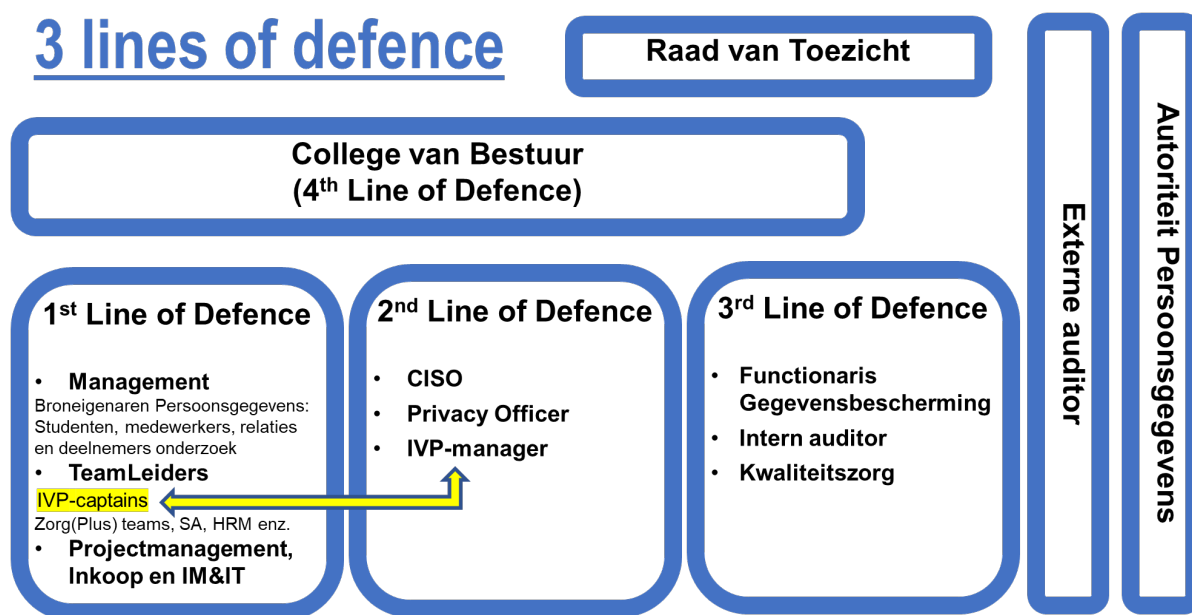
2.9 Logging en monitoring

Door middel van logging en monitoring worden gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (pogingen tot) ongeautoriseerde toegang tot het netwerk. Zadkine beoordeelt deze logbestanden met regelmaat.

3 Governance

3.1 Rollen en verantwoordelijkheden

Zadkine hanteert het three lines of defence model, waarbij het als vierde lijn het College van Bestuur is toegevoegd. De eerste lijn binnen dit model is cruciaal, immers de managers moeten er op toezien dat de AVG wordt nageleefd. Daartoe zijn alle managers geschoold en zij zien erop toe dat al hun teamleden handelen volgens het vastgesteld IBP beleid. Schematisch als volgt weergegeven.



IM-IT: Informatiemanager, applicatiebeheerders, functioneel beheerders en technisch beheerders.

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

De eerste lijn bewaakt het privacybeleid binnen het eigen organisatorische onderdeel. Zij vormen de first line of defense als het gaat om de bescherming van persoonsgegevens en voeren de daarbij horende operationele taken uit, zoals:

- erop toezien dat de gegevensverwerkingen in lijn zijn met het betreffende dataregister
- toetsen dat er geen gegevens door externe verwerkers worden verwerkt of aan externe partijen worden overgedragen zonder een wettelijke grondslag dan wel een geldige overeenkomst (Verwerkersovereenkomst of een Gezamenlijk Verantwoordelijksovereenkomst),
- beoordelen van incidenten rond persoonsgegevens en de interne melding daarvan als het vermoeden bestaat dat het gaat om een datalek,
- toezien dat de medewerkers voldoende geschoold zijn in het kader van de AVG,
- definiëren van de (extra) taken en rollen van medewerkers en de daarbij behorende rechten binnen de bijbehorende systemen/processen (autorisatiematrix).

3.3 De second line of defense: de IVP-organisatie van Zadkine

Experts op het gebied van informatieveiligheid en privacybescherming monitoren de toepassing en naleving van het informatieveiligheids- en privacybeleid. Zij adviseren, gevraagd en ongevraagd, over informatiebeveiliging en privacybescherming en ondersteunen de first line, bijvoorbeeld bij het afsluiten van overeenkomsten met derde partijen. De IVP-organisatie ontwikkelt waar nodig beleid op het gebied van informatieveiligheid en privacy, het College van Bestuur stelt dit voorgenomen beleid vast. De medewerkers van de IVP-organisatie vormen daarmee de second line of defense als het gaat om de bescherming van persoonsgegevens.

3.4 De third line of defense: de FG en de (interne) auditfunctie

a) de Functionaris voor gegevensbescherming

Zadkine heeft een interne toezichthouder op de verwerking van persoonsgegevens aangesteld: de functionaris voor de gegevensbescherming (hierna: "FG"). De FG zal door Zadkine tijdig worden betrokken bij alle aangelegenheden waar persoonsgegevens in het geding zijn. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie binnen Zadkine. Zadkine heeft de FG aangemeld bij de nationale toezichthoudende autoriteit, de 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 privacy beleid door Zadkine,
- het toezien op de inzet en uitvoering van Data Protection Impact Assessments (DPIA's),
- het behandelen van klachten over de toepassing van het privacyreglement,
- fungeren als eerste aanspreekpunt voor en samenwerken met de Autoriteit Persoonsgegevens.

b) (Interne) audit

Op basis van het Toetsingskader IB (en daarmee de ISO27001 norm), aangevuld met de plusclusters 7 (privacy) en 8 (examenring), vindt minimaal jaarlijks een interne beoordeling plaats door middel van een self-assessment, peer-review en/of interne audit. Ook kunnen externe controles worden uitgevoerd door onafhankelijke accountants.

3.5 De taken van de medewerkers

Onderwerp	1 st line of defence	2 nd line of defence	3 rd line of defence
Autorisaties	Management brengt autorisaties in kaart (SOLL) en toetst dit bij de Functioneel beheerders (IST).	IVP-team controleert of het SOLL en IST autorisatie vergelijk is uitgevoerd.	De FG controleert of de autorisaties zijn ingericht op basis van <i>need-to-know</i> en <i>least privilege</i> .
Beleidsdocumenten	Management ziet er op toe dat de goedgekeurde kaders en richtlijnen uit de beleidsdocumenten worden uitgevoerd.	IBP-team schrijft en evalueert de beleidsdocumenten en bespreekt deze met alle stakeholders en de FG'er en dient ze in bij het CvB ter goedkeuring.	De FG toetst de kwaliteit van het beleid en de werking van het door het CvB goedgekeurde beleid.
Bewaartermijn	Directeur, teamleider en FB zijn verantwoordelijk voor het handhaven van de bewaartermijnen conform het Documentair StructuurPlan (DSP).	IBP-team adviseert aan de hand van de het Documentair Structuurplan over de geldende bewaartermijnen.	De FG ziet er op toe dat de bewaartermijnen worden nageleefd.
Bewustwording	Management voert het opleidingsplan van het IBP-team uit of stelt een afgeleid opleidingsplan vast.	IBP-team stelt een opleidingsplan op voor IBP-scholings- en awareness plannen en faciliteert ook centrale trainingen.	De FG toetst het gewenste kennisniveau aan de scholings- en awareness plannen en komt zo nodig met aanbevelingen.
DPIA's	- Management en projectleiders voeren een pré DPIA uit bij ieder nieuwe IV project. - Management en projectleider voert een DPIA uit in opdracht van de FG.	IBP-team komt op basis van de pré DPIA, uitgevoerd door de 1 st line, tot een voorstel om al dan niet een DPIA uit te voeren en wordt betrokken bij de uitvoering van de DPIA.	De FG besluit op basis van het voorstel van het IBP-team of er een DPIA moet worden uitgevoerd en adviseert gevraagd of ongegevraagd over de DPIA. De DPIA wordt vastgesteld na goedkeuring van de FG.
Datalekken	Medewerkers melden zelf intern een datalek via een registratiesysteem. Het management draagt zorg voor bekendheid van de meldprocedure en scholing van haar medewerkers.	De FG informeert de IBP-organisatie over de gemelde datalekken.	De FG besluit, na overleg met het CvB, om al dan niet het datalek bij de AP en/of de betrokkenen te melden.
Dataregisters centraal	De aangewezen verantwoordelijke directeuren (broneigenaren) bewaken de actualiteit van het dataregister.	Het IBP-team adviseert en controleert op volledigheid, juistheid en actualiteit van de Dataregisters.	De FG toetst of het dataregister voldoet aan wet- en regelgeving.
Door het management aangewezen uitvoerders	Het management wijst de deelprocesuitvoerders aan (bijv. examinering, roostering, stage, etc.).	Het IVP-team toetst het toegewezen eigenaarschap aan de autorisatie.	De FG toetst of het eigenaarschap beschreven is.
Rechten van de betrokkenen	Het servicepunt van de locatie (studenten) of hrm (mw) voert id-controle uit en maakt aanvraag aan t.b.v. het IVP-team.	IVP-team registreert de aanvragen en handelt af.	IVP-manager rapporteert aanvragen aan FG / CvB. FG toetst aard van de verzoeken en de kwaliteit van afhandeling.
Verwerkersovereenkomsten	De betrokken proces/systeemeigenaar zorgt dat er altijd een verwerkersovereenkomst is opgesteld en kan het IBP-team hiervoor advies vragen.	Het IBP-team adviseert bij verwerkersovereenkomsten op verzoek van de proces/systeemeigenaar.	De FG toetst de verwerkersovereenkomst op rechtmatigheid en volledigheid. Het College van Bestuur tekent na akkoord van de FG.
Vragen van medewerkers betreffende IBP gerelateerde onderwerpen	Management is het eerste aanspreekpunt voor vragen inzake privacy en security, medewerkers kunnen het IBP-team ook zelf benaderen	IBP-team adviseert de manager en/of medewerker.	De FG controleert de gestelde vragen en de oplossingen.

3.6 Implementatie beleid

Het College van Bestuur is verantwoordelijk voor verwerkingen van persoonsgegevens waarvoor het doel en de middelen vaststelt. Het wordt aangemerkt als de verwerkingsverantwoordelijke in de zin van de AVG. Die 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.

3.7 Verdeling van de verantwoordelijkheden

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

- De studentenadministratie (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle onderwijsdeelnemers van Zadkine. De studentenadministratie is verantwoordelijk voor het Dataregister met studentgegevens,
- De personeelsadministratie (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle personen die in opdracht van Zadkine, zowel centraal als decentraal, werk verrichten. De personeelsadministratie is verantwoordelijk voor het Dataregister van medewerkers,
- De dienst Marketing en Communicatie (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle mensen waarmee Zadkine centraal een relatie onderhoudt, zoals belangstellenden, sollicitanten, oud-werknemers, contactpersonen van de stage verlenende organisaties en leveranciers, projects en alumni. Deze dienst is verantwoordelijk voor het Dataregister van deze relaties,
- De opdrachtgever van onderzoek (broneigenaar) dat Zadkine 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 IBP-organisatie en getoetst door de FG.

Er worden geen persoonsgegevens verwerkt buiten de verantwoordelijkheid van een van bovengenoemde broneigenaren, tenzij dit met toestemming van de FG gebeurt. De FG bepaalt op welke manier deze verwerkingen worden gedocumenteerd.

3.8 Inpassing in de governance 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 informatiebeveiliging en 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 IBP-organisatie.

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan. Het operationeel niveau wordt ingevuld door diverse rollen: directeur, teamleider, IM, Inkoop, FB 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 onze instelling de bewustwording van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn trainingen voor medewerkers en regelmatig terugkerende bewustwordingscampagnes gericht op medewerkers, studenten en relaties. Verhoging van het bewustzijn is de verantwoordelijkheid van elke leidinggevende en wordt gefaciliteerd door het de IBP-organisatie.

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 de interne auditfunctie 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 auditfunctie van Zadkine.

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

Bijlage 1: Ondersteunende documenten en richtlijnen

Met betrekking tot de volgende onderwerpen wordt aanbevolen om volgens een vastgestelde richtlijn te werken. De onderwerpen voor deze richtlijnen zijn gegroepeerd op de categorieën informatiebeveiliging en privacy. De instelling moet de richtlijn zelf meer gedetailleerd uitwerken en vaststellen. Vervolgens kan de richtlijn als bewijslast. Veel richtlijnen worden ondersteund met handreikingen en formats in het Framework IBP in het mbo, versie 2.0 (de IBPDOC's)

Informatiebeveiliging

- Classificatiemodel
- Bewaartermijnen
- Lidmaatschap ibp-netwerken
- Intellectuele eigendomsrechten
- Clear Desk, clear screen
- Responsible disclosure beleid (IBPDOC27)
- Acceptable use policy (IBPDOC26) – (evidence: gebruik network)
- Mobiele apparatuur
- Thuiswerken
- Back-up van informatie
- Registratie beveiligingsincidenten
- Calamiteitenplan ICT
- Wachtwoordbeleid (evidence: ww-beleid)
- Toegangsbeveiliging
- Logging (Evidence: logs ICT)

Privacy

- Procedure toestemming gebruik beeldmateriaal (toestemmingsverklaring)
- Procedure voor verwijderen van gegevens (bewaartermijnen)
- Communicatie rechten betrokkenen
- Privacyreglementen
- Procesbeschrijving melden datalekken
- Dataregisters
- Verwerkersovereenkomsten
- Procedure Gegevensbeschermingseffectbeoordeling (DPIA)

A. Richtlijnen informatiebeveiliging

Classificatiemodel

1.7	8.2.1	Classificatie van informatie
-----	-------	------------------------------

Richtlijn: informatie dient te worden geclassificeerd, waarbij gebruikgemaakt wordt van een vastgesteld classificeringsschema (bijvoorbeeld het ROSA-classificatiemodel).

Evidence: dataregisters, verwerkersovereenkomsten

Bewaartermijnen

1.19	18.1.3	Beschermen van registraties
------	--------	-----------------------------

Richtlijn: bij de registratie van gegevens wordt rekening gehouden met de classificatie ervan en wordt rekening gehouden met de minimale en maximale bewaartermijnen (bijvoorbeeld volgens het Documentair Structuur Plan van de MBO Raad).

evidence: dataregisters, verwerkersovereenkomsten

Lidmaatschap ibp netwerken

1.23	6.1.4	NIEUW: Contact met speciale belangengroepen
------	-------	---

Richtlijn: om te borgen dat de kennis van informatiebeveiliging actueel en volledig is de instelling actief betrokken bij saMBO-ICT (met name het Netwerk IBP), SCIPR en SCIRT.

Evidence: lidmaatschap medewerkers IVP-organisatie van o.a. SCIPR en SCIRT; aantoonbaar bijgewoonde bijeenkomsten van o.a. saMBO-ICT, SURF

Intellectuele eigendomsrechten

1.26	18.1.2	NIEUW: Intellectuele eigendomsrechten
------	--------	---------------------------------------

Richtlijn: gebruikte software wordt via een formeel proces geregistreerd en beheerd.

Evidence: contract- en licentiebeheer CMDB

Clear desk, clear screen

2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid
-----	--------	--

Richtlijn: er is clear-desk en clear-screen beleid vastgesteld dat wordt ondersteund door awareness activiteiten.

Evidence: Reglement Verantwoord Netwerkgebruik (IBPDO26) artikel 2.1; aantoonbaar door awareness-campagnes

Responsible disclosure

2.6	16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging
-----	--------	---

Richtlijn: in- en externe medewerkers zijn verplicht zwakke plekken binnen de informatiebeveiliging en privacy te melden (mogelijk als onderdeel van reglement netwerkgebruik in-/externe medewerkers), zie ook Responsible Disclosure; IBPDO27

Evidence: Reglement Verantwoord Netwerkgebruik (IBPDO26) artikel 2.4

Acceptable use policy

3.18	8.1.3	NIEUW: Aanvaardbaar gebruik van bedrijfsmiddelen
3.20	8.3.1	NIEUW: Beheer van verwijderbare media

Richtlijn: in- en externe medewerkers worden gewezen op hun verantwoordelijkheid voor het zorgvuldig omgaan met de aan hen beschikbaar gestelde faciliteiten en de toegang tot informatie (mogelijk als onderdeel van reglement netwerkgebruik in-/externe medewerkers), zie ook Verantwoord Netwerkgebruik, IBPDO26

Evidence: Reglement Verantwoord Netwerkgebruik (IBPDO26)

Mobiele apparatuur

1.6	6.2.1	Beleid voor mobiele apparatuur
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen
1.27	18.1.5	NIEUW: Voorschriften voor het gebruik van cryptografische beheersmaatregelen
5.10	10.1.2	Sleutelbeheer

Richtlijn: bij de configuratie van mobiele apparatuur wordt rekening gehouden met kwetsbaarheden als gevolg van het werken buiten de organisatie (bijvoorbeeld door encryptie / VPN-client) en er is een reglement voor het gebruik van mobiele apparatuur.

Thuiswerken.

2.8	6.2.2	NIEUW: Telewerken (thuiswerken)
-----	-------	---------------------------------

Richtlijn: er zijn voorwaarden vastgesteld waaronder medewerkers mogen thuiswerken (werkzaamheden die verder gaan dan het verwerken van e-mail, bijvoorbeeld m.b.t. een medewerker salarisadministratie).

Back-up van informatie

4.5	12.3.1	Back-up van informatie
-----	--------	------------------------

Richtlijn: er is een back-up-procedure vastgesteld waarbij voor de bedrijfskritische applicaties de belangrijkste eisen zijn vastgelegd (bijv. frequentie, bewaarlocatie, testprocedures).

Evidence: back-up plan ProAct Backup-as-a-Service (BAAS)

Registratie beveiligingsincidenten

4.12	16.1.4	Beeoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen
4.13	16.1.5	Respons op informatiebeveiligingsincidenten

Richtlijn: informatiebeveiligingsgebeurtenissen worden geregistreerd en er vindt een beoordeling plaats of deze moeten worden geclassificeerd als informatiebeveiligingsincidenten. Op beveiligingsincidenten wordt adequaat gereageerd, volgens vastgestelde procedures.

Evidence: IVP-meldingenregister

Calamiteitenplan ICT

4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren
4.18	17.1.1	NIEUW: Informatiebeveiligingscontinuïteit plannen
4.19	17.1.3	NIEUW: Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren

Richtlijn: er is een calamiteitenplan voor de informatiebeveiliging (suggestie: zoek aansluiting bij algemeen calamiteitenplan).

Evidence: Disaster Recovery, OZON, Algemeen Crisisplan

Toegangsbeveiliging/wachtwoordbeleid

2.3	9.2.6	Toegangsrechten intrekken of aanpassen
5.1	9.1.1	Beleid voor toegangsbeveiliging
5.2	9.1.2	Toegang tot netwerken en netwerkdiensten
5.3	9.2.1	Registratie en afmelden van gebruikers
5.4	9.2.2	Gebruikers toegang verlenen
5.5	9.2.3	Beheren van speciale toegangsrechten
5.6	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers
5.7	9.3.1	Geheime authenticatie-informatie gebruiken
5.8	9.4.1	Beperking toegang tot informatie
5.9	9.4.2	Beveiligde inlogprocedures
5.18	9.4.3	NIEUW: Systeem voor wachtwoordbeheer
5.19	9.4.4	NIEUW: Speciale systeemhulpmiddelen gebruiken
5.20	9.4.5	NIEUW: Toegangsbeveiliging op programmabroncode
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers

Richtlijn: pas het beleid zoals beschreven in het document *Model Autorisatie- en authenticatiebeleid* (IBDOC37) toe, met betrekking tot de statements toegangsbeveiliging en wachtwoordbeleid.

Evidence: Wachtwoordbeleid en autorisatiematrixen

Logging

6.2	12.4.1	Gebeurtenissen registreren
6.3	12.4.3	Logbestanden van beheerders en operators

Richtlijn: registreer relevante gebruikersactiviteiten en gebeurtenissen en wees transparant welke applicaties en medewerkers/rollen worden gelogd en wie toegang heeft tot deze logbestanden.

Evidence: log-bestanden IM-IT; verwerkersovereenkomsten externe verwerkers

B. Richtlijnen Privacy

Procedure toestemming gebruik beeldmateriaal

P3	Rechtmatige verwerking van persoonsgegevens
-----------	--

Document: Procedure toestemming gebruik beeldmateriaal (toestemmingsverklaring). Zie <https://aanpakibp.kennisnet.nl/toestemming/>

Evidence: toestemmingsverklaringen M&C

Dataregisters

P4	Register van verwerkingsactiviteiten (dataregister)
-----------	--

Document: Dataregisters, IBPDO20, IBPDO20-1 t/m IBPDO20-5

Evidence: dataregisters

Procedure voor verwijderen van gegevens

P5	Bewaartermijnen
-----------	------------------------

Document: Procedure voor verwijderen van gegevens (bijv. op basis van Documentair Structuur Plan MBO Raad).

Evidence: Dataregisters, verwerkersovereenkomsten

Verwerkersovereenkomsten

P10	Verwerkersovereenkomsten
------------	---------------------------------

Document: Generiek model verwerkersovereenkomst (IBPDO18) of het Privacyconvenant Onderwijs, Model-overeenkomst 3.0

Evidence: Dataregisters, verwerkersovereenkomsten

Privacyreglementen

P11	Transparantie privacy beleid
------------	-------------------------------------

P12	Informatieplicht verwerkingen
------------	--------------------------------------

Document: Model Privacyreglement Studenten (IBPDO35) en het Model Privacyreglement Medewerkers (IBPDO36)

Evidence: privacyreglement en -statements

Communicatie rechten betrokkenen

P13	Rechten van betrokkenen
------------	--------------------------------

Document: Privacy voor studenten in het mbo, rechten betrokkenen (IBPDO33)

Evidence: privacyreglement en -statements;
procesbeschrijving servicepunt (studenten) of hrm (medewerker) > IVP-organisatie

Procedure melden datalekken

P18	Datalekken en beveiligingsincidenten
------------	---

Document: Handreiking informatiebeveiligingsincidenten en datalekken (IBPDO39) >> nog te maken <<

Evidence: Servicedesk-portaal en IVP-website

Procedure Gegevensbeschermingseffectbeoordeling (DPIA)

P21	Data Protection Impact Assessment (DPIA)
------------	---

Document: Handreiking DPIA (IBPDO38) >> nog te maken <<

Evidence: (modellen) DPIA's, uitgevoerde DPIA's