

Generieke gedragscode voor de verwerking van persoonsgegevens en vertrouwelijke informatie

Inhoud

1.	Situering en doelstelling van dit document.....	2
2.	Definities.....	2
3.	Wettelijk kader	4
4.	Toepassingsgebied.....	4
4.1.	Materieel toepassingsgebied.....	4
4.2.	Personeel toepassingsgebied	4
5.	Gedragscode.....	5
5.1.	Na te leven beginselen inzake Verwerking van persoonsgegevens	5
5.1.1.	'Rechtmatigheid, behoorlijkheid en transparantie':.....	5
5.1.2.	'Doelbinding' (finaliteitsprincipe en verenigbaarheid)	6
5.1.3.	'Minimale gegevensverwerking' (Principe van proportionaliteit en subsidiariteit)	6
5.1.4.	'Juistheid'.....	6
5.1.5.	'Opslagbeperking'	7
5.1.6.	Verwerking van bijzondere categorieën van Persoonsgegevens.....	7
5.1.7.	'Vertrouwelijkheid en Integriteit '	7
5.1.8.	(Zelf)Verantwoordingsplicht.....	7
5.2.	Gebruik van IT-toepassingen en IT-middelen	8
5.3.	Meedelen van Persoonsgegevens en/of Vertrouwelijke informatie	8
6.	Toepassingen.....	9
7.	Naleving.....	11
8.	Functionaris gegevensbescherming	11

Generieke gedragscode voor de verwerking van persoonsgegevens en vertrouwelijke informatie

1. Situering en doelstelling van dit document

Privacy is belangrijk en vereist ieders zorg. De eerbiediging van het privé-, familie- en gezinsleven, huis en briefwisseling behoort tot de fundamenteën van ieders persoonlijke levenssfeer.

Ook aan de verwerking van persoonsgegevens dient met de steeds verdergaande digitalisering van onze maatschappij bijzondere aandacht besteed te worden.

De Algemene Verordening Gegevensbescherming (AVG of General Data Protection Regulation of GDPR;) biedt hiervoor het wettelijk kader en stimuleert de opmaak van gedragscodes die de toepassing van de AVG expliciteren.

Het Bestuurscollege keurde eerder reeds een ‘Gedragscode voor Informatiebeheerders’¹ goed die richtsnoeren bevat met betrekking tot ethische integriteit van de informatiebeheerder en de integriteit van een computersysteem, informatiebescherming en informatieplicht.

Het voorliggende document legt een gedragscode op voor de verwerking van persoonsgegevens aan HOGENT vanuit de optiek van de AVG, alsook de verwerking van vertrouwelijke informatie in het algemeen binnen HOGENT. De verplichting om de AVG na te leven berust immers niet alleen bij de (eind)verantwoordelijke van de verwerking, met name de HOGENT; ook alle medewerkers zijn mede verantwoordelijk voor een correcte naleving van de AVG.

2. Definities

De hierna en hiervoor in deze gedragscode vermelde met een hoofdletter geschreven begrippen, hebben de volgende betekenis:

1. **Persoonsgegevens:** alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke levende persoon (deze persoon wordt in de AVG de **Betrokkene** genoemd).

Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

¹ Zie BC/B/2018/FICT/61320

Van de 'gewone' persoonsgegevens² onderscheiden zich de 'bijzondere categorieën van persoonsgegevens'. Met deze laatste worden bedoeld: persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, alsook persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten.

- 2. Verwerking:** een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Met andere woorden: elke manipulatie van persoonsgegevens kan als Verwerking beschouwd worden.

- 3. Gebruiker:** elke persoon (lesgever, student, HOGENT-medewerker, externe,...) die op een of andere manier Verwerkingen van Persoonsgegevens en/of Vertrouwelijke informatie uitvoert, in het bijzonder iemand die toegang heeft tot één of meerdere functionaliteiten binnen een Toepassing.
- 4. Toepassing:** Een IT-systeem ter ondersteuning van processen en/of activiteiten binnen de HOGENT.
- 5. Toepassingseigenaar:** de persoon of instantie die voor een Toepassing het doel en de middelen bepaalt, en die tevens beslist welke Gebruikers op welke wijze toegang krijgen tot de Toepassing en welke informatie zij kunnen raadplegen.
- 6. Vertrouwelijke informatie:** Alle informatie die hetzij:
- op grond van een wettelijke of reglementaire grond als vertrouwelijk wordt beschouwd;
 - van die aard is dat door de bekendmaking ervan de financiële, economische, of commerciële belangen van HOGENT geschaad worden of het vertrouwelijk karakter van de relatie met een andere instelling of instantie kan schaden;
 - opgenomen is in een voorbereidend document voor advies-, overleg- of bestuursinstanties van HOGENT en informatie bevat zoals omschreven onder a) of b) waarvan de vertrouwelijkheid tijdelijk doch noodzakelijk is in de fase van conceptuele denkoefeningen en visieontwikkelingen over instellingsbrede thema's en dossiers;
 - berust op een vertrouwensrelatie tussen individuen;
 - door iemand uitdrukkelijk als 'vertrouwelijk' wordt bestempeld;

² Dit zijn bv. identificatiegegevens, financiële gegevens, fysieke gegevens, leefgewoonten, psychische gegevens, samenstelling van het gezin, vrijetijdsbesteding en interesses, lidmaatschappen, consumptiegewoonten, woningkenmerken en/of (ver)huurgegegevens, opleiding en vorming, beroep en betrekking, beeld- en / of geluidsopnamen, gerechtelijke gegevens (géén strafrechtelijke).

- f) door de persoon die rechtmatig over deze informatie beschikt, onderworpen is aan redelijke maatregelen om deze, gezien de omstandigheden, geheim te houden omdat de belangen, of de naam en/of faam van betrokkene kan geschaad worden door de bekendmaking ervan;
- g) tot de persoonlijke levenssfeer behoren, tenzij deze informatie vrijwillig door de betrokkene wordt verspreid zonder aanspraak te maken op vertrouwelijkheid.

3. Wettelijk kader

Het wettelijk kader voor de Verwerking van persoonsgegevens en vertrouwelijke informatie wordt bepaald door:

- Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming, Publicatieblad van de Europese Unie, L119, 59e jaargang, 4 mei 2016, met haar wijzigingen en uitvoeringswetgeving;
- Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (BS 18/3/1993), samen met alle amendementen en uitvoeringsbesluiten.

In geval van tegenstrijdigheid tussen deze gedragscode en voornoemde wetgeving, zal de wetgeving van toepassing zijn, waarbij de Europese verordening voorrang heeft op de Belgische wet.

4. Toepassingsgebied

4.1. Materieel toepassingsgebied

Deze gedragscode geldt t.a.v. iedere Verwerking van Persoonsgegevens en Vertrouwelijke informatie, of deze nu gebeurt via een geheel of gedeeltelijke geautomatiseerde verwerking, dan wel om een handmatige verwerking.

4.2. Personeel toepassingsgebied

De voorliggende gedragscode is van toepassing t.a.v. alle personen die Persoonsgegevens of Vertrouwelijke informatie verwerken in het kader van activiteiten die binnen de werkingssfeer van HOGENT vallen.

Het gaat dus om:

1. Medewerkers die een statutaire en/of contractuele arbeidsrelatie hebben met HOGENT;
2. Onbezoldigde medewerkers, studenten of andere personen die geen contractuele arbeidsrelatie hebben met HOGENT.

Voor deze groep mensen zal de verantwoordelijkheid voor een rechtmatige verwerking van Persoonsgegevens en Vertrouwelijke informatie geregeld worden in een specifieke overeenkomst waarin de persoon in kwestie aan voorliggende gedragscode gebonden wordt.

In sommige gevallen wordt voor de Verwerking van Persoonsgegevens een beroep gedaan op een externe dienstverlener. In dat geval bepaalt de verantwoordelijke voor de Verwerking het doel en de middelen voor deze Verwerking en handelt de verwerker in opdracht van de verantwoordelijke voor de Verwerking op basis van schriftelijke instructies. In dergelijk geval dient een **verwerkersovereenkomst** te worden afgesloten. De inhoud daarvan wordt bepaald door de AVG.

Het afsluiten van dergelijke overeenkomst is enkel mogelijk via tussenkomst van de functionaris gegevensbescherming van HOGENT.

Omgekeerd is het mogelijk dat een externe persoon / instantie voor de Verwerking van Persoonsgegevens een beroep doet op HOGENT in opdracht van deze externe persoon / instantie met schriftelijke instructies; hierbij treedt HOGENT op als verwerker.

Ook hier dient een verwerkersovereenkomst te worden afgesloten en dit via tussenkomst van de functionaris gegevensbescherming.

5. Gedragscode

5.1. Na te leven beginselen inzake Verwerking van persoonsgegevens³

5.1.1. 'Rechtmatigheid, behoorlijkheid en transparantie':

Elke Verwerking van persoonsgegevens en/of Vertrouwelijke informatie dient te gebeuren met respect voor de toepasselijke regelgeving. Tevens dient voor elke Verwerking een rechtsgrond aanwezig te zijn (*cf. infra*). De persoon die instaat voor de Verwerking legt hierbij de nodige integriteit⁴ aan de dag en zorgt voor de nodige transparantie t.a.v. Betrokkenen.

Onder 'rechtmatigheid' wordt ook verstaan dat er een wettelijke grondslag of rechtsgrond moet zijn die de Verwerking rechtvaardigt.

Voor de Verwerking van Persoonsgegevens dient de Gebruiker minstens één van volgende zes rechtsgronden aan te tonen⁵:

- 1° betrokkene heeft **toestemming** gegeven voor de Verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden; die toestemming moet vrij, specifiek, op informatie berustend en ondubbelzinnig gegeven zijn (*deze voorwaarden dienen cumulatief begrepen te worden*);

³ Zie art. 5 AVG

⁴ Zie ook BC/B/2018/FICT/61320, punt 2:

De informatiebeheerder:

- stelt zich objectief en onpartijdig op in de uitvoering van zijn werk;
- streeft ernaar persoonlijke belangenconflicten te vermijden; wanneer deze zich voordoen licht hij/zij zijn/haar oversten in;
- zal zijn vaardigheden steeds op een gepaste wijze ten dienste stellen van de hogeschool en de gebruikers van IT-systemen;
- streeft ernaar in de best mogelijke verstandhouding samen te werken met iedereen binnen de hogeschool;
- vermijdt foutieve voorstellingen van zijn/haar capaciteiten te geven en zal wanneer dit nodig blijkt, professionele hulp inroepen voor technische bijstand;
- zal een voortdurende inspanning leveren om op de hoogte te blijven van de stand van de techniek en van de maatschappelijke aangelegenheden die een impact hebben op de manier waarop hij/zij zijn/haar functie uitoefent.

⁵ Zie art. 6 AVG

- 2° de Verwerking is **noodzakelijk** voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
- 3° de Verwerking is **noodzakelijk** om te voldoen aan een **wettelijke verplichting** die op de verwerkingsverantwoordelijke rust;
- 4° de Verwerking is **noodzakelijk** om de **vitale belangen** van de betrokkene of van een andere natuurlijke persoon te beschermen;
- 5° de Verwerking is **noodzakelijk** voor de vervulling van een taak van **algemeen belang** of van een taak in het kader van de **uitoefening van het openbaar gezag** dat aan de verwerkingsverantwoordelijke is opgedragen;
- 6° de Verwerking is **noodzakelijk** voor de behartiging van de **gerechtvaardigde belangen** van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

5.1.2. 'Doelbinding' (finaliteitsprincipe en verenigbaarheid)

Gebruikers mogen enkel Persoonsgegevens verwerken voor welbepaalde en gerechtvaardigde doeleinden. Deze doeleinden dienen vooraf duidelijk vastgelegd zijn. De Gebruikers mogen vervolgens deze Persoonsgegevens niet verder verwerken voor een ander doel dat niet verenigbaar is met het doel waarvoor de persoonsgegevens zijn verzameld.

Andere, bijkomende Verwerkingen zijn dus in principe niet toegelaten; uitzonderingen hierop vormen bijkomende Verwerkingen in het kader van daartoe voorziene wetgeving of reglementen (bv. in het kader van wetenschappelijk of historisch onderzoek, statistische doeleinden, archivering in het algemeen belang, ...)

5.1.3. 'Minimale gegevensverwerking' (Principe van proportionaliteit en subsidiariteit)

Gebruikers mogen enkel Persoonsgegevens gebruiken wanneer deze toereikend zijn, ter zake dienend en beperkt tot wat **noodzakelijk** is voor de doeleinden waarvoor zij worden verwerkt.

Zij mogen niet méér gegevens verwerken dan **noodzakelijk** voor de vastgestelde doeleinden ('need to know' ipv 'nice to know'; d.i. het principe van de *proportionaliteit*).

Persoonsgegevens mogen alleen verwerkt worden wanneer het doel van de Verwerking niet redelijkerwijs op een andere manier kan gerealiseerd worden (*subsidiariteit*).

Bij voorkeur en waar mogelijk wordt gewerkt met geanonimiseerde gegevens (geen mogelijkheid meer tot identificeren). Indien door anonimisering het beoogde doel niet kan bereikt worden, dient met gepseudonimiseerde gegevens (versleutelde gegevens die door gebruik van de sleutel wel tot identificatie kunnen leiden) gewerkt te worden.

Ruwe Persoonsgegevens mogen gebruikt worden wanneer het vooropgestelde doel niet kan bereikt worden door anonimisering of pseudonimisering.

5.1.4. 'Juistheid'

Gebruikers dienen erover te waken dat de Persoonsgegevens juist zijn en zo nodig worden geactualiseerd. Gebruikers nemen alle redelijke maatregelen om de persoonsgegevens die onjuist zijn, onverwijld te wissen of te rectificeren.

5.1.5. 'Opslagbeperking'

Gebruikers mogen Persoonsgegevens niet langer bewaren in een vorm die het mogelijk maakt de betrokkenen te identificeren dan noodzakelijk voor de doeleinden waarvoor de persoonsgegevens worden verwerkt. Dit betekent dat de **bewaartermijn** van Persoonsgegevens dient te worden vastgelegd conform wettelijke bepalingen en toepasselijke overeenkomsten, en dat de bewaartermijnen in overeenstemming zijn met de vooropgestelde doelstelling.

Persoonsgegevens mogen enkel voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt. Na het verstrijken van de bewaartermijn dienen de Persoonsgegevens op een veilige manier gewist te worden.

5.1.6. Verwerking van bijzondere categorieën van Persoonsgegevens

In principe is de Verwerking van de bijzondere categorieën van Persoonsgegevens (cfr. *supra* punt. 2) **verboden**, tenzij wanneer voldaan is aan één van de in de AVG voorziene uitzonderingen⁶. Deze uitzonderingen situeren zich o.m. in de context van arbeidsrecht, sociaal zekerheidsrecht, of van preventieve of arbeidsgeneeskunde; of wanneer de Betrokkene uitdrukkelijke toestemming heeft gegeven of kennelijk zelf de Persoonsgegevens openbaar heeft gemaakt; of wanneer vitale belangen van de Betrokkene of andere natuurlijke personen dienen beschermd te worden.

5.1.7. 'Vertrouwelijkheid en Integriteit'

Alle Gebruikers zijn ertoe gehouden om op een confidentiële wijze om te gaan met Persoonsgegevens en/of Vertrouwelijk informatie. Van Gebruikers wordt verwacht dat zij alle mogelijke redelijke maatregelen nemen om de vertrouwelijkheid en integriteit van de verwerkte gegevens te garanderen.

Vanuit deze optiek dienen zij erover te waken dat zij Persoonsgegevens verwerken met een passende beveiliging, zodat deze beschermd zijn tegen ongeoorloofde of onrechtmatige Verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Elke Gebruiker waakt over de integriteit van de apparatuur die voor de Verwerking wordt gebruikt (bv. bescherming tegen diefstal, verlies, beschadiging en vernietiging).

Wanneer een Gebruiker een datalek⁷ vaststelt, dient dit onmiddellijk gemeld worden via de daartoe voorziene procedure.

5.1.8. (Zelf)Verantwoordingsplicht

Als verwerkings(eind)verantwoordelijke dient de HOGENT aan te tonen dat de Verwerkingen van Persoonsgegevens voldoen aan de regels van de AVG. Daarnaast draagt elke Gebruiker ook **mede-verantwoordelijkheid** voor de Verwerking van Persoonsgegevens, en wordt van de Gebruikers verwacht dat zij hun verantwoordelijkheid opnemen om de beginselen van de AVG na te komen en deze Verwerkingen op een rechtmatige en veilige manier laten verlopen.

⁶ Art. 9 en 10 AVG

⁷ Een datalek is een (technisch of fysisch) beveiligingsincident waarbij persoonsgegevens mogelijk verloren zijn gegaan, gewijzigd zijn of onbedoeld toegankelijk waren voor derden.

Eén van de manieren om tegemoet te komen aan de verantwoordingsplicht is het bijhouden van een **gegevensverwerkingsregister**. Hierin worden alle processen waarbij Persoonsgegevens worden verwerkt geïnterpreteerd. Voor wat betreft de faculteiten, de School of Arts, het Interfacultair Centrum voor Ondernemen, de entiteit GO5, de directies en diensten van het servicecenter wordt dit per organisatie-entiteit opgemaakt.

Gezien de specificiteit van Verwerkingen van (persoons)gegevens door onderzoekers (zowel op niveau van de aard en de categorieën van Persoonsgegevens, als op het vlak van de categorieën en het aantal betrokkenen, de eventuele ontvangers, en verschillende risicograad) wordt elk onderzoeksproject waarbij Persoonsgegevens worden verwerkt, als een afzonderlijk Verwerking aanzien die apart wordt geregistreerd. Voor de opmaak en het bijhouden van het gegevensverwerkingsregister, kan het advies worden ingewonnen van de functionaris gegevensbescherming.

5.2. Gebruik van IT-toepassingen en IT-middelen

De toegang tot IT-Toepassingen is strikt persoonlijk via de HOGENT-account, of via een persoonlijke toepassings-specifieke niet-HOGENT account voor het gebruik en beheer van IT-Toepassingen, of via specifieke accounts voor externe gebruikers.

Iedere Gebruiker staat in voor de bescherming van zijn/haar persoonlijk account en volgt daarbij de richtlijnen die hiertoe door de dienst IT worden opgelegd.

Logingegevens mogen niet doorgegeven worden.

De Gebruiker is verantwoordelijk voor wat er onder de account gebeurt, tenzij de Gebruiker ondanks gepaste zorg zelf het slachtoffer is van misbruik van de betreffende account.

De Gebruikers zijn ertoe gehouden de richtlijnen van de dienst IT mbt. het veilig gebruik IT-infrastructuur en IT-middelen strikt na te leven.

Wie vaststelt verkeerdelijk toegang te hebben tot een IT-Toepassing, dient dit onmiddellijk te melden aan de helpdesk van de dienst IT. Evenzo moet een rechtmatige gebruiker die vaststelt toegang te hebben tot ruimere functionaliteiten dan welke normaliter voorzien zijn voor zijn of haar respectieve rol, dit melden aan de helpdesk van de dienst IT.

5.3. Meedelen van Persoonsgegevens en/of Vertrouwelijke informatie

Persoonsgegevens en/of Vertrouwelijke informatie kunnen niet zomaar of zonder rechtsgrond overgemaakt worden aan derden.

Dit betekent ook dat derden geen inzage hebben in Persoonsgegevens en/of Vertrouwelijke informatie, tenzij

- 1° daarvoor een wettelijk kader is (bv. op grond van een gerechtelijk bevel, ten behoeve van de openbaarheid van bestuur,...);
- 2° ingeval de vertrouwelijke informatie berust op een vertrouwensrelatie tussen individuen en de betrokkene of de persoon ten aanzien van wie de vertrouwelijkheidsverplichting geldt, uitdrukkelijke toestemming geeft om inzage te verlenen.

Wanneer Persoonsgegevens (systematisch) aan derden worden doorgegeven, zal HOGENT in de Privacyverklaring duidelijk vermelden, om welke Verwerkingen en welke Persoonsgegevens het gaat, alsook de doelstelling en de rechtsgrond.

Persoonsgegevens kunnen niet doorgegeven worden voor commerciële of publicitaire doeleinden.

HOGENT kan Persoonsgegevens en/of Vertrouwelijke informatie wel doorgeven aan derden wanneer de Betrokkene daartoe op basis van specifieke en correcte informatie, ondubbelzinnig en vrij toestemming heeft gegeven.

Het verschaffen van informatie mbt aanvragen tot openbaarmaking, verbetering of aanvulling van bestuursdocumenten en het antwoorden op vragen mbt. het uitoefenen van het recht op inzage, zal steeds gebeuren door de communicatieambtenaar c.q. de functionaris gegevensbescherming.

6. Toepassingen

De naleving van deze Gedragscode dringt zich op ten aanzien van:

1° Gebruikers van administratieve Toepassingen

Alle HOGENT medewerkers die met Persoonsgegevens werken en daarvoor een beroep doen op (een) administratieve Toepassing(en), dienen deze Gedragscode na te leven, met bijzondere aandacht voor de bepalingen m.b.t. het gebruik van IT-Toepassingen en IT-middelen (cfr. supra 5.2).

Worden met Gebruikers van administratieve Toepassingen bedoeld: medewerkers van de diensten personeelsadministratie, HR, financiën, studentenaangelegenheden, leernetwerken, kwaliteitsborging, onderwijsontwikkeling, studentenvoorzieningen, decanaats- en secretariaatsmedewerkers,...

Gebruikers van Toepassingen dienen de vertrouwelijkheid te eerbiedigen van de Persoonsgegevens waarmee zij in contact komen door gebruik van de Toepassing. Enkel de Verwerkingen van Persoonsgegevens die noodzakelijk zijn voor de uitvoering van de overeenkomst met de Betrokkene, of voor de uitvoering van de decretale opdracht van HOGENT zijn toegelaten.

Indien een Gebruiker niet meer de functie uitoefent waarvoor hij/zij gebruiksrechten heeft op een Toepassing, dient de leidinggevende dit te melden aan de Toepassingseigenaar, zodat de gebruiksrechten kunnen aangepast worden.

2° IT-medewerkers en beheerders van IT-Toepassingen

IT-medewerkers en beheerders van IT-Toepassingen hebben uitgebreide mogelijkheden voor toegang tot IT-toepassingen en de achterliggende data en persoonsgegevens. Bij uitbreiding van de toepassing van de gedragscode voor informatiebeheerders⁸, dienen zij voorliggende gedragscode na te leven.

Meer specifiek dient bijzondere aandacht besteed te worden aan onderstaande punten:

- Gebruik van een persoonlijk account van andere Gebruikers

Werken met de persoonlijke account van een Gebruiker is niet geoorloofd, tenzij in het kader van ondersteuningsactiviteiten van de IT-Helpdesk.

⁸ BC/B/2018/FICT/61320

Deze ondersteuning, waarbij de IT-medewerker dan wel toegang heeft tot het persoonlijk account van de Gebruiker, kan dan gebeuren op twee manieren:

- de IT-medewerker biedt ondersteuning in het bijzijn van de Gebruiker nadat de Gebruiker zelf heeft ingelogd in de Toepassing;
- De Gebruiker geeft toestemming aan de IT-medewerker om het scherm over te nemen.

- Persoonlijke mailbox

Zonder expliciete toestemming van de Gebruikers mag de ICT-medewerker geen kennis nemen van de persoonlijke mailbox en/of de persoonlijke bestanden die zich op de persoonlijke schijfruimte van de Gebruikers bevinden.

In uitzonderlijke omstandigheden is de toegang tot privé gegevens slechts mogelijk op gerechtelijk of politieel bevel.

- Gegevensbeschermingseffectenbeoordeling

Wanneer er bij de ontwikkeling van applicaties er een kans is dat een Verwerking een waarschijnlijk hoog risico kan inhouden voor de rechten en vrijheden van Betrokkenen, dient een gegevensbeschermingseffectenbeoordeling te worden uitgevoerd. Hiertoe wordt verplicht het advies ingewonnen van de functionaris gegevensbescherming.

- Logging en monitoring

Het gebruik van Toepassingen via de ICT-infrastructuur van HOGENT wordt gemonitord en gelogd. De toegang tot Persoonsgegevens is slechts mogelijk overeenkomstig deze gedragscode en na het verplicht in te winnen advies van het diensthoofd van de Juridische Dienst en/of de functionaris gegevensbescherming.

3° Leden van het Onderwijzend Personeel

Vermits puntenlijsten, aanwezigheidslijsten, alle vormen van evaluatie, bijhouden van contactgegevens van personen uit een netwerk of van alumni,... als Persoonsgegevens dienen beschouwd te worden, is de AVG, mede vanuit de optiek van mede-verantwoordelijkheid van toepassing op de leden van het Onderwijzend Personeel, en is deze Gedragscode ook voor hen bindend.

Zo dient o.m. bijzondere aandacht besteed te worden aan:

- het opmaken / bewerken van 'gedeelde puntenlijsten': aanbevelen wordt om dit te doen in de Office 365 omgeving ipv. mailen of gebruik van (onbeveiligde) USB-sticks;
- de bewaartermijnen voor bijhouden van contactgegevens, persoons- en evaluatiegebonden activiteiten, portfolio's, enz. van studenten;
- het gebruik van gegevensbanken van contactpersonen binnen het eigen netwerk van het vakgebied; deze gegevens mogen niet zomaar doorgegeven worden of gebruikt voor andere, niet met de oorspronkelijke doelstelling verenigbare, doelstellingen.

4° Onderzoekers

Naast de verantwoordingsplicht die ook op onderzoekers rust (cfr. supra: de registratie van verwerkingsactiviteiten in het gegevensverwerkingsregister), kunnen onderzoekers in het bijzonder gevat worden door deze gedragscode aangezien het bij het onderzoek gevoelige gegevens verwerkt worden of wanneer het onderzoek over kwetsbare groepen gaat.

Vanuit die optiek verdienen gegevensbescherming en informatieveiligheid een bijzondere aandacht, vooral onder meer op het vlak van

- risico-analyse en –beheersing; in overleg met de functionaris gegevensbescherming kan desgevallend een gegevensbeschermings-effectenbeoordeling uitgevoerd worden
- transparantie naar de betrokkenen over de Verwerking van de Persoonsgegevens
- dataminimalisatie
- anonimisering en/of pseudonimisering
- verwerkings-, bewarings-, en vernietigingsstrategie

Voor bepaalde directies/diensten kunnen in bepaalde gevallen en binnen een bepaalde context bijkomende en specifieke richtlijnen, procedures,... uitgewerkt worden die deze Gedragscode expliciteren. Ook deze bijkomende richtlijnen dienen nageleefd te worden.

7. Naleving

Elke Gebruiker is ertoe gehouden om de voorliggende gedragscode na te leven. HOGENT dient in te staan voor acties voor bewustmaking en responsabilisering in het kader van deze gedragscode, voor het communiceren en verder concretiseren in richtlijnen en procedures, en voor de ondersteuning van de Gebruikers bij de naleving ervan.

Iedere Gebruiker draagt een mede-verantwoordelijkheid bij het naleven van deze Gedragscode. Het niet-naleven van deze Gedragscode kan leiden tot formele (re)acties (waaronder tuchtsancties, sancties in de arbeidsrechtelijke sfeer,...) wanneer blijkt dat het gedrag als sanctioneerbaar wordt beschouwd.

Wanneer er een risico bestaat dat bij een Verwerking van Persoonsgegevens rechten en vrijheden van betrokkenen worden geschonden, dient het advies van de functionaris gegevensbescherming te worden ingewonnen.

8. Functionaris gegevensbescherming

De functionaris gegevensbescherming is het *single point-of-contact* bij het verstrekken van advies ivm verplichtingen van de AVG in het algemeen, en het interpreteren van deze gedragscode alsook het oplossen van problemen en adviesverstrekking van bijzondere situaties mbt. deze gedragscode in het bijzonder.

Tevens is de functionaris gegevensbescherming gemachtigd om toe te zien op de naleving van de toepassing van de AVG en de Verwerking van Persoonsgegevens in HOGENT, alsook van de naleving van deze gedragscode. Vanuit die optiek kunnen audits georganiseerd worden.