Privacy beleid 2018

Vastgesteld door het College van Bestuur op 23-04-2018

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

Het naleven van wet- en regelgeving betreffende het beschermen van de privacy van betrokkenen, de bescherming van persoonsgegevens vereist een beheerstructuur en beheersing. Om sturing te kunnen geven aan deze beheerstructuur wordt het privacy beleid opgesteld.

1.2 Doel

Het doel van dit document is het geformuleerde Privacy beleid vastleggen en ter accordering aanbieden aan het College van Bestuur. Het beleid wordt gecommuniceerd aan medewerkers en relevante externe partijen en gepubliceerd op de website en het intranet van het Alfa-college.
Dit document is een dynamisch document. Een keer per jaar worden alle mutaties en aanpassingen verwerkt in een nieuwe versie van het Privacy beleid om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.

2. Privacywetgeving

2.1 Begrippen

Persoonsgegeven:
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon

Verwerking:
Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Betrokkene:
Degene op wie een persoonsgegeven betrekking heeft.

Verantwoordelijke:
Het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Ontvanger:
Degene aan wie de persoonsgegevens worden verstrekt.

Verwerker:
Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

Ondubbelzinnige toestemming:
De betrokkene heeft voor de verwerking zijn **ondubbelzinnige** toestemming gegeven. Deze uitdrukkelijke toestemming wordt ook *geïnformeerde toestemming* of *informed consent* genoemd. Dat betekent dat de betrokkene exact weet waar hij of zij toestemming voor gegeven heeft.

Datalek:

Er is sprake van een datalek wanneer persoonsgegevens verloren raken of onrechtmatig worden verwerkt.

2.2 Uitgangspunten en begrippen

Bij privacywetgeving zijn de volgende uitgangspunten en beginselen van belang:

1. **Doel**
   Persoonsgegevens worden altijd verzameld met een vooraf vastgesteld doel. Eenmaal verzamelde gegevens mogen dus niet zomaar voor een nieuw doel gebruikt worden.

2. **Doelbinding**
   Persoonsgegevens mogen alleen worden verwerkt voor zover dat nodig is om het vastgestelde doel te bereiken. Gegevens die daarmee niet in verband staan, mogen dus ook niet worden verwerkt.

3. **Grondslag**
   Persoonsgegevens mogen alleen verwerkt worden als er een grondslag voor is namelijk indien:

   a. De betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;

   b. De gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is;

   c. De gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;

   d. De gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;

   e. De gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt;

   f. De gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

4. **Transparantie**

De betrokkene is **vooraf in begrijpelijke taal geïnformeerd** over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is.
De betrokkene heeft recht op inzage, correctie, verwijdering van zijn persoonsgegevens.

5. **Dataminimalisatie**:
Het **verzamelen van persoonlijke data moet minimaal zijn**. De persoonsgegevens moeten redelijkerwijs nodig zijn om het doel te bereiken:
Ze moeten in verhouding staan tot het doel (proportioneel);
Het doel kan niet met minder dan deze verzamelde gegevens worden bereikt (subsidiair).

2.3 Reikwijdte

Het Privacy beleid is bedoeld voor de verwerking van persoonsgegevens van alle gebruikers van de informatievoorziening van het Alfa-College.

3. Uitgangspunten en randvoorwaarden

Het Alfa-college houdt zich aan de geldende wet- en regelgeving.

3.1 Normen

Privacy compliance kader MBO
Surf juridisch normenkader (Cloud)services
Privacy Impact Assessment (PIA) Norea

3.2 Wet- en regelgeving

Voor de naleving van de privacywetgeving zijn de volgende wetgevingen van belang:

Wet- en regelgeving	Relevantie
Richtlijn 95/46/EG	Een Europese Richtlijn betreffende privacy en gegevensbescherming. Deze is omgezet in alle lidstaten in een nationale wet.
Wet bescherming persoonsgegevens	De Nederlandse vertaling van de Richtlijn 95/46/EG. Eindigt per 25-05-2018
Algemene verordening gegevensbescherming	De AVG zal vanaf 25 mei 2018 de Richtlijn 95/46/EG vervangen.
Europees Verdrag Rechten van de Mens en fundamentele vrijheden (EVRM), artikel 8.	Artikel 8 EVRM vormt de basis van het privacy recht in de breedste zin van het woord. Het is een verdrag van de Raad van Europa.
Grondwet, artikel 10	De Nederlandse basis voor het privacy recht
Internationaal Verdrag inzake Burgerrechten en Politieke Rechten (IVBPR), artikel 17	Het internationale recht op privacy en gegevensbescherming
Handvest Grondrechten van de EU, artikel 7, 8 en 52(1)	De basis voor privacy recht vanuit de Europese Unie
Wet algemene bepalingen Burgerservicenummer	
Sectorale Europese regelgeving	Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), 2002/58/EG, 31 juli 2002 Richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen, 7 februari 2013, NIB COM (2013) 48 final Verordening nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt, 4 juni 2012

Vrijstellingsbesluit WBP	Een besluit waar de verwerkingen in staan die niet gemeld hoeven worden bij de AP.
Sectorale Nederlandse regelgeving	In de onderwijssector is specifieke regelgeving van toepassing. Denk aan de WEB, Wet op de loonbelasting, Ziektewet, WIA, de Jeugdwet.

4. Beleidsuitspraken

4.1 Register van verwerkingen

De verantwoordelijke van het Alfa-college houdt een register van verwerkingsactiviteiten bij die onder haar verantwoordelijkheid valt.
De volgende onderdelen worden hier in verwerkt:
- Verwerkingsdoeleinden;
- Beschrijving Categorieën betrokkenen en categorieën persoonsgegevens;
- Contactgegevens FG, verantwoordelijke en verwerker;
- Categorieën ontvangers;
- Bewaartermijnen;
- Technische en organisatorische beveiligingsmaatregelen;
- Indien van toepassing doorgifte naar derde land of internationale organisatie.

4.2 Gegevensbeschermingseffectbeoordeling (Privacy Impact Assessment, PIA)

Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden een hoog risico inhoudt voor de rechten en vrijheden van personen voert de verwerkingsverantwoordelijke van het Alfa-college vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.

Een PIA is verplicht bij:

1) Profiling
2) Grootschalige verwerking van bijzondere persoonsgegevens
3) Gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten
4) Stelselmatige en grootschalige monitoring van openbare ruimten
5) Alle andere verwerkingen die de Autoriteit Persoonsgegevens (AP) aanwijst.

De PIA richt zich op technische infrastructuur, processen, systemen en administratieve organisatie. Maar ook op het beoordelen van de Privacywetgeving.

4.3 Verwerkersovereenkomst

Daar waar het Alfa-college een verwerker aanstelt om de verwerking van de persoonsgegevens uit te voeren zal een verwerkersovereenkomst worden afgesloten.

4.4 Functionaris gegevensbescherming

Organisaties hebben de mogelijkheid zelf een interne toezichthouder op de verwerking van persoonsgegevens aan te stellen. Dit wordt een functionaris voor de gegevensbescherming (FG)

genoemd. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Privacywetgeving.

4.5 Privacy bij design:

Bij het ontwerpen van producten en diensten houdt men al rekening met dat voldaan moet worden aan de Privacywetgeving.

4.6 Privacy bij default:

De standaardinstellingen van producten en diensten moeten zo worden ingericht dat wordt voldaan aan de Privacywetgeving.

4.7 Bewaartermijnen

De verantwoordelijke moet het volgende geregeld hebben:

1) Bepalen wat de bewaartermijnen van de persoonsgegevens zijn. Leg de bewaartermijnen of de criteria vast in een bewaarbeleid (het Alfa-college gebruikt het Basis selectie document en het Document Structure Plan (DSP) model);
2) De bewaartermijnen moeten in het register van verwerkingen worden opgenomen;
3) De betrokkenen moeten geïnformeerd worden over de bewaartermijnen.

4.8 Gedragscode en geheimhoudingsverklaring

Een belangrijke manier om medewerkers bewust te maken van informatiebeveiliging en de naleving van de Privacywetgeving is de Gedragscode voor medewerkers en studenten. Bij het inhuren van externe medewerkers wordt gevraagd een geheimhoudingsverklaring te tekenen.

4.9 Technische en organisatorische maatregelen

De verantwoordelijke van het Alfa-college en de door de verantwoordelijke aangestelde verwerkers nemen passende technische en organisatorische maatregelen om persoonsgegevens te beschermen. Zij kunnen beiden de effectieve werking van deze maatregelen aantonen.

4.10 Rechten van betrokkenen

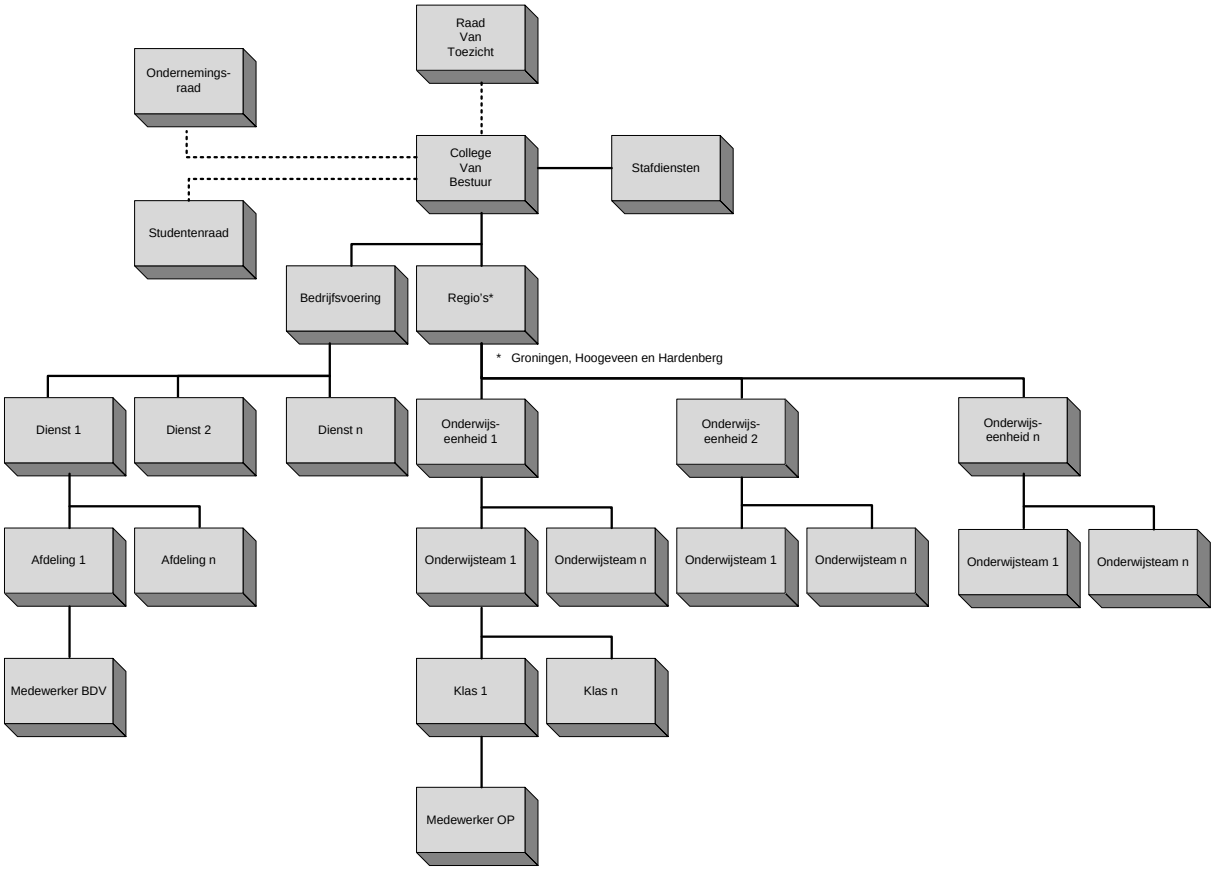
Het Alfa-college moet de rechten van Betrokkenen respecteren.
Deze rechten zijn:

1) Recht op informatie;
2) Recht om vergeten te worden;
3) Recht op dataportabiliteit (overdraagbaarheid);
4) Recht van inzage;
5) Recht op rectificatie en wissen;
6) Recht op beperking van de verwerking;
7) Recht van bezwaar;
8) Recht om niet te worden onderworpen aan profiling.

5. Organisatie, taken en verantwoordelijkheden

5.1 Privacy organisatie

5.1.1 Organigram



5.1.2 Taken en bevoegdheden

College van Bestuur:

Het College van Bestuur is verantwoordelijk voor het opstellen en uitdragen van het organisatiebeleid en het Privacy beleid dat daarvan is afgeleid.

Daarnaast houdt het College van Bestuur controle op de naleving van het afgesproken beleid en bijbehorende wet- en regelgeving en is de "Verwerkingsverantwoordelijke" in het kader van de Algemene Verordening Gegevensbescherming (AVG).

Directeuren

De directeuren zijn verantwoordelijk voor de implementatie, de uitvoering en naleving van het Privacy beleid in hun organisatorische eenheid.

Manager Informatisering en Projecten

De manager van de dienst Informatisering en Projecten is verantwoordelijk voor de voorbereiding van het strategisch, tactisch en operationeel beleid op het gebied van informatisering en is verantwoordelijk voor het implementeren, de uitvoering en naleving van het Privacy beleid in zijn organisatorische eenheid.

Informatiemanagers en Beleidsmedewerker/adviseur Informatiebeveiliging

De beleidsmedewerker/adviseur Informatiebeveiliging en de informatiemanagers dragen zorg voor de ontwikkeling, implementatie, uitvoering en naleving van het beleid binnen de dienst Informatisering en Projecten. Zij bewaken en evalueren dit beleid waaronder het Privacy beleid.

Lijnmanagers:

De opleidingsmanagers en de managers van de diensten zijn verantwoordelijk voor de uitvoering en naleving van het Privacy beleid binnen de eigen organisatorische eenheid.

Medewerkers:

Alle medewerkers van het Alfa-college zijn verantwoordelijk voor de uitvoering en naleving van het Privacy beleid binnen hun eigen werkzaamheden.

Studenten:

Alle studenten van het Alfa-college zijn aanspreekbaar op de uitvoering en naleving van het Privacy beleid in het kader van hun opleidingsactiviteiten.

Functionaris Gegevensbescherming:

De functionaris gegevensbescherming(FG) informeert en adviseert de verwerkingsverantwoordelijke, de medewerkers en studenten van het Alfa-college over hun verplichtingen ten aanzien van de Algemene Verordening Gegevensbescherming en andere gegevensbeschermingsbepalingen.
De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de privacywetgeving en het Privacy beleid. De FG zorgt voor training en bewustwording van de medewerkers en studenten ten aanzien van de privacywetgeving, voert audits uit en beoordeeld de privacy impact assessments. (PIA's).

6. Informatiebeveiligingsincidenten en datalekken

6.1 Procedure datalekken

1) Inleiding

Vanaf 1 januari 2016 is het wettelijk verplicht om datalekken te melden.
Zowel grootschalige inbraak als ieder kwijtraken, diefstal of onbevoegd gebruik van persoonsgegevens telt als een datalek.
Wie data laat lekken of persoonsgegevens verwerkt zonder zich aan de wet te houden, loopt kans op hele hoge boetes.

2) Wat is een datalek?

De wet spreekt van een datalek wanneer persoonsgegevens verloren raken of onrechtmatig worden verwerkt. Er is dus niet alleen sprake van een datalek als een hacker toegang tot persoonsgegevens krijgt. Ook verlies van een USB-stick, of het sturen van een mailing met adressen in het CC-veld (in plaats van het BCC-veld) telt al als datalek. En het verlies van gegevens zoals bij een brand in het datacentrum terwijl er geen back up beschikbaar is, ziet de wet als een datalek.

3) Wanneer moet een datalek gemeld worden aan de toezichthouder?

De toezichthouder is de Autoriteit Persoonsgegevens.
De wet bepaalt dat 'ernstige' datalekken binnen 72 uur bij de toezichthouder gemeld moeten worden. Een lek kan ernstig zijn als het een grote hoeveelheid data betreft (kwantitatief ernstig), maar ook als het om gevoelige gegevens gaat (kwalitatief ernstig).
Een paar voorbeelden uit de tweede categorie zijn:

1) Inloggegevens;
2) Financiële gegevens;
3) Kopieën van identiteitsbewijzen;
4) Gegevens die betrekking hebben op levensovertuiging;
5) Gegevens die betrekking hebben op gezondheid.

4) Wanneer moet een datalek gemeld worden aan de getroffen personen?

Indien het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de personen van wie de gegevens gelekt zijn, dient het lek binnen 72 uur gemeld te worden aan de getroffen personen, de betrokkenen.
Ongunstige gevolgen zijn bijvoorbeeld:
identiteitsfraude;
discriminatie;
reputatieschade.

5) Wat zijn de gevolgen van de wet?

De wet kent vanaf 1 januari 2016 de mogelijkheid om boetes op te leggen wanneer niet voldaan wordt aan de wet. Deze boetes kunnen onder meer opgelegd worden voor:

1) Het niet melden van een datalek terwijl dat wel moet;
2) Het niet op orde hebben van de beveiliging van de persoonsgegevens;
3) Het verwerken van persoonsgegevens zonder toestemming;
4) Export van persoonsgegevens naar landen buiten de EU zonder dat goed geregeld te hebben.

De Autoriteit Persoonsgegevens kan extreem hoge boetes opleggen die (per 25-05-2018) kunnen oplopen tot maximaal 20.000000 of 4% van de wereldwijde omzet. Vaak zal er eerst een waarschuwing gegeven worden, maar de toezichthouder mag besluiten direct een boete op te leggen als er opzettelijk of grof nalatig gehandeld is.

6) Melden en registreren

De medewerkers en studenten dienen informatiebeveiliging- en privacy incidenten(datalekken) te melden bij het ICT-Servicepunt of rechtstreeks bij de Functionaris voor de gegevensbescherming. De incidenten worden geregistreerd als Informatiebeveiligingsincidenten. Bij het vermoeden van een datalek wordt het incident doorgezet naar de Functionaris voor de gegevensbescherming (FG) als het incident in eerste instantie bij het ICT-Servicepunt is gemeld.
Datalekken worden zo snel mogelijk (uiterlijk binnen 24 uur gemeld) bij de Functionaris voor de gegevensbescherming (FG). Zodat dit beoordeeld kan worden en de FG indien nodig binnen 72 uur kan melden bij de Autoriteit Persoonsgegevens (AP).

6.2 Doelen

De doelen die nagestreefd worden met het melden van incidenten zijn:

- Het minimaliseren van de schade die veroorzaakt wordt door incidenten;
- Het wegnemen van de kwetsbaarheid of de oorzaak;
- Het monitoren van incidenten;
- Er lering uit trekken.

6.3 Incidentrapportage en register van datalekken.

Er dient een rapportage van incidenten gemaakt te worden voor zowel Informatiebeveiliging- als Privacy incidenten. Met deze rapportage kan de Functionaris gegevensbescherming beoordelen of de bestaande maatregelen en of beleid passend en toereikend zijn of dat zij moeten worden aangepast. Deze rapportage stelt de Functionaris ook in staat het College van Bestuur en de Directeur Bedrijfsvoering hiervan op de hoogte te stellen. De Functionaris besteedt aandacht aan bewustwording ten aanzien van datalekken en privacywetgeving binnen de organisatie. De datalekken met bijbehorende afwegingen, correspondentie en besluiten worden vastgelegd in een datalekregister.

7. Evaluatie en rapportage

7.1 Evaluatie

Bij de evaluatie van Privacy beleid wordt aandacht besteed aan:

- De effectiviteit van de geïmplementeerde maatregelen;

- De aansluiting van het beleid bij de nieuwe privacy-eisen van de organisatie;
- De effectiviteit van het beleid;
- Bovenstaande bevindingen kunnen leiden tot aanpassingen in maatregelen, procedures, processen of beleid.

7.2 Rapportage

Jaarlijks levert de Functionaris gegevensbescherming een rapport op met de status van het voldoen aan de Privacywetgeving. Dit rapport wordt aan het College van Bestuur en de directeur Bedrijfsvoering gepresenteerd. De daaruit volgende verbeter- en ontwikkelpunten worden in het jaarplan voor het volgende jaar verwerkt.