Christelijke Onderwijs Groep
Vallei & Gelderland - Midden

Leerpark Presikhaaf · Thomas a Kempis · Titus Brandsma · Arentheem College
Het Perron · UPGRADE · Knooppunt techniek
Astrum College · Dulon College · TECHNOVA College · ROC A12

Algemene
Verordening
Gegevensverwerking

Informatiebeveiliging en privacy beleid

Christelijke Onderwijs Groep

Versiebeheer

Versie	Status	Datum	Auteur	Omschrijving
0.1	Concept	22-6-2020	Ludo Cuijpers	1e Draft
0.2	Concept	3-8-2020	Henk, Niels en Ludo	2e Draft
0.3	Concept	10-8-2020	Henk, Niels en Ludo	Aanpassing governance
0.4	Concept	11-8-2020	Ludo	Aanpassing grafische vormgeving en verwijzingen
0.5	Concept	12-8-2020	Henk en Ludo	Aanpassingen naamgeving COG onderdelen
0.6	Concept	13-8-2020	Ludo en Henk	Aanpassingen Henk, doorgesproken met Ludo
0.7	Concept	18-8-2020	Henk, Niels en Ludo	Aanpassing bijlage 1 en 2
0.8	Concept	21-8-2020	Pauline, Henk, Niels en Ludo	Aanvullingen Pauline Satter (opdrachtgever CvB)
0.81	Concept	31-8-2020	Ludo, Henk	Correcties Henk versie 0.7 (agendaversie) inge-voegd
0.9	Concept	8-9-2020		Besproken binnen het COGD (geen wijzigingen)
1.0	Vastgesteld	14-9-2020		Ongewijzigd

Vastgesteld door COG:

Versie	Datum	Naam	Functie
1.0	14-9-2020	Jan Jacob van Dijk en Pauline Satter	College van Bestuur

1. Verantwoording en richtlijnen

1.1. Het belang van informatiebeveiliging en privacy

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

1.2. Toelichting informatiebeveiliging

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

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

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

1.3. Toelichting privacy

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

1.4. Vervlechting informatiebeveiliging en privacy

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

1.5. Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

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

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

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

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

1.6. Reikwijdte

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

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

- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van COG 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 COG raakvlakken met:
  - *Algemeen veiligheidsbeleid;* 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/leerlingen, hun ouders/verzorgers en medewerkers.
  - *Informatiebeveiligingsbeleid COG.* Dit beleid zal in 2021 worden ontwikkeld en zal een "technische" aanvulling zijn op het IBP-beleid COG.

1.7. Concretisering[3]

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

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

3. Bij COG 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 COG 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 intrekken of herzien.

4. COG 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.

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

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

6. Binnen COG 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. COG 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/leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

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

10. COG verwacht van alle **medewerkers, studenten/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. COG heeft hiervoor een **gedragscode** geformuleerd, vastgesteld en geïmplementeerd.

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

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

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

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

2. Compliance

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

2.1. Relevante wet- en regelgeving

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

- Wet Educatie en Beroepsonderwijs (WEB)
- Wet op het Voortgezet Onderwijs
- Branche code Goed Bestuur MBO, MBO Raad
- Code Onderwijsbestuur VO, VO Raad
- Wet op het Onderwijstoezicht
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Archiefwet
- Auteurswet
- Wetboek van Strafrecht
- Koppelingswet

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

2.2. Basisregels bij het omgaan met persoonsgegevens

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

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld, inclusief de bewaartermijnen. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes grondslagen, die worden genoemd in de AVG.
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/leerlingen, 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. [5]

[5] Bij Data-integriteit is veilig en discreet omgaan met de toevertrouwde persoonsgegevens uitgangspunt.

2.3. 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 een dataregister. Bijlage 1 geeft een overzicht van de diverse aanvullende documenten die gepubliceerd worden op het COG intranet.

2.4. Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd op basis van het ROSA model. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitscriteria die van belang zijn.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden middels een centraal ingeregeld DPIA (Data Protection Impact Assessment). Vanaf de start van elk nieuw project wordt rekening gehouden met informatiebeveiliging en privacy.

2.5. Incidenten en datalekken

Alle medewerkers die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in het beleid datalekken COG. Bij de afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten kunnen worden gemeld bij de IT-servicedesk of digitaal via meldpuntdatalek@cog.nl.
De (beveiligings)incidenten worden vastgelegd in een incidentenregister en minimaal 2 keer per jaar besproken worden binnen de Information Board. Waar nodig zullen aanvullende passende beleidsmaatregelen genomen worden.

2.6. Planning en controle

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

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

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

2.7. Naleving en sancties

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

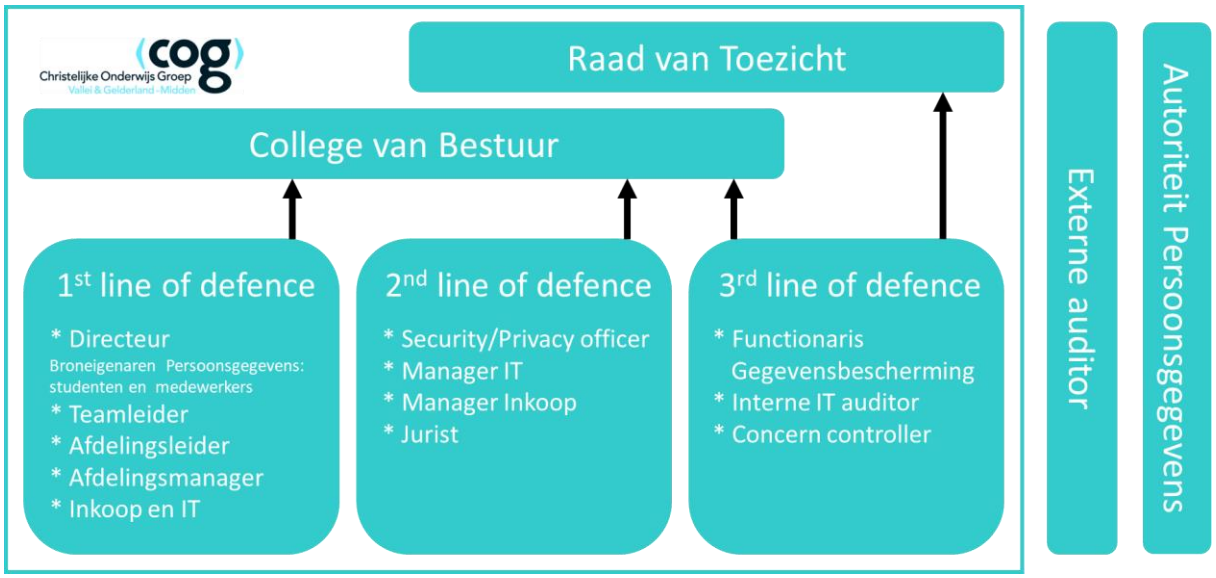
2.8. Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt er voor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens worden vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk. COG zal deze logging regelmatig laten beoordelen door de security/privacy officer.

3. Governance

3.1. Rollen en verantwoordelijkheden

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



3.2. De first line of defense: directeur, teamleider, afdelingsleider, afdelingsmanager, Inkoop en IT

De eerste lijn bewaakt het privacybeleid binnen hun eigen organisatorische onderdeel (bijvoorbeeld onderwijs). Directeuren, teamleiders, afdelingsleiders, afdelingsmanagers, Inkoop en IT vormen de first line of defense als het gaat om de bescherming van persoonsgegevens. Eerstelijnsleidinggevenden (directeuren, teamleiders, afdelingsleiders, afdelingsmanagers, Inkoop en IT) zijn verantwoordelijk en dragen zorg voor de daarbij behorende taken, zoals:

- Toetsen dat geen andere verwerkingen plaatsvinden dan vastgelegd in de dataregisters voor studenten/leerlingen, medewerkers en relaties.
- Toetsen dat een Verwerkersovereenkomst of een Gezamenlijk Verantwoordelijkenovereenkomst wordt afgesloten als persoonsgegevens respectievelijk verwerkt worden door, of overgedragen aan externe partijen.
- Beoordelen van incidenten rondom persoonsgegevens en het intern melden daarvan als het vermoeden bestaat dat het gaat om een datalek.
- Toetsen dat hun medewerkers voldoende geschoold zijn in het kader van de AVG.
- Vastleggen van de extra taken en rollen van medewerkers en de daarbij behorende rechten binnen de bijbehorende systemen/processen.

3.3. De second line of defense: security/privacy officer, manager inkoop, manager IT en de jurist van COG

Experts op het gebied van informatiebeveiliging en privacybescherming werken samen binnen de 2e lijn. De 2e lijn monitort de toepassing en naleving van het informatiebeveiligings- en privacy beleid, adviseert, gevraagd en ongevraagd, over informatiebeveiliging en privacybescherming en ondersteunt de 1e lijn.
De security/privacy officer ontwikkelt waar nodig beleid op het gebied van informatiebeveiliging en privacy, het College van Bestuur stelt dit voorgenomen beleid vast.

3.4. De third line of defense: de Functionaris voor Gegevensbescherming, Interne IT auditor en Concern controller

a) Functionaris voor gegevensbescherming

COG heeft een interne toezichthouder op de verwerking van persoonsgegevens aangesteld. Deze toezichthouder wordt functionaris voor gegevensbescherming genoemd (hierna: "FG"). De FG zal door COG tijdig worden betrokken bij alle aangelegenheden waar persoonsgegevens bij komen kijken. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie binnen COG. COG 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 IBP beleid door COG.
- Het toezien op Data Protection Impact Assessments.
- Het behandelen van klachten over de toepassing van het privacyreglement.
- Fungeren als eerste aanspreekpunt voor en samenwerken met de Autoriteit Persoonsgegevens.

b) Interne IT auditor

De interne IT auditor voert jaarlijks de IBP assessments uit, zowel op centraal niveau als op het niveau van alle organisatorische eenheden, decentraal niveau. Het decentrale IBP assessment is beperkt van aard.

c) Concern controller

Externe controles worden uitgevoerd door onafhankelijke accountants. Deze worden gepland en geformuleerd door de controller van COG.

3.5. De taken van de medewerkers

Onderwerp	1st line of defence	2nd line of defence	3rd line of defence
Autorisaties	Eerstelijnsleidinggevenden brengen autorisaties in kaart (SOLL) en toetsten dit bij de Functioneel beheerders (IST). ❶ (stap 1)	De security/privacy officer en de IT manager controleert of het SOLL en IST autorisatie vergelijk is uitgevoerd. ❷ (stap 2)	De FG'er controleert of de autorisaties zijn ingericht op basis van *need-to-know* en *least privilege*. ❸ (stap 3)
Beleidsdocumenten	Eerstelijnsleidinggevenden zien er op toe dat de goedgekeurde kaders en richtlijnen uit de beleidsdocumenten worden uitgevoerd. ❷	De security/privacy officer schrijft en evalueert de beleidsdocumenten en bespreekt deze met alle stakeholders en de FG'er en dient ze in bij het CvB ter goedkeuring. ❶	De FG'er toetst de kwaliteit van het beleid en de werking van het door het CvB goedgekeurde beleid. ❸
Bewaartermijn	Eerstelijnsleidinggevenden zijn verantwoordelijk voor het handhaven van de bewaartermijnen conform het Documentair StructuurPlan (DSP). ❶	De security/privacy officer adviseert aan de hand van de het Documentair Structuur Plan (DSP) de eerstelijnsleidinggevenden over de geldende bewaartermijnen. ❷	De FG'er ziet er op toe dat de bewaartermijnen worden nageleefd. ❸
Bewustwording	Eerstelijnsleidinggevenden voeren het opleidingsplan van de security/privacy officer uit of stellen een afgeleid opleidingsplan vast. ❶	De security/privacy officer stelt een opleidingsplan op voor IBP-scholings- en awareness plannen en faciliteert ook centrale trainingen. ❷	De FG'er toetst het gewenste kennisniveau aan de scholings- en awareness plannen en komt eventueel met aanbevelingen. ❸
DPIA's	• Eerstelijnsleidinggevenden voeren een pré DPIA uit bij ieder nieuw project. ❶ • Eerstelijnsleidinggevenden voeren een DPIA samen met de security/privacy officer uit. ❸	De security/privacy officer komt op basis van de pré DPIA, uitgevoerd door de eerstelijnsleidinggevenden, tot een voorstel om al dan niet een DPIA uit te voeren en wordt betrokken bij de uitvoering van de DPIA. ❷	De DPIA wordt slechts vastgesteld na goedkeuring van de FG. ❹

Datalekken	Medewerkers melden zelf intern een datalek via IT servicedesk of via meldpuntdatalek@COG.nl. Eerstelijnsleidinggevenden dragen zorg voor bekendheid van de meldprocedure en scholing van haar medewerkers. ❶	De security/privacy officer en/of FG'er beoordelen de melding conform "Beleid melding datalekken". ❷	De FG'er adviseert het CvB om al dan niet het datalek bij de AP en/of de betrokkenen te melden. ❸ Als besloten wordt te melden, zorgt de FG'er dat deze melding tijdig en volledig plaatsvindt. ❹
Dataregisters centraal	De in § 3.7 aangewezen verantwoordelijke eerstelijnsleidinggevenden (broneigenaren) voor de Dataregisters bewaken de actualiteit van het dataregister. ❶	De security/privacy officer adviseert en controleert op volledigheid, juistheid en actualiteit van de Dataregisters. ❷	De FG'er toetst of het dataregister voldoet aan wet- en regelgeving. ❸
Door het management aangewezen uitvoerders	Eerstelijnsleidinggevenden wijzen de deelprocesuitvoerders aan (bijv. examinering, roostering, stage, etc.). ❶	De security/privacy officer toetst het toegewezen eigenaarschap aan de autorisatie. ❷	De interne IT auditor toetst of het eigenaarschap beschreven is. ❸
Rechten van de betrokkenen	Eerstelijnsleidinggevenden ontvangen het verzoek van de FG'er en nemen deze in behandeling (controle door afdeling Studentzaken of afdeling Personele Zaken). ❷	De security/privacy officer rapporteert jaarlijks het aantal verzoeken. ❹	De FG'er is het eerste aanspreekpunt en volgt de vastgestelde procedure. ❶ De FG'er informeert de security/privacy officer . ❸
Verwerkersovereenkomsten	De betrokken eerstelijnsleidinggevende zorgt dat er altijd een verwerkersovereenkomst is opgesteld en kan de security/privacy officer om advies vragen. De eerstelijnsleidinggevende stuurt de verwerkersovereenkomst ter goedkeuring naar de FG'er. ❶	De security/privacy officer en Inkoop adviseren bij verwerkersovereenkomsten op verzoek van de eerstelijnsleidinggevenden. ❷	De FG'er toetst de verwerkersovereenkomst op rechtmatigheid en volledigheid. Het College van Bestuur of door het CvB gemandateerde medewerker tekent de verwerkersovereenkomst. ❸
Vragen van medewerkers betreffende IBP gerelateerde onderwerpen	De eerstelijnsleidinggevende is het eerste aanspreekpunt voor vragen inzake privacy en security, medewerkers kunnen de security/privacy officer ook zelf benaderen. ❶	De security/privacy officer adviseert de eerstelijnsleidinggevende en/of medewerker. ❷	De FG'er toetst de oplossingen bij de gestelde vragen. ❸

3.6. Implementatie beleid

Het College van Bestuur is verantwoordelijk voor de verwerkingen van persoonsgegevens binnen COG. Het College van Bestuur wordt aangemerkt als de verwerkingsverantwoordelijke in de zin van de wet AVG.

De verantwoordelijkheid houdt kort samengevat in:

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

De feitelijke verwerking van persoonsgegevens wordt echter op allerlei lagen van COG uitgevoerd. Het is niet één instituut of dienst die effectief verantwoordelijk kan zijn voor alle persoonsgegevens die COG verwerkt. Er is een onderscheid tussen centrale verwerkingen, waarvoor de centrale organisatie verantwoordelijk zijn, en, aanvullend daarop, decentrale verwerkingen, waarvoor organisatorische eenheden zelf verantwoordelijk zijn.

3.7. Verdeling van de verantwoordelijkheden

COG onderscheidt een drietal soorten verwerkingen van persoonsgegevens met daarbij benoemde broneigenaren:

- De Onderwijsadministraties[6] VO / Studentenadministratie mbo (broneigenaar) zijn verantwoordelijk voor de verwerkingen van persoonsgegevens van alle personen die bij COG onderwijs volgen. De Onderwijsadministraties VO / Studentenadministratie mbo zijn verantwoordelijk voor de volgende dataregisters: Leerling (VO), Student (mbo) en Student tijdelijk niet actief (mbo).
- HRM (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle personen die in opdracht van COG, zowel centraal als decentraal, werk verrichten. HR is verantwoordelijk voor de dataregisters: Medewerkers in loondienst en Medewerkers niet in loondienst.
- Marketing en Communicatie (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle mensen waarmee COG centraal een relatie onderhoudt, zoals belangstellenden, sollicitanten, oud-werknemers, contactpersonen van de stageverlenende organisaties en leveranciers, potentials en alumni. Deze dienst is verantwoordelijk voor het Dataregister van deze relaties.

Elke eerstelijnsleidinggevende die buiten de genoemde broneigenaren om persoonsgegevens verwerkt of verrijkt is zélf verantwoordelijk voor die aanvullende persoonsgegevens.

3.8. Inpassing in instellingsgovernance en afstemming met aanpalende beleidsterreinen

Om de samenhang in de organisatie met betrekking tot gegevensbescherming goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van verwerking van persoonsgegevens binnen de verschillende onderdelen op elkaar af te stemmen, is het belangrijk om gestructureerd overleg te voeren over het onderwerp privacy op verschillende niveaus.
Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van privacyaspecten. Het strategisch niveau wordt voorbereid door de 2e en 3e lijn.
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 2e lijn.
Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan. Het operationeel niveau wordt ingevuld door de eerstelijnsleidinggevenden 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 beheersbaar te houden. Noodzakelijk is het om het bewustzijn voortdurend aan te scherpen, zodat bij COG kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordings-campagnes voor medewerkers, studenten/leerlingen en relaties. Verhoging van het bewustzijn is de verantwoordelijkheid van elke leidinggevende en wordt gefaciliteerd door het de 2e lijn. HRM is hier ook bij betrokken.

3.10. Controle en naleving

Assessments maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert gezamenlijk met de 2e en 3e lijn 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 3e lijn van COG.
Mocht de naleving op de bescherming van data- en privacygegevens ernstig tekortschieten, dan kan COG de betrokken verantwoordelijke medewerkers een maatregel opleggen, binnen de kaders cao-mbo en de wettelijke mogelijkheden.
Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten COG maken het noodzakelijk om periodiek te bezien of men nog voldoende op koers zit met het beleid.

[6] Ook bekend als Leerlingenadministratie.

Bijlage 1: Ondersteunende documenten

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

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

Bijlage 2: Besluitenlijst

Besluit 1: Mobiele apparatuur.

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

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

Trede 2 - Gebruik de door COG beschikbaar gestelde (en beveiligde) IT-omgeving.

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

Trede 3 - Gebruik encryptie.

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

Samenvattend:

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

Besluit 2: Classificatiemodel.

COG hanteert het ROSA classificatiemodel en de uitkomsten van de classificatie worden opgenomen in het dataregister.

Besluit 3: Bewaartermijnen.

COG hanteert:

- Overzicht bewaartermijnen onderwijswetgeving van PO-Raad/VO-Raad/Kennisnet.
- Het DSP (Documentair Structuur Plan) van de MBO Raad.

Besluit 4: Lidmaatschap IBP-netwerk, SCIRT en SCIPR.

COG is actief lid van communities op gebied van IBP, bijvoorbeeld VO-Raad, Kennisnet, saMBO-ICT, SCIPR- en SCIRT-communities van SURF.

Besluit 5: Thuiswerken.

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

Besluit 6: Responsible disclosure procedure.

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

Wat wij van de hacker eisen:

- *Geen openbaarmaking of wijziging van onze gegevens;*
- *Onze gegevens en/of de kwetsbaarheid niet delen met anderen;*

- *Ons zo snel mogelijk (maar uiterlijk binnen 24 uur) en zo volledig mogelijk informeren op fg@cog.nl;*
- *Geen gebruik te maken van deze gegevens door bijvoorbeeld extracties te maken van de database of andere handelingen met de gegevens uit te voeren.*

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

Dit beleid is gepubliceerd op de openbare website van COG.

Besluit 7: Clear desk, Clear screen.

Clear desk en clear screen betekent dat er **geen belangrijke informatie** zichtbaar of bereikbaar is voor mensen die deze informatie niet mogen zien. Zorg er altijd voor dat er geen vertrouwelijke informatie zichtbaar of bereikbaar is voor mensen die deze informatie niet mogen zien

Clear Screen:
Medewerkers dienen hun laptop, computers of andere device te vergrendelen, zodra zij hun device achterlaten. Medewerkers dienen dit bijvoorbeeld te doen als zij een kop koffie gaan halen, naar het toilet gaan etc.
Een device mag niet onvergrendeld toegankelijk zijn voor studenten/leerlingen en collega's of andere derden. Hoewel vergrendeling door COG beheerde apparatuur technisch afgedwongen kan worden, blijft de medewerker zelf verantwoordelijk om zelfstandig voor het vergrendelen van het apparaat als deze niet wordt gebruikt. Tevens moet voorkomen worden dat er ongewenst meegekeken kan worden.

Clean desk:
Medewerkers dienen voorzichtig om te gaan met privacygevoelige en bedrijfskritische informatie. Ze moeten voorkomen dat onbevoegden deze informatie tot zich kunnen nemen. Medewerkers mogen deze informatie niet onbeheerd op hun bureau laten liggen. Medewerkers zijn verplicht de aangewezen kasten te gebruiken voor de opslag van hun fysieke documenten en dienen deze kasten ook telkens af te sluiten.

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

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

Besluit 8: Back-up van informatie.

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

Besluit 9: Logging.

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

Algemeen
Het raadplegen van de technische logbestanden kan alleen door de IT-afdeling of medewerkers die hiertoe zijn gedelegeerd door de IT-afdeling. Bij het toepassen van logging gelden de volgende regels:

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

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

Besluit 10: Crisis ICT
- Een Crisis ICT sluit aan bij het wettelijke calamiteitenplan van het COG.
- Bij een ICT crisis is er een crisisteam beschikbaar tenminste bestaande uit: CvB, directeur Bedrijfsvoering, Security/Privacy officer, FG, één directeur onderwijs en directeur M&C.
- Voor datalekken geldt het beleid c.q. procedure datalekken.

Besluit 11: Dit besluit (BOEK9) is gebaseerd op hoofdstuk 9 van ISO27002, Toegangsbeveiliging.

Bijlage 3: Verklarende woordenlijst

AVG:	Algemene Verordening Gegevensbescherming.
Beleid:	Beleid met betrekking tot het verwerken van persoonsgegevens door COG.
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 COG. 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. Het COG heeft drie centrale registers: dat voor studentgegevens, voor medewerker gegevens en voor relatiegegevens. Het dataregister is het Register van Verwerkingsactiviteiten aangevuld met de BIV-classificatie en de autorisatie matrix op hoofdlijnen.
DPIA:	Data Protection Impact Assessment (Gegevensbeschermingseffectbeoordeling): een beoordeling die helpt bij het identificeren van privacy risico's en de handvaten levert om deze risico's te verkleinen tot een acceptabel niveau. Soms ook wordt de term PIA gebruikt, Privacy Impact Assessment.
Functionaris voor Gegevensbescherming:	Interne toezichthouder en privacy adviseur aangesteld door het College van Bestuur, op grond van artikel 37 van de AVG, ook wel aangeduid als FG.
Kernsystemen:	De hoofdsystemen voor: SIS, HR, Financiën, Rooster, ELO, MIS, CRM, IDM, Office en ARBO.
Minderjarige:	Voor de AVG geldt iedere persoon die de leeftijd van 16 jaar nog niet heeft bereikt. Buiten de AVG geldt uiteraard jonger als 18 jaar.
Niet-geautomatiseerde verwerking:	Voorbeelden: aangetekende stukken, pasjes die zichtbaar gedragen worden, klassenlijsten met foto's (smoelenboek), etc.
Persoonsgegeven:	Elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon.
Privacy by Default:	Een gegevensverwerking waarbij de standaardinstellingen van producten en diensten zo zijn ingesteld dat de privacy van betrokkenen maximaal wordt gewaarborgd. Dit betekent onder meer dat er zo min mogelijk gegevens worden gevraagd en verwerkt.
Privacy by Design:	Al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) wordt ten eerste aandacht besteed aan privacy verhogende maatregelen. Ten tweede wordt rekening gehouden met dataminimalisatie: er worden zo min mogelijk persoonsgegevens verwerkt, alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.
Verwerker:	een door COG ingeschakelde (derde) partij die ten behoeve van COG, 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 COG dat het doel en de middelen van de verwerking van persoonsgegevens vaststelt.