PRIVACYBELEID AVG

2COLLEGE
2023-2024

Vastgesteld	Datum
(Gemeenschappelijke) Medezeggenschapsraad	07-03-2024
Datum inwerkingtreding	20-03-2024
Geldigheidsduur	Tot nieuw beleid wordt vastgesteld
Publicatie	Extern/~~Intern~~

1 Inhoud

2 Inleiding

De Algemene Verordening Gegevensbescherming (AVG) is een verplichting die ons in positieve zin uitdaagt om een stevige ambitie uit te spreken ten aanzien van het privacybeschermingsniveau van zowel leerlingen, ouders als medewerkers. Betrokkenen moeten er te allen tijde op kunnen vertrouwen dat hun gegevens bij ons in veilige handen zijn. Daarnaast is ook de samenleving kritischer en veeleisender geworden ten aanzien van de wijze waarop met privacygevoelige informatie wordt omgegaan. Onze medewerkers spelen hier dan ook een cruciale rol. Datalekken ontstaan immers vaak door menselijke fouten (een tas met stukken in de trein, verloren usb-sticks, versturen van verkeerde e-mail, etc.). AVG-compliance vraagt dan ook een behoorlijke inzet van alle medewerkers maar brengt dan ook het nodige, namelijk de zekerheid voor de leerling en ouders dat hun persoonsgegevens bij ons in veilige handen zijn.

3 Privacy

Binnen 2College werken wij veel met persoonsgegevens van leerlingen, ouders en medewerkers. Deze verzamelen wij voornamelijk voor het goed uitvoeren van onze taken. Zij moeten erop kunnen vertrouwen dat 2College zorgvuldig en veilig met hun persoonsgegevens omgaat.

Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitaal onderwijs stellen andere eisen aan de bescherming van gegevens en privacy. 2College is zich hiervan bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen te treffen op het gebied van (informatie)beveiliging en dataminimalisatie.

Met de inwerkingtreding van de AVG is er sprake van een versterking en uitbreiding van privacyrechten en ontstaan er meer verantwoordelijkheden voor organisaties. De bevoegdheden van de Europese toezichthouders, voor Nederland de Autoriteit Persoonsgegevens, worden uitgebreid. Een voorbeeld hiervan is de bevoegdheid om boetes tot 20 miljoen euro op te leggen of 4% van de wereldwijde jaaromzet. Het bestuur, management en de medewerkers spelen een cruciale rol bij het waarborgen van privacy.

2College geeft met dit beleid duidelijk richting aan hoe de organisatie om moet gaan met privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie en op alle processen, onderdelen, objecten en gegevensverzamelingen van 2College waarin persoonsgegevens worden verwerkt. Het ontwikkelde beleid is dan ook vooraf breed afgestemd voordat het ter instemming bij de Medezeggenschapsraad werd aangeboden. Het privacybeleid van 2College is in lijn met het Privacyreglement van Ons Middelbaar Onderwijs (OMO) en de relevante nationale en Europese wet- en regelgeving.

4 Privacybeleidskader

Dit privacybeleid treedt in werking na vaststelling door de Kerndirectie van 2College en na instemming van de Medezeggenschapsraad. Het beleid wordt elk jaar geëvalueerd en indien nodig herzien.

5 Organisatie

De verantwoordelijkheid binnen 2College voor de zorgvuldige omgang met persoonsgegevens ligt bij de rector en bij de vestigingen. Dat betekent ook dat de lijn (de preventiemedewerker/vestigingsdirecteur) binnen de vestiging zelf wordt aangesproken op het nakomen van de uit dit privacybeleid voortvloeiende eisen. Privacy is immers niet een op zichzelf staand iets, maar is onlosmakelijk verbonden met onze diensteverlening.

5.1 Verwerkingsverantwoordelijke

In de AVG wordt de nadruk gelegd op de verantwoordelijkheid van organisaties en instanties (in de AVG aangeduid als 'verwerkingsverantwoordelijken') om aan te kunnen tonen dat zij zich aan de wet houden (accountability). De verwerkingsverantwoordelijke is degene die alleen of samen met anderen het doel van en de middelen voor de verwerking vaststelt.

Omdat 2College valt onder het bestuur van de vereniging Ons Middelbaar Onderwijs, is het bestuur van OMO het verantwoordelijke orgaan die invulling geeft aan de taken en verantwoordelijkheid die krachtens de AVG zijn toebedeeld aan de verwerkingsverantwoordelijke. Formeel is het bestuur van OMO dan ook verantwoordelijk voor de verwerkingen die onder de reikwijdte van de AVG vallen.

De verwerkingsverantwoordelijken zijn verantwoordelijk voor:

- De naleving van de beginselen voor de verwerking van persoonsgegevens.
- De maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd.

5.1.1 Functionaris voor de gegevensbescherming (FG)

De AVG stelt het aanstellen van een FG verplicht voor overheidsinstanties en publieke organisaties. OMO heeft een FG welke toeziet dat OMO voldoet aan de wettelijke verplichtingen bij het verwerken van persoonsgegevens. Hij toetst onder andere de naleving van de wettelijke eisen, richtlijnen op het gebied van privacy, het privacybeleid en informatiebeveiligingsbeleid. 2College heeft ook een eigen FG welke in nauw contact staat met de eindverantwoordelijk FG van OMO en met de Privacy Officer van OMO. De FG van 2College ziet toe dat 2College voldoet aan de verplichtingen bij het verwerken van persoonsgegevens. Hij toetst, onder andere, de naleving van de wettelijke eisen, richtlijnen op het gebied van privacy, het privacybeleid en informatiebeveiligingsbeleid.

5.1.2 Preventiemedewerker

Op iedere vestiging is een preventiemedewerker aanwezig (Zie meer in het *Schoolveiligheidsplan*) en deze is verantwoordelijk voor het uitvoeren van het privacybeleid op de vestiging en is tevens aanspreekpunt van en voor de FG van 2College en voor de medewerkers op de desbetreffende vestiging.

5.2 Verantwoordingsplicht

De verantwoordingsplicht van, ook wel accountability genoemd, brengt met zich mee dat 2College niet alleen de regels moet naleven, maar dit ook, al dan niet via OMO, moet kunnen aantonen. In dit kader neemt de desbetreffende verantwoordelijke de volgende maatregelen:

1. Een actueel en volledig registerverwerkingen.
2. Opname in het verwerkingenregister van alle relevante documenten die betrekking hebben op de naleving van de verplichtingen uit de AVG, zoals informatieplicht en de afspraken met verwerkers.
3. Openbaarmaking van het onderhavige privacybeleid.
4. Zorgen voor de aantoonbaarheid van de juiste behandeling van informatie.

Tevens houdt de verantwoordingsplicht in dat 2College een register van datalekken die zijn opgetreden bijhoudt en, waar passend, een gegevensbeschermingseffect beoordeling uitvoert.

N.B. Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is.

5.3 Rechten van betrokkenen

Binnen het beleid worden de rechten van betrokkenen geborgd in de *Privacyverklaring personeel 2College* en in de *Privacyverklaring leerlingen 2College (afgeleid van het privacyreglement OMO)*:

5.4 Uitoefening van rechten

Om gebruik te maken van de bovenstaande rechten kunnen de betrokkenen een verzoek indienen. Hoe dit gedaan moet worden is opgenomen in de privacyverklaring personeel 2College en in de privacyverklaring leerlingen 2College.

5.5 Klachten

Elke betrokkene heeft het recht bij 2College een klacht in te dienen of bezwaar te maken tegen de wijze waarop zijn of haar persoonsgegevens worden verwerkt. Hoe dit gedaan moet worden is opgenomen in de privacyverklaring personeel 2College en in de privacyverklaring leerlingen 2College.

5.6 Bewustwording

De vestigingen zorgen voor voldoende bewustwording bij hun medewerkers op het gebied van privacy. Hierbij dienen zij minimaal op de hoogte te zijn van de privacyregels en de voor hun werkzaamheden relevante bepalingen zodat zij deze in hun dagelijkse werk kunnen toepassen. De verantwoordelijkheid voor bewustwording ligt bij de vestigingen waarbij vanuit de FG (aan)sturing plaatsvindt. Er wordt namelijk vanuit 2College een awareness plan opgesteld met daarin zowel jaarlijks terugkerende als eenmalige activiteiten.

6 Informatiebeveiliging en Datalekken

6.1 Informatiebeveiligingsbeleid

Informatiebeveiliging is de verzamelnaam voor de processen, die 2College inricht om de betrouwbaarheid van informatie te beschermen, ook als die zich in processen of in informatiesystemen bevinden. Het begrip 'informatiebeveiliging' heeft betrekking op:

- Beschikbaarheid: het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Vertrouwelijkheid: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- Integriteit: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Het I*nformatiebeveiligingsbeleid*, dat door OMO is vastgesteld, heeft betrekking op alle processen, waaronder de processen waarin (persoons)gegevens worden verwerkt. Op basis van dit *Informatiebeveiligingsbeleid* heeft 2College een *Informatiebeveiligingsplan* opgesteld waarbij het beleid van OMO verder is uitgewerkt.

6.2 Meldplicht datalekken

Indien zich een informatiebeveiligingsincident voordoet, waarbij bijvoorbeeld persoonsgegevens in verkeerde handen kunnen komen of zijn gekomen, handelt 2College in overeenstemming met de vastgestelde werkwijze in het *Protocol melden: incidenten, datalek en arbeidsongevallen 2College*. Dit protocol bevat een vastgesteld proces van de te doorlopen stappen om de eventuele schade of de kans hierop, bij een datalek te beperken en de getroffen perso(o)n(en) te beschermen.

Het gaat bij een datalek om situaties waarbij een onrechtmatige verwerking van persoonsgegevens heeft plaatsgevonden, waarbij beveiligingsmaatregelen (on)bewust zijn omzeild of doorbroken of dat geen of onvoldoende beveiligingsmaatregelen zijn genomen. Het gaat ook om situaties waarbij persoonsgegevens verloren zijn gegaan, waardoor ze niet meer beschikbaar zijn en om situaties waarin gegevens in handen kunnen komen of zijn gekomen van derden die geen toegang tot die gegevens mogen hebben.

De plicht tot het melden van een (vermoeden van een) datalek geldt als er sprake is van een aanzienlijke kans op ernstige nadelige gevolgen voor betrokkene, dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens. Het betreft situaties van het (mogelijk) lekken van persoonsgegevens uit 2College bestanden en/of gegevens waarvoor 2College verantwoordelijkheid draagt. Wanneer er een dergelijk datalek heeft plaatsgevonden, wordt dit zonder onredelijke vertraging, uiterlijk 72 uur nadat er kennis van de inbreuk is vernomen, gemeld aan de Autoriteit Persoonsgegevens. Dit melden wordt gedaan door de Functionaris Gegevensbescherming van OMO. Als dit later dan 72 uur is wordt er een motivering voor de vertraging bij de melding gevoegd. Het kan zijn dat de inbreuk een hoog risico met zich meebrengt voor de rechten en vrijheden van de betrokkenen. In dit geval wordt dit ook aan de betrokkenen gemeld, in eenvoudige en duidelijke taal.

6.3 Beveiligingsmaatregelen

Deze (technische, procesmatige, communicatie en organisatorische) maatregelen omvatten bij de verwerking van persoonsgegevens een op het risico afgestemd beveiligingsniveau. Hierbij wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, en ook met de aard, de omvang, de context en de verwerkingsdoeleinden etc. Tevens wordt rekening gehouden met de, qua waarschijnlijkheid en ernst, uiteenlopende risico's voor de rechten en vrijheden van personen. Waar passend omvatten de maatregelen op grond van artikel 32 AVG onder meer het volgende:

a. De pseudonimisering en versleuteling van persoonsgegevens;

b. Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

c. Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

d. Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Wanneer 2College persoonsgegevens verwerkt of laat verwerken door een derde, zorgt 2College ervoor dat passende beveiligingsmaatregelen (conform het *informatiebeveiligingsbeleid*) worden getroffen om de betreffende persoonsgegevens te beschermen tegen de verschillende risico's.

6.4 Het register van verwerkingsactiviteiten

De FG van OMO houdt namens de verantwoordelijke een register bij, bestemd voor de inschrijving van verwerkingen van persoonsgegevens.

Bij de inschrijving worden in ieder geval de volgende gegevens vermeld:

a. de naam van de verwerking;
b. wie de verantwoordelijke is voor de verwerking;
c. het doel van de verwerking;
d. de groep van personen van wie persoonsgegevens worden verwerkt (betrokkenen);
e. de categorie persoonsgegevens die bij de verwerking worden gebruikt;
f. de ontvangers van de gegevens;
g. de rechtmatige grondslag voor de verwerking van de persoonsgegevens;
h. eventuele verstrekkingen aan andere landen buiten de Europese Economische Ruimte;
i. de verwijderingstermijnen die in acht genomen worden;

De FG van OMO houdt toezicht op de volledigheid en rechtmatigheid van de in het register ingeschreven verwerkingen van persoonsgegevens en de daarbij behorende documenten (eventuele verwerkersovereenkomst). Bij wijzigingen van de bij de inschrijving opgenomen gegevens draagt de Privacy Officer OMO zorg voor wijziging hiervan in het register en informeert de FG van OMO hierover.

7 Naleving van het beleid

7.1 Risico-beheersing (en controlemechanismen)

Vanuit de gedachte van risicobeheersing, neemt 2College verschillende maatregelen om de risico's bij de verwerking van persoonsgegevens in kaart te brengen en te verminderen.

Hiervoor gelden vier cycli van risicobeheersing:

1. In kaart brengen verwerkingen met persoonsgegevens;
2. Uitvoeren Gegevensbeschermingseffectbeoordelingen, evaluatie van getroffen maatregelen, of formuleren van aanvullende maatregelen;
3. Afleggen verantwoording aan toezichthoudende FG;
4. Periodiek evalueren van privacy incidenten.

De cycli van risicobeheersing worden in de praktijk aan de hand van de hieronder toegelichte controlemechanismen ten uitvoer gebracht.

7.2 Gegevensbeschermingseffectbeoordeling[1]

Een Gegevensbeschermingseffectbeoordeling[2] (GEB) is een instrument waarmee het effect van beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens op een gestructureerde en heldere manier in beeld in kaart wordt gebracht om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.

Een GEB wordt doorgaans uitgevoerd door de Privacy Officer, voorafgaand aan de verwerking en bij bestaande verwerkingen, waar sprake is van een gegevensverwerking die een hoog privacyrisico oplevert voor de betrokkenen. Tevens stelt de Autoriteit Persoonsgegevens een lijst samen voor verwerkingen waarbij een GEB altijd verplicht is. Of er sprake is van een hoog privacyrisico, toetst 2College dan wel OMO aan de hand van een Risk Impact Assessment (RIA).

Op grond van de AVG is verder in ieder geval sprake van een hoog privacyrisico indien 2College:

- Systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling;
- Op grote schaal bijzondere persoonsgegevens verwerkt of op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied;

  Hierbij wordt gelet op het aantal betrokkenen, het volume van gegevens en/of het bereik van verschillende gegevens/items die worden verwerkt, de duur of het permanente karakter van de gegevensverwerkingsactiviteit en de geografische omvang van de verwerkingsactiviteit;
- Indien wordt voldaan aan twee of meer criteria van de criteria van de werkgroep van Europese privacy-toezichthouders (WP29).

Voor de GEB gelden de volgende kaders:

- Een GEB vindt plaats voordat met de betreffende verwerking wordt gestart.
- Een GEB wordt na maximaal 3 jaar herhaald ter evaluatie, alsmede bij wijzigingen waardoor de risico's van de verwerking toenemen.
- Bij het uitvoeren van een GEB wordt de FG van OMO altijd geïnformeerd.

[1] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp248_rev.01_nl.pdf

[2] Ook wel een Data Protection Impact Assessment (DPIA)

- De FG van 2College ziet toe op het nemen van maatregelen die blijkens de GEB nodig zijn om de risico's te verkleinen.
- Het resultaat van de GEB en de genomen maatregelen om het risico te beperken worden aan de FG van OMO voorgelegd ter toetsing en opneming in het registerverwerkingen.
- Indien 2College niet in staat is om voldoende maatregelen te treffen om de risico's te beperken, wordt de AP om een voorafgaande raadpleging gevraagd.
- GEB die binnen 2College worden uitgevoerd vinden plaats volgens de standaard die bepaald is door de FG van OMO.

7.3 Privacy door ontwerp (privacy by design)

Privacy door ontwerp omvat vier uitgangspunten:

- Minimaal gebruik van persoonsgegevens
- Passende bescherming van de persoonsgegevens
- Gerechtvaardigd gebruik van persoonsgegevens
- Borg de rechten van betrokkenen

Dit betekent dat 2College bij het ontwerpen van producten en/of diensten, het inkopen van systemen en bij de uitvoering van haar werkzaamheden de volgende uitganspunten hanteert:

Minimaal gebruik van persoonsgegevens:

- 2College verzamelt (of vraagt om) niet meer gegevens dan noodzakelijk of juridisch mogelijk;
- 2College verwerkt alleen gegevens voor het doel waarvoor zij zijn verzameld en verwerkt deze verder alleen op een manier die verenigbaar is met dit doel;
- Bij configuratie van systemen kiest 2College, indien mogelijk, voor de privacy-vriendelijke variant (privacy by default);
- De informatie die 2College verwerkt is correct en actueel;
- 2College maakt geen onnodige kopieën;
- 2College verwijdert wat niet meer nodig is.

Passende bescherming:

- 2College slaat gegevens zo op dat voldaan kan worden aan de wettelijke kaders van de AVG, dit betekent in verband met de doelbinding vaak gescheiden opslag;
- 2College beperkt de toegang tot inzage en wijzigen van gegevens tot degenen die dit vanuit hun functie nodig hebben;
- 2College beschermt persoonsgegevens door o.a. het aggregeren, versleutelen en anonimiseren van deze gegevens. Hierdoor wordt de mate waarin de verwerkte persoonsgegevens kunnen worden herleid verminderd.

Als uitgangspunt kiest 2College voor technische maatregelen om de privacy door ontwerp te waarborgen. Daar waar de technische mogelijkheden ontbreken of disproportioneel hoge kosten met zich meebrengen zoekt 2College naar organisatorische en of procesmatige maatregelen als alternatief voor of als aanvulling op de technische maatregelen. Dit wordt uiteraard samen en in overleg met de verantwoordelijke voor informatiebeveiliging uitgewerkt.

7.4 Privacyprotocol

2College stelt, indien nodig, aanvullend een specifiek privacyprotocol vast voor een bepaald proces waarbij persoonsgegevens worden verwerkt, indien:

- De verwerking blijkens de GEB extra privacywaarborgen behoeft; of

- De FG van 2College daartoe adviseert.

De FG van 2College toetst het desbetreffende privacyprotocol op rechtmatigheid en volledigheid en neemt dit op in de registerverwerkingen.

8 Inschakeling verwerkers, verwerkersovereenkomst

8.1 Verwerkers

Wanneer 2College een partij inschakelt om ten behoeve van 2College persoonsgegevens te verwerken en het verwerken van de persoonsgegevens de (primaire) taak is van deze partij, kan deze partij worden beschouwd als verwerker. 2College schakelt enkel verwerkers in die afdoende garanties bieden met betrekking tot het toepassen van passende technische, procesmatige, communicatieve en organisatorische maatregelen. De afspraken omtrent de verwerking door de verwerker worden schriftelijk vastgelegd met OMO in een verwerkersovereenkomst en worden periodiek of steekproefsgewijs getoetst door 2College dan wel OMO.

8.2 Camerabeelden

2College past op verschillende plekken binnen haar organisatie registratie van bewegende beelden toe. Het gaat hierbij om bewakingscamera's. Om dit conform de AVG goed geregeld en geborgd te hebben beschikken wij over een *Cameratoezichtbeleid* en een *reglement Cameratoezicht.*

9 Afwijken van beleid

Afwijken van het beleid is niet toegestaan.

Dit privacybeleid treedt in werking na vaststelling door de Kerndirectie van 2College en na instemming van de Medezeggenschapsraad. Het beleid wordt elk jaar geëvalueerd en indien nodig herzien.

10 Overzicht van de protocollen

Cameratoezichtbeleid
Reglement Cameratoezicht
Informatiebeveiligingsbeleid
Informatiebeveiligingsplan
Protocol melden: incidenten, datalek en arbeidsongevallen 2College
Privacyverklaring personeel 2College
Privacyverklaring leerlingen 2College
Privacyreglement OMO
ICT-gedragscode 2College (ICT Gebruiksvoorwaarden) personeel
ICT-gedragscode 2College (ICT Gebruiksvoorwaarden) leerlingen