UNIVERSITEIT GENT

GENERIEKE GEDRAGSCODE VOOR DE VERWERKING VAN PERSOONSGEGEVENS EN ANDERE VERTROUWELIJKE INFORMATIE

(goedgekeurd door het Bestuurscollege van 18 mei 2018 en gewijzigd op 1 september 2023)

Inhoudsopgave

1. DOELSTELLING VAN DIT DOCUMENT

Dit document legt een generieke gedragscode vast voor de verwerking van persoonsgegevens aan de Universiteit Gent (hierna de UGent) door middel van IT-toepassingen. Bij uitbreiding geldt deze gedragscode ook voor manuele verwerkingen van persoonsgegevens aan de UGent, en eveneens voor de verwerking van andere vertrouwelijke informatie van de UGent.

Deze gedragscode bevat onder meer regels voor geoorloofde toegang tot, en geoorloofd gebruik van dergelijke gegevens in de IT-toepassingen aan de UGent. Deze gedragscode moet daarom samen gelezen worden met het Reglement voor correct gebruik van de ICT-infrastructuur van de Universiteit Gent.

Voorliggende gedragscode kadert in het algemeen gegevensbeschermingsbeleid (het beleid voor rechtmatig en veilig verwerken van persoonsgegevens) dat aan de UGent gevoerd wordt.

Deze generieke gedragscode kan waar nodig aangevuld worden met gedragscodes toegespitst op specifieke toepassingen en verwerkingsactiviteiten.

2. DEFINITIES

In deze gedragscode worden onderstaande begrippen gebruikt met de hiernavolgende betekenis:

1° Verwerking: elke volledig of deels geautomatiseerde of handmatige handeling (bewerking of geheel van bewerkingen) met betrekking tot de gehele levensloop van gegevens: 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,… (niet exhaustieve opsomming).

2° Persoonsgegevens: elke informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (deze laatste wordt de **Betrokkene** genoemd). Deze definitie is overeenkomstig de Europese en Belgische privacywetgeving zeer ruim[1]. Hieronder vallen ook medische gegevens, zijnde elke informatie die, direct of indirect, betrekking heeft op de gezondheid of lichamelijke en/of geestelijke toestand van een natuurlijke persoon[2].

3° Vertrouwelijke informatie: informatie en data (waaronder persoonsgegevens) wordt aan de UGent beschouwd als vertrouwelijk[3] ofwel wanneer de (toepassings)eigenaar of

[1] Zie de Algemene Verordening Gegevensbescherming (AVG) Art. 4, 1): als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
[2] Zie ook de definitie van “gegevens over gezondheid” in Art. 4, 15) van de AVG: persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.
[3] Zie ook het beleidsdocument “Richtlijn voor classificatie van informatie en data” (BC van 10.7.2015

verantwoordelijke op basis van gegronde redenen aangeeft of aangemerkt heeft dat dit het geval is op basis van een nominatieve of functionele aanduiding van een kring[4]; de classificatie, en in het bijzonder het vastleggen van een nominatieve of functionele verspreidingskring, moet gebeuren op basis van een inschatting van negatieve impact van eventuele ongewenste verspreiding buiten die kring (al dan niet opzettelijk); ofwel wanneer de informatie niet als vertrouwelijk is aangemerkt, maar de ontvanger redelijkerwijze dient aan te nemen dat het om vertrouwelijke informatie gaat wegens de inhoud of de aard van de informatie, wanneer hier een wettelijke, contractuele of reglementaire grond voor is[5]; bij twijfel kan de ontvanger terugkoppelen naar de (toepassings)eigenaar of verantwoordelijke.

4° Toepassing: Een IT-systeem ter ondersteuning van processen en activiteiten aan de UGent.

5° Toepassingseigenaar: dit is de persoon die over de Toepassing de verantwoordelijkheid draagt, het doel en de middelen vastlegt, en die tevens beslist welke gebruikers(rollen) op welke wijze toegang (kunnen) krijgen tot de Toepassing en welke informatie zij kunnen raadplegen.

6° Gebruiker[6]: elke persoon (student, lesgever, UGent-medewerker, externe,…) die op een of andere manier verwerkingen van persoonsgegevens en/of andere vertrouwelijke informatie uitvoert, in het bijzonder iemand die toegang heeft tot een of meerdere functionaliteiten binnen een Toepassing.

3. WETTELIJK KADER

en geüpdatet op BC van 11.03.2022), beschikbaar via https://codex.ugent.be?regid=REG000272

[4] Zoals een eerste ontwerp van universitaire beleidsvisie of voorstel van bestuurlijk standpunt, dat vervolgens al dan niet kan uitmonden in een formele bestuurlijke besluitvorming. Het uitdrukkelijk als vertrouwelijk bestempelen van deze bestuurlijke of beleidsinformatie(dragers) (bv. door het vermelden van 'vertrouwelijk' op een nota) is in deze context steeds tijdelijk van aard. De vertrouwelijkheid kan door de Toepassingseigenaar worden opgeheven in de loop van de conceptfase, maar dient altijd te worden opgeheven vóór de formele start van het beslissingstraject waarin de verschillende stappen van advies, onderhandeling en goedkeuring achtereenvolgens worden doorlopen.

[5] Dit is met name het geval wanneer: de inhoud informatie over identificeerbare personen bevat. De vertrouwelijkheid vloeit in dit geval voort uit de inhoud van de informatie; de vertrouwelijkheid voortvloeit uit de aard van de informatie: bijvoorbeeld wanneer de ontvangen informatie valoriseerbare onderzoeksresultaten bevat; er een wettelijke grond is voor de vertrouwelijkheid: bijvoorbeeld een studentenarts die in het kader van een gedeeld beroepsgeheim informatie meegedeeld krijgt van een collega-studentenarts, is als ontvanger gebonden door het beroepsgeheim ex art. 458 Sw., en kan daar niet van worden ontslagen omdat de verzendende collega de medische informatie in kwestie niet uitdrukkelijk als vertrouwelijk heeft gelabeld; er een contractuele grond is voor de vertrouwelijkheid en er bijgevolg een contractuele vertrouwelijkheidsverplichting geldt. Bijvoorbeeld wanneer onderzoekers samenwerken met een extern bedrijf en daarvoor een confidentialiteitsovereenkomst hebben afgesloten. Deze onderzoekers zullen als ontvangende partij tot vertrouwelijkheid gehouden zijn, van degene die de informatie verzendt of deelt kan niet worden verwacht dat de verstrekte of toegankelijk gemaakte informatie uitdrukkelijk als vertrouwelijk wordt gelabeld; er een reglementaire grond geldt: er zijn bijvoorbeeld UGent-reglementen die (op onderdelen) vertrouwelijkheid voorschrijven. Bij het ontvangen van informatie die onder die vertrouwelijkheid valt, vervalt deze vertrouwelijkheid niet wanneer de verzender de informatie niet uitdrukkelijk als vertrouwelijk heeft gelabeld. Deze voorbeelden zijn niet limitatief.

[6] Het gebruik van de term "verwerker" wordt hiermee vermeden, omdat "verwerker" in de context van de privacywetgeving een andere, specifieke betekenis heeft.

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

- de Algemene Verordening Gegevensbescherming (AVG, of in het Engels: General Data Protection Regulation, GDPR). Deze Europese privacyregelgeving is rechtstreeks van toepassing sinds 25 mei 2018.

- De Belgische privacywetgeving, met name de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, 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 voor alle geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens en andere vertrouwelijke informatie.

Ze geldt ook voor handmatige verwerking van bestanden met persoonsgegevens of vertrouwelijke informatie.

Wanneer in dit document de term “gegevens” gebruikt wordt, gaat het dus over persoonsgegevens of, bij uitbreiding en indien toepasbaar, vertrouwelijke informatie.

Niet-vertrouwelijke informatie en publieke toegankelijke informatie die geen persoonsgegevens bevat, worden in deze gedragscode buiten beschouwing gelaten.

4.2. Personeel toepassingsgebied

Voorliggende gedragscode geldt voor alle personen die persoonsgegevens of andere vertrouwelijke informatie verwerken in het kader van activiteiten die binnen de werkingssfeer van de UGent vallen.

Personen waarvoor deze gedragscode bedoeld is, kunnen uiteenlopende statuten hebben:

- Medewerkers die een **statutaire of contractuele arbeidsrelatie hebben met de UGent** (bezoldigde medewerkers) worden via het Arbeidsreglement en deze gedragscode gebonden aan hun verantwoordelijkheden voor rechtmatige en veilige verwerking van persoonsgegevens en vertrouwelijke informatie.

    - Voor **onbezoldigde medewerkers**, **studenten** of andere personen die **geen contractuele arbeidsrelatie** hebben met de UGent, moet de

verantwoordelijkheid voor rechtmatige en veilige verwerking van persoonsgegevens en vertrouwelijke informatie geregeld worden in een specifieke overeenkomst waarin de persoon in kwestie aan voorliggende gedragscode gebonden wordt. In het bijzonder voor studenten moet dit gezien worden als behorende tot de algemene voorwaarden vastgelegd in het OER van de UGent.

Externe bestuurders zijn conform punt 6 van de Ethische code voor bestuurders van de UGent gebonden tot naleving van de huidige Generieke Gedragscode voor de verwerking van persoonsgegevens en vertrouwelijke informatie aan de UGent.

Bij verwerking van persoonsgegevens door externe dienstverleners moet een verwerkersovereenkomst afgesloten worden tussen deze verwerker (de "processor") en de UGent als verantwoordelijke voor de verwerking (de "controller"). In zo een verwerkersovereenkomst moet van de verwerker geëist worden dat die het informatieveiligheidsbeleid van de UGent zal naleven en in het bijzonder ook de voorliggende gedragscode.

Omgekeerd zal de UGent in bepaalde gevallen in de rol van verwerker van persoonsgegevens treden, waarbij een verwerkersovereenkomst zal moeten afgesloten worden met de (externe) verantwoordelijke voor de verwerking. Ook in dat geval kan een dergelijke verwerkersovereenkomst verwijzen naar voorliggende gedragscode.

5. GEDRAGSCODE

5.1. Principes die moeten nageleefd worden[7]

1° **"Zelfverantwoordingsplicht":** Van ieder die in het kader van activiteiten aan de UGent medeverantwoordelijkheid draagt voor de verwerking van persoonsgegevens, wordt verwacht dat hij of zij kan aantonen dat **actief verantwoordelijkheid** genomen is om de verwerking op **rechtmatige en veilige** manier te laten gebeuren. Dit houdt o.a. in dat wordt gedocumenteerd welke persoonsgegevens precies verwerkt worden en voor welke doeleinden. Dit moet door de Toepassingseigenaren en onderzoekers gebeuren in het door de UGent voorziene **register van verwerkingsactiviteiten**, pragmatisch en met minimale zorglast[8]. Wanneer de verwerking potentieel een hoog risico inhoudt, moeten de risico's en voorziene maatregelen vóór de verwerking beoordeeld en gedocumenteerd worden[9]. Het register van verwerkingsactiviteiten is het eerste hulpmiddel om in te schatten welke verwerkingen een hoog risico kunnen inhouden. Waar nodig wordt het advies ingewonnen van de Data Protection Officer van de UGent.

[7] Zie ook Art. 5 en overweging 39) van de AVG.
[8] Algemene modaliteiten overeenkomstig artikel 30 van de AVG.
Het register van verwerkingsactiviteiten aan de UGent bevat de verwerkingsactiviteiten binnen en buiten onderzoekscontext, zie https://sharepoint.ugent.be/sites/AVGRegister.
[9] In een zogenaamde gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment), overeenkomstig artikel 35 van de AVG. Zie daartoe de relevante pagina van de Gegevensbeschermingsautoriteit https://www.gegevensbeschermingsautoriteit.be/professioneel/avg/effectbeoordeling-geb.[10] Zie https://www.ugent.be/informatieveiligheid.

2° **"Vertrouwelijkheid en integriteit":** Alle gebruikers zijn er toe gehouden op een confidentiële manier om te gaan met de persoonsgegevens en/of andere vertrouwelijke informatie waartoe ze toegang hebben. Bovendien wordt van elke gebruiker verwacht alle redelijke maatregelen te nemen om de vertrouwelijkheid en de integriteit van de verwerkte gegevens te garanderen. Hij of zij staat dus mee in voor een passende beveiliging van de gegevens ter voorkoming van ongeoorloofde verspreiding. Daartoe kan teruggegrepen worden naar het informatieveiligheidsbeleid[10] van de UGent, en in het bijzonder de praktische richtlijnen voor veilig werken met IT-middelen. Elke gebruiker staat ook mee in voor de integriteit van de apparatuur die voor de verwerking wordt gebruikt, bv. bescherming tegen diefstal, verlies, beschadiging of vernietiging. Indien een gebruiker een datalek (of een ander gerelateerd incident) vaststelt, dan moet dit onmiddellijk gemeld worden aan de helpdesk van de Directie ICT, die hiervoor als centraal contactpunt fungeert.

3° **"Rechtmatigheid, behoorlijkheid en transparantie":** Elke gebruiker voert verwerkingen van persoonsgegevens en/of andere vertrouwelijke informatie uit met respect voor alle wetten, reglementen en regels die van toepassing zijn. Hij of zij legt hiervoor de nodige integriteit aan de dag. Het moet bovendien transparant zijn ten overstaan van de hiërarchische lijn en van Betrokkenen, dat de gebruiker deze gegevens verzamelt, gebruikt, raadpleegt of anderszins verwerkt.

4° **"Doelbinding" (finaliteit en proportionaliteit):** Elke gebruiker moet de specifieke doeleinden waarvoor de gegevens verwerkt worden, respecteren. Deze doeleinden moeten voor elke toepassing duidelijk vastgelegd én gedocumenteerd zijn. De verwerking moet redelijk zijn en proportioneel aan de doelstelling van elke toepassing. Ander, bijkomend en dus oneigenlijk gebruik van de gegevens is niet toegelaten. Dit houdt ook in dat gebruikers enkel toegang mogen krijgen en/of nemen op een "need-to-know" basis. Dit wordt waar mogelijk ook technisch afgedwongen. Uitzonderingen voor bijkomende of verdere verwerking kunnen enkel in het kader van daarvoor voorziene wetgeving of reglementen (bv. ten behoeve van wetenschappelijk of historisch onderzoek of statistische doeleinden, met het oog op archivering in het algemeen belang, of in het kader van voortgezet onderzoek of controlemechanismen voor wetenschappelijke integriteit).

5° **"Minimale gegevensverwerking":** Gebruikers mogen niet meer gegevens verwerken (verzamelen, consulteren,…) dan noodzakelijk voor de vastgestelde doeleinden. Persoonsgegevens mogen alleen worden verwerkt indien het doel van de verwerking niet redelijkerwijs op een andere wijze kan worden verwezenlijkt. Waar mogelijk moet met geanonimiseerde gegevens gewerkt worden. Indien daarmee het beoogde doel niet kan bereikt worden, moet met gepseudonimiseerde (ook genoemd "gecodeerde") persoonsgegevens gewerkt worden. Enkel waar correct gemotiveerd wordt dat het beoogde doel niet met geanonimiseerde of gepseudonimiseerde gegevens kan bereikt worden, mogen ruwe persoonsgegevens verwerkt worden.

6° **"Juistheid":** Gebruikers letten er met gepaste zorg op dat de gegevens die ze verwerken juist zijn en geactualiseerd. Gebruikers nemen alle redelijke maatregelen om ervoor te zorgen dat onjuiste gegevens worden gecorrigeerd, op eigen initiatief of op verzoek van

[10] Zie https://www.ugent.be/informatieveiligheid.

Betrokkenen.[11]

7° **"Opslagbeperking":** Gebruikers zorgen ervoor dat de opslagperiode/bewaartermijn van persoonsgegevens en vertrouwelijke informatie wordt vastgelegd overeenkomstig alle relevante wettelijke bepalingen en toepasselijke overeenkomsten. De opslagperiode/bewaartermijn moet daarnaast beperkt worden tot wat noodzakelijk is en in overeenstemming met de oorspronkelijke doelen. Uitzonderingen voor langere bewaring kunnen enkel in het kader van daarvoor voorziene wetgeving of reglementen (bv. ten behoeve van wetenschappelijk of historisch onderzoek of statistische doeleinden, met het oog op archivering in het algemeen belang, of in het kader van voortgezet onderzoek of controlemechanismen voor wetenschappelijke integriteit). Na afloop van de bewaartermijn moeten de gegevens volledig en op een veilige manier gewist worden, overeenkomstig de richtlijnen in het informatieveiligheidsbeleid van de UGent[12].

5.2. Gebruik van IT-toepassingen aan de UGent

Elk gebruik van IT-toepassingen is onderworpen aan het Reglement voor correct gebruik van de ICT-infrastructuur van de Universiteit Gent.

De toegang tot IT-toepassingen is strikt persoonlijk via de UGent account of via specifieke accounts voor externe gebruikers.

Elke gebruiker is verantwoordelijk voor wat er onder de account gebeurt (behalve indien de gebruiker ondanks gepaste zorg zelf slachtoffer is van misbruik van de betreffende account).

5.3. Registratie van gebruikers van IT-toepassingen

1° Bepaalde gebruikers krijgen automatisch toegang tot een IT-toepassing op basis van hun statuut of de gebruikersrollen die door de Toepassingseigenaar aangeduid werden. Binnen die toepassing mogen zij enkel toegang nemen tot de gegevens die voor hun gebruikersrol relevant zijn. Dit wordt waar mogelijk technisch afgedwongen (Rol-gebaseerde toegang overeenkomstig de principes van het minste privilege ('least privilege') en van functiesplitsing ('separation of duties')).

2° Andere personen of rollen kunnen eventueel toegang krijgen tot een toepassing op individuele basis mits akkoord van de Toepassingseigenaar. De modaliteiten hiertoe worden voor elke toepassing apart vastgelegd en gedocumenteerd.

3° Gebruikerstoegang zoals vermeld onder punt 1° wordt bij wijziging van de gebruikersrol automatisch aangepast of opgeheven via een geautomatiseerd procedé. Gebruikerstoegang zoals vermeld onder punt 2° wordt waar nodig zo snel mogelijk aangepast of opgeheven onder de verantwoordelijkheid van de Toepassingseigenaar, overeenkomstig een daarvoor vastgelegde procedure[13].

---

[11] De mogelijkheid daartoe wordt bekendgemaakt aan Betrokkenen, bv. via een informatieformulier voor deelname aan wetenschappelijk onderzoek of via een online privacy notice.
[12] Zie https://www.ugent.be/informatieveiligheid.
[13] De Toepassingseigenaar is verantwoordelijk voor het vastleggen en (laten) naleven van die procedure.

4° Om de juistheid van het gebruikersbeheer te verifiëren worden periodieke controles uitgevoerd door of in opdracht van de Toepassingseigenaar en/of de Data Protection Officer van de UGent.

5° Een aantal gebruikers met meerdere rollen zullen op basis van die verschillende rollen die zij binnen de UGent vervullen een ruimere toegang hebben tot informatie. Zo kan bv. een gebruiker op basis van zijn/haar gebruikersprofiel toegang hebben tot de gegevens van één specifieke vakgroep. Indien deze gebruiker ook lid is van de Raad van Bestuur, dan zal zijn/haar gebruikersprofiel toelaten om bestuurlijke informatie UGent-breed te bekijken. Dergelijke gebruikers met meerdere rollen worden geacht de nodige deontologische integriteit aan de dag te leggen om de beschikbare informatie enkel te gebruiken overeenkomstig de correcte finaliteit en proportionaliteit binnen hun respectievelijke rollen.

6° Wie vaststelt verkeerdelijk toegang te hebben tot een IT-toepassing terwijl hij of zij niet behoort tot de onder punt 1° of 2° vermelde toegelaten gebruikers, dient dit onmiddellijk te melden aan de helpdesk van de Directie ICT, met eventueel kopie aan de Toepassingseigenaar. 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 directie ICT, met eventueel kopie aan de Toepassingseigenaar.

5.4. Mededeling van persoonsgegevens of vertrouwelijke informatie

1° Derden – waaronder ook overheden, (semi)publieke instanties en organisaties – hebben geen recht op inzage in persoonsgegevens of vertrouwelijke informatie van de UGent tenzij daarvoor een wettelijk of bestuurlijk kader[14] bestaat.

Wanneer persoonsgegevens systematisch worden doorgegeven aan derden zal de Toepassingseigenaar erop toezien dat de privacyverklaring (‘privacy notice’) van de toepassing in kwestie aangeeft om welke persoonsgegevens het gaat, en aan welke verwerking ze zullen worden onderworpen door die derden.
Persoonsgegevens mogen nooit doorgegeven worden voor commerciële of publicitaire doeleinden, noch worden doorgegeven aan derden die deze gegevens voor dergelijke doeleinden zouden gebruiken.

2° Met toestemming van de Betrokkene mag de UGent wel gegevens doorgeven of openbaar maken. Dit kan enkel indien de Betrokkene zelf op schriftelijke of elektronische wijze en op

[14] Dergelijk kader bestaat bijvoorbeeld voor (niet limitatieve opsomming):
- het opvragen van bestuursdocumenten ten behoeve van de openbaarheid van bestuur (Openbaarheidsdecreet: Decreet van 26 maart 2004 betreffende de openbaarheid van bestuur, B.S. 1 juli 2004)
- het opvragen van archiefdocumenten (Archiefdecreet: Decreet van 9 juli 2010 betreffende de bestuurlijk- administratieve archiefwerking, B.S. 5 augustus 2010 en de bepalingen inzake toegankelijkheid, openbaarheid en raadpleegbaarheid vervat in het Huishoudelijk reglement voor de archiefdienst van de Universiteit Gent).
- het opvragen van gegevens op basis van een gerechtelijk bevel in het licht van een politioneel of gerechtelijk onderzoek
- het opvragen van gegevens door de Veiligheid van de Staat (Federale Overheidsdienst Justitie).

basis van specifieke en correcte informatie de toelating heeft gegeven tot het op een bepaalde wijze doorgeven of openbaar maken van zijn of haar persoonsgegevens. Enkel de Betrokkene zelf kan deze toelating verlenen.

3° Om opzettelijke en onopzettelijke datalekken te vermijden verloopt het toegang geven tot, of de mededeling van persoonsgegevens of vertrouwelijke informatie van de UGent aan derden enkel via daartoe voorziene officiële procedures (bv. in het kader van openbaarheid van bestuur).

6. TOEPASSINGEN EN VOORBEELDEN

6.1. (ICT-)medewerkers

Sommige medewerkers[15] kunnen om technische redenen zeer uitgebreide mogelijkheden hebben om de interne werking van toepassingen te kennen en ook de daarmee geassocieerde data. Zij moeten daarom ten allen tijde met de nodige deontologische integriteit de voorliggende gedragscode naleven.

Enkele bijzondere aandachtspunten:

- Het is niet toegestaan de elektronische post op de persoonlijke mailbox of de niet-gedeelde bestanden (in het bijzonder die op de persoonlijke schijfruimte of "homedrive") van een andere gebruiker te lezen tenzij met diens toestemming.
- Het is niet toegelaten onder het persoonlijke account van een andere gebruiker te werken, tenzij uitzonderlijk en zeer tijdelijk voor onderhouds- of ondersteuningsactiviteiten:
  - ofwel lokaal, in het bijzijn van die gebruiker (waarbij de gebruiker zelf ingelogd heeft op het systeem)
  - ofwel van op afstand, nadat de gebruiker toestemming heeft gegeven om het scherm te laten overnemen waarbij begin en einde van de overname duidelijk wordt aangegeven door een melding op het scherm van de gebruiker[16].
- Indien gegevens van een bepaalde gebruiker door andere personen geraadpleegd moeten kunnen worden, moet ervoor gezorgd worden dat deze op gedeelde schijfruimte of in een gedeelde mailbox zitten, of moet van een andere proxy-functionaliteit gebruik gemaakt worden.
- Toegang nemen of geven tot privé-gegevens is enkel toegestaan in individuele uitzonderingsgevallen op gerechtelijk bevel of op verzoek van de Staatsveiligheid.
- Uitzonderlijke toegang tot data van personen die langdurig of definitief handelingsonbekwaam zijn (bv. in geval van zwaar ongeval, coma, overlijden,…) kan enkel overeenkomstig een specifieke procedure die hiervoor is vastgelegd.
- In toepassingen waar dat nodig geacht wordt (bv. als conclusie van een gegevens-beschermingseffectbeoordeling (“Data Protection Impact Assessment”)), moet de Toepassingseigenaar laten voorzien in bijkomende technische en/of organisatorische

[15] Het kan gaan over allerlei medewerkers, maar in het bijzonder ICT-medewerkers zoals systeembeheerders, helpdeskmedewerkers, ontwikkelaars & toepassingsbeheerders,… (niet limitatieve opsomming).
[16] Zie http://helpdesk.ugent.be/help/.

maatregelen (bv. encryptie) om de confidentialiteit van de data ook ten overstaan van de ICT-medewerkers te verhogen.

- De ICT-infrastructuur van de UGent wordt door ICT-systeembeheerders gecontroleerd (logging en monitoring) om de goede werking ervan te kunnen verzekeren en om misbruik op te sporen en te voorkomen. Opslag van en toegang tot de bijhorende gegevens kan enkel gebeuren overeenkomstig de principes van deze gedragscode. Dit betekent onder meer dat het niveau van detail van die gegevens niet meer en de bewaarduur niet langer mag zijn dan nodig zijn om het doel te bereiken.

6.2. Administratieve toepassingen

Alle medewerkers van de UGent die met persoonsgegevens in administratieve toepassingen werken, worden verondersteld kennis te nemen van deze gedragscode en ze na te leven.

Typische voorbeelden centraal zijn de personeelsadministratie, de studentenadministratie, de administratie van studentenvoorzieningen etc. Typische voorbeelden decentraal zijn de administraties van vakgroepen en faculteiten.

Voor bepaalde administratieve toepassingen kan het nuttig zijn (bv. ter verduidelijking voor de concrete toepassing) om specifieke bijkomende beleidsdocumenten of gedragscodes op te stellen[17].

6.3. Bestuurlijke en beleidsinformatie

Bestuurlijke en beleidsinformatie is alle informatie die wordt verzameld, vastgelegd en verwerkt ten behoeve van het besturen, het doen functioneren en het beheersen van de organisatie alsmede ten behoeve van het afleggen van verantwoording.

UGI is het UGent Geïntegreerd (beleids-) Informatiesysteem ter ondersteuning van de beleids- en besluitvormingsprocessen. Elke individuele UGI-toepassing stelt een afgebakend geheel van beleidsinformatie ter beschikking, gericht op een specifieke bestuurlijke doelstelling via specifieke visualisatie (bv. onderwijskwaliteitszorg, interfacultaire personeelsverdeelsleutel, etc.).

UGI verwerkt en verzamelt daartoe basisgegevens uit één of meerdere databanken van binnen en van buiten de UGent (bv. OASIS (onderwijsadministratie en studenteninformatie systeem), SAP (boekhouding, personeelszaken, gebouwen en facilitair beheer …), en publieke databases).

Elke UGI-toepassing heeft een Toepassingseigenaar (bv. beheerder, directeur of afdelingshoofd) die onder meer beslist welke beleidsinformatie nodig is binnen een UGI-toepassing (finaliteit en proportionaliteit van de UGI-toepassing) en welke gebruikersrollen op welke wijze toegang (kunnen) krijgen tot de toepassing en welke beleidsinformatie zij kunnen raadplegen.

[17] Als voorbeeld wordt hier verwezen naar de “Gedragscode voor het gebruik van het onderwijsadministratie- en studenteninformatiesysteem OASIS” (Vastgelegd bij beslissing van het BC 05/09/2013), zie https://codex.ugent.be?regid=REG000198.

Elke gebruiker van een UGI-toepassing wordt verondersteld kennis te nemen van deze gedragscode en ze na te leven.

6.4. Onderzoeksactiviteiten

Alle onderzoekers (zowel personeelsleden als Masterproef-studenten en doctoraatsstudenten) die met persoonsgegevens of andere vertrouwelijke informatie van de UGent werken, worden verondersteld kennis te nemen van deze gedragscode en ze na te leven.

De UGent draagt als instelling in beginsel de aansprakelijkheid en de eindverantwoordelijkheid voor de rechtmatige en veilige verwerking van persoonsgegevens of andere vertrouwelijke informatie . Op basis van het principe van **responsabilisering** wordt die verantwoordelijkheid echter gedeeld met de **verantwoordelijke(n) voor het onderzoek, d.i. de promotor** en/of de leider van de onderzoeksgroep en de andere deelnemers aan het onderzoek (eventueel ook studenten).

Er wordt in het bijzonder gewezen op de (**zelf-)verantwoordingsplicht** voor de verwerking van persoonsgegevens, die eigenlijk een uitgebreide documentatieplicht inhoudt (zie punt 5.1 1°). **Research datamanagement**[18] of een goede, efficiënte omgang met onderzoeksdata is een essentieel onderdeel van het onderzoeksproces. Wanneer persoonsgegevens verwerkt worden, dan zijn privacybescherming en veilige verwerking belangrijke aandachtspunten in het datamanagement. Dit kan geconcretiseerd worden in het **datamanagementplan** (zoals voor doctorandi en in sommige faculteiten voor masterproefstudenten trouwens reeds vereist wordt) en maakt tevens deel uit van het AVG of GDPR record[19].

Wat betreft gegevensbescherming en informatieveiligheid omvat datamanagement het nadenken over en/of implementeren van (niet-limitatieve opsomming):

- risicobeheersing: wat zijn de privacy- en informatieveiligheidsrisico's met betrekking tot de data ?
- transparantie: hoe worden Betrokkenen correct op de hoogte gebracht van de verwerking van hun persoonsgegevens? Hoe wordt toestemming verkregen?
- dataminimalisatie (enkel die persoonsgegevens verzamelen en/of verwerken die nodig zijn voor de onderzoeksdoelen)
- anonimiseren of pseudonimiseren van persoonsgegevens
- een veilige bewaarstrategie (incl. vastleggen van correcte bewaartermijn)
- een veilige verwerkingsstrategie
- een veilige vernietigingsstrategie (na verstrijken van de vooropgestelde bewaartermijn)

Waar nodig neemt de onderzoeker zelf het initiatief om zich voor de genoemde aspecten van gegevensbescherming en informatieveiligheid bijkomend te laten informeren en adviseren, bv. via de facultaire of centrale steunpunten voor research data management, en/of door de Data Protection Officer van de UGent, desgevallend in samenwerking met de Data Protection Officer van het UZ Gent, bv. voor de verwerking van medische gegevens.

[18] Zie https://www.ugent.be/intranet/nl/onderzoek/beleid/datamanagement.
[19] Alle verwerkingsactiviteiten binnen onderzoekscontext dienen geregistreerd te worden in het AVG Register van de UGent. Deze registratie gebeurt via dmponline.be.

7. NALEVING

Elke gebruiker is er toe verbonden om voorliggende gedragscode na te leven, onverminderd algemeen geldende regelgeving.

Het bestuur van de UGent zal passende acties voorzien voor bewustmaking en responsabilisering in het kader van deze gedragscode, voor het communiceren en uitdragen van de erin vervatte principes en informatie, voor het verder concretiseren in praktische richtlijnen en procedures, en voor de ondersteuning van alle gebruikers bij de naleving ervan.

In de eerste plaats rekent de UGent op de eigen verantwoordelijkheidszin van elke gebruiker bij het naleven van deze gedragscode.

Indien gebruikers, na voldoende te zijn ingelicht, toch afwijken van deze gedragscode kan dat aanleiding geven tot formele (re)acties wanneer het gedrag, na toetsing, als sanctioneerbaar wordt beschouwd.

Wanneer de gebruiker een contractueel of statutair personeelslid betreft, kan deze hier desgevallend op aangesproken worden in het kader van feedback- en evaluatiegesprekken.

Mogelijke maatregelen en sancties die kunnen worden genomen bij vaststelling van inbreuken op deze gedragscode en rekening houdend met de ernst van de inbreuk zijn:

- Ordemaatregelen door de rector: de tijdelijke opheffing van een account of de tijdelijke of – bij herhaalde inbreuken – permanente beperking van de toegang tot (delen van) de ICT-infrastructuur en/of IT-toepassingen (waarbij een evenwicht wordt gezocht tussen het belang van de dienst, de bescherming van de systemen en de rechten van de Betrokkene, aangezien het account in veel gevallen noodzakelijk is voor het uitvoeren van de job of voor de studies);
- Maatregelen en sancties zoals voorzien in de toepasselijke (bv. arbeidsrechtelijke) regelgeving en in de interne reglementen van de UGent, o.a. de tuchtreglementen.

8. DATA PROTECTION OFFICER

8.1. Ondersteuning

De Data Protection Officer van de UGent is het single-point-of-contact bij het interpreteren van deze gedragscode, bij vragen en opmerkingen, bij het adviseren in geval van problemen en bijzondere situaties in het kader van deze gedragscode.

8.2. Toezicht

De Data Protection Officer van de UGent is gemachtigd om toe te zien op de rechtmatige en veilige verwerking van persoonsgegevens aan de UGent. Zo kunnen door de Data Protection Officer steekproefsgewijs audits georganiseerd worden met betrekking tot aan de UGent

verwerkte persoonsgegevens.