Informatiebeveiligings- en privacy beleid

Bron
Kennisnet

Bewerkt door:
KPO Roosendaal, Leon van Iersel

Versie	Datum	Auteur	Omschrijving
2.0	25-05-2018	Leon van Iersel	Kennisnet versie aangepast voor KPO Roosendaal.
2.1	5-10-2018	Leon van Iersel	Aangepast n.a.v. opmerkingen GMR
2.2	31-3-2021	Leon van Iersel	Toevoeging bedrijfsmiddelenbeleid en aanscherping audits

Vastgesteld door KPO Roosendaal:

Versie	Datum	Naam	Functie
2.0	25-05-2018	Kees Mens	College van Bestuur
2.1	5-10-2018	Kees Mens	College van Bestuur
2.2	21-6-2021	Kees Mens	College van Bestuur

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. 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.

2. Toelichting informatiebeveiliging en privacy

2.1 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 juist en volledig 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 en imagoverlies.

2.2 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.

2.3 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 om informatiebeveiliging en privacy binnen KPO Roosendaal te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3. Doel en reikwijdte

3.1 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 waarvan KPO Roosendaal persoonsgegevens verwerkt, waaronder leerlingen, 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, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en KPO Roosendaal voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen KPO Roosendaal geldt voor alle medewerkers, stagiaires, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.

- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen KPO Roosendaal waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan KPO Roosendaal persoonsgegevens verwerkt.

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van KPO Roosendaal. 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 leerlingen in discussies op (persoonlijke pagina's van) websites en of social media.). Zie protocol internet en sociale media op school.

- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van KPO Roosendaal 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.

4. Beleid – Hoe doen we dat?

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

1. Het schoolbestuur van KPO Roosendaal 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. KPO Roosendaal voldoet aan alle relevante wet- en regelgeving.
3. Bij KPO Roosendaal 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 KPO Roosendaal 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 te allen tijde hun toestemming herzien.
4. KPO Roosendaal 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, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering. Dit zoals vastgesteld in het privacyreglement en dataregister.
5. KPO Roosendaal legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. KPO Roosendaal voldoet hiermee aan de documentatieplicht. Het dataregister bevat alle persoonsgegevens met de daaraan gekoppelde autorisaties en eventuele externe verwerkers van deze gegevens.
6. Binnen KPO Roosendaal is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.
7. KPO Roosendaal 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 leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
8. KPO Roosendaal classificeert informatie en informatiesystemen volgens het dataregister. 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. KPO Roosendaal sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.
10. KPO Roosendaal verwacht van alle medewerkers, leerlingen, (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. KPO Roosendaal heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd in het protocol internet en sociale media op school.
11. Informatiebeveiliging en privacy is bij KPO Roosendaal een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst en/of noodzakelijk is.
12. KPO Roosendaal 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. KPO Roosendaal neemt passende 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.

Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt KPO Roosendaal aanvullende afspraken over de technische maatregelen vast in een verwerkersovereenkomst.

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

5. Uitwerking van het beleid – Wat doen we?

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

5.1 Relevante wet- en regelgeving

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

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)*
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

5.2 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. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

2. **Grondslag**: vewerking van persoonsgegevens is gebaseerd op één van de zes wettelijke grondslagen (toestemming betrokken persoon, noodzakelijk voor uitvoering van een overeenkomst, noodzakelijk voor het nakomen van een wettelijke verplichting, noodzakelijk ter bescherming van de vitale belangen, noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag of noodzakelijk voor de behartiging van de gerechtvaardigde belangen), als omschreven in de AVG en toegelicht in het dataregister.

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 (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens middels het dataregister, alsmede over het gevoerde IBP-beleid. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming 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 juist en actueel zijn zoals vastgesteld in het dataregister.

5.3 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.

5.4 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 aangemoedigd. Zowel in het directieberaad als op de teamvergaderingen van de scholen is informatiebeveiliging en privacy een vast agendapunt en worden medewerkers actief hierbij betrokken. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de FG en de schooldirectie met het College van Bestuur als eindverantwoordelijke.

5.5 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, 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 betrouwbaarheidsaspecten 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. Vanaf de start van nieuwe (ICT)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

5.6 DPIA testen en controle

KPO Roosendaal is lid van SIVON en volgt kritisch de resultaten van de door SIVON uitgevoerde DPIA (Data Protection Impact Assessment) testen op de door KPO Roosendaal gebruikte software (Microsoft, Google, ESIS) waarin persoonsgegevens verwerkt worden.
(Zie https://www.sivon.nl/actueel/dpia-leerlingadministratiesystemen-gestart/)

Van het personeelsadministratiesysteem (AFAS) en het ouderportaal (Social Schools) worden jaarlijks de testrapporten opgevraagd en kritisch beoordeeld. Het verslag hiervan wordt vastgelegd. Daarnaast wordt om toerbeurt van één uitgeverij dit proces doorlopen.

5.7 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 privacy@kporoosendaal.nl.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.8 Planning en controle

Dit IBP-beleid wordt jaarlijks getoetst en 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

KPO Roosendaal wijzigt de noodzakelijke stukken m.b.t. IBP ook op basis van eventuele aangepaste wet- en regelgeving.

5.9 Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode en tijdens de teamvergaderingen.

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 KPO Roosendaal de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

6. Organisatie - Wie doet wat?

6.1 Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij KPO Roosendaal.
IBP is op drie niveaus georganiseerd

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij KPO Roosendaal voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

6.2 Richtinggevend

Eindverantwoordelijke
Het College van Bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.

6.3 Sturend

Functionaris voor Gegevensbescherming (FG)
De functionaris voor gegevensbescherming (FG) houdt binnen KPO Roosendaal toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het verbeteren en stimuleren van bewustwording rondom IBP, het afhandelen van informatiebeveiligingsincidenten, adviseert over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (het College van Bestuur). Daarnaast kan de FG ook direct contact leggen met de Raad van Toezicht indien de situatie daarom vraagt. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.
De FG geeft terugkoppeling en advies aan de eindverantwoordelijke (het College van Bestuur) en stuurt de mensen aan op uitvoerend niveau. De FG moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen KPO Roosendaal
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen KPO Roosendaal coördineren

MT verantwoordelijkheid
Binnen KPO Roosendaal zijn er verschillende beleidsterreinen, zoals Onderwijs, ICT, Personeel (HRM, P&O), Vastgoed & Facilitaire zaken en Financiën. Op elk van deze terreinen is een MT-lid verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Deze MT-leden zijn tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben zij de volgende specifieke taken:

- Samen met de eindverantwoordelijke stellen zij het beleid voor toegang (autorisaties) vast.
- Samen met ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

6.4 Uitvoerend

Functionaris voor Gegevensbescherming
De functionaris voor gegevensbescherming vormt een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Medewerkers worden in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.
Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR)

Leidinggevenden en schooldirecties
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het IBP-beleid;
- toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de functionaris voor gegevensbescherming. Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

Documenten:	Aandachtspunten:
Procedure toestemming gebruik beeldmateriaal	(toestemmingsbrief)
Procedure voor verwijderen van gegevens	(bewaartermijnen)
Privacyreglement	
Protocol internet en sociale media	
Gedragscode bedrijfsmiddelen	

Verplicht vanuit de AVG:

Protocol informatiebeveiligingsincidenten en datalekken
Registratie beveiligingsincidenten
Dataregister om te voldoen aan de registratieplicht
Verwerkersovereenkomsten
Procedure gegevensbeschermingseffectbeoordeling
Risicoanalyse
Functionaris voor Gegevensbescherming