INFORMATION GOVERNANCE RISK & COMPLIANCE REGLEMENT 2023

Aangaande Gegevensbescherming, Informatiebeveiliging en Archivering

Dit Reglement is vastgesteld door de COLLEGE VAN BESTUUR op [datum].

Dit Reglement is goedgekeurd door het College op [datum].

Dit Reglement treedt in werking op 1 januari 2023.

Inhoud

Voorwoord

Het CIO Office ondersteunt de CIO bij het voeren van de centrale regie op Informatievoorziening. De verschillende disciplines, te weten Informatiemanagement, Architectuur, Portfoliomanagement, Privacy, Security en Archivering, maken deel uit van het CIO Office. In dit Reglement wordt de Governance Information Risk & Compliance van de laatste drie disciplines in kaart gebracht.

De discipline Informatiemanagement is zowel centraal als decentraal georganiseerd via informatiemanagers in faculteiten en diensten. In dit Reglement gaat het over de discipline Informatiemanagement die centraal binnen CIO Office georganiseerd is, tenzij uitdrukkelijk staat aangegeven dat het om de Informatiemanagement in faculteiten of diensten gaat.

Dit Reglement is opgebouwd uit de navolgende onderdelen:

- Het algemene deel waarin de definities van termen uit dit Reglement worden beschreven, het risk & compliance model dat de EUR hanteert wordt uitgelegd en de wet- en regelgeving die de basis vormen voor dit Reglement (Hoofdstukken I en II)
- Het tweede deel geeft een beschrijving van de beheerstaken, de mandatering van deze taken aan de beheerders en wie de beheerstaken uitvoert die het CvB zich voorbehouden (Hoofdstuk III)
- Het derde deel vormt de interne instructie van het CIO Office, waarin tot uitdrukking komt welke de taken binnen de disciplines toekomen (Hoofdstuk VI)
- In het vierde deel worden de verantwoordelijkheden van alle stakeholders op het niveau van het College beschreven om de rolvastheid te bevorderen en om een basis te leggen voor de RASCI Matrixen (Hoofdstuk V)

Tot slot wordt voor toezichthouders beschreven op welke wijze zij hun onafhankelijk positie kunnen waarborgen ten aanzien van de signaleringstaken. Er is voor gekozen om in dit stadium alles vrij uitvoerig te beschrijven. Op deze manier is getracht een Reglement te creëren dat duidelijkheid schept voor alle betrokken functies en een volledig overzicht geeft.

De verwachting is dat via de halfjaarlijkse reviews dit Reglement en de RASCI Matrixen verfijnd zullen worden. Na verloop van tijd, als processen zijn ingebed in de organisatie, zal de noodzaak tot de uitvoerige beschrijving afnemen en mogelijk komen te vervallen.

De deadlines voor het verwerken van de halfjaarlijkse reviews zijn 15 juni en 15 december. Bijdragen voor de reviews kunnen worden ingediend bij: legal.privacy@eur.nl.

Hoofdstuk I - Algemeen

Artikel 1.1 - Begripsomschrijving

1. In dit Reglement wordt verstaan onder:

- *ABD* De Algemene Bestuursdienst van de EUR
- *Archiefwaardige informatieobject* Een informatieobject (brieven en besluiten, cijfers en rapporten, interne nota's, e-mails, websites, foto's, video's, een geluidsopname, een algoritme, een database of zelfs een applicatie) dat een relatie heeft met de uitvoering van de taken van de EUR.
- *Architectuur* de discipline Architectuur binnen het CIO Office
- *Archivering* Het geheel van beleid, proces, procedure, informatie, systeem, middelen en mensen voor het beheer en management van de aan een (werk)proces gerelateerde informatie of informatieobject.
- *Afdeling Inkoop* de afdeling Inkoop en Contractmanagement, gepositioneerd onder de dienst Real Estate & Facilities. De door het College van Bestuur aan de afdeling Inkoop toegekende rol is omschreven in het Inkoopbeleid.
- *Audit & Review Charter* document waarin staat beschreven hoe de Internal Audit & Review Functie binnen de EUR is vormgegeven
- *Autoriteit Persoonsgegevens:* de toezichthoudende autoriteit die toezicht houdt op de naleving van de Algemene Verordening Gegevensbescherming.
- AVG Algemene verordening Gegevensbescherming;
- *Awb* Algemene wet bestuursrecht;
- *BBR-EUR*: het geldende Bestuurs- en Beheersreglement EUR, zoals bedoeld in art. 9.4 van de Wet;
- *Beheer*: geheel van besluiten en beschikkingen, verrichtingen en handelingen waarmee uitvoering wordt gegeven aan het beleid met betrekking tot de verkrijging en beschikbaarstelling van de financiële middelen, de aanschaf, de verzorging en het onderhoud van de materiële middelen, alsmede de inzet van het Personeel en de doelmatige en rechtmatige aanwending van deze middelen, zoals beschreven in art. 1.1 lid 1 BBR-EUR;
- *Beheerder*: diegene, die in opdracht, in naam en onder verantwoordelijkheid van het College is belast met de uitvoering van taken op het gebied van het Beheer,
- *Beheerregime* Het onder architectuur, risico gebaseerd en volgens (internationale) standaarden (o.a. NEN-ISO, HORA, HOSA) en kaders ontworpen regime voor het borgen van de duurzame toegankelijkheid van de informatieobjecten van de EUR.
- *Beheerseenheid*: een door het College ingestelde organisatorische

	eenheid, waarbinnen het Beheer door de Beheerder wordt gevoerd, zoals bedoeld in art. 1.1 lid 1 BBR-EUR
- *Beheerinstructie*	de nadere regeling per beheereenheid als bedoeld in art. 42 van het BBR-EUR
- *Besluit(en)*	een schriftelijke beslissing van een bestuursorgaan op grond van de Awb
- *Betrokkenen:*	de natuurlijke persoon die geïdentificeerd of identificeerbaar is, op wie de gegevens betrekking hebben;
- *BW*:	Burgerlijk Wetboek;
- *CISO*	Chief Information Security Officer
- *CIO*	Chief Information Officer
- *CIO Office*	de ondersteunende staf van de CIO (het Office van de Chief Information Officer)
- *College*	het College van Bestuur van de EUR;
- *Commissie*	Een vaste dan wel ad-hoc commissie, ingesteld door een bestuursorgaan van de EUR
- *CPO*	Chief Privacy Officer
- *DIM*	Discipline Documentary Information Management binnen het CIO Office
- *DPIA*	Gegevenseffectenbeoordeling/Data Protection Impact Assessment, een instrument om vooraf de privacy risico's van verwerkingen met persoonsgegevens en de effecten voor betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen, te beoordelen en maatregelen voor te stellen. Om vervolgens deze maatregelen te kunnen nemen om deze effecten voor betrokkenen te voorkomen of te verkleinen
- *EDIS*	Erasmus Digitalization & Information Services
- *EER*	Europese Economische Ruimte
- *EUR*:	Erasmus Universiteit Rotterdam;
- *FG*	Functionaris Gegevensbescherming
- *Gegevensbescherming*	bescherming van persoonsgegevens in overeenstemming met de AVG
- *Informatiebeveiliging*	de beveiliging van informatie om de beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen
- *Informatiebeveiligingsbeleid*	het beleid van de EUR waarin vorm en kaders worden gegeven aan de wijze waaraan de informatiebeveiliging binnen de EUR dient te voldoen
- *Informatiemanagement*	de discipline Informatiemanagement binnen het CIO Office
- *Inkoopbeleid*	Het beleid van de EUR waarin vorm en kaders worden gegeven aan de wijze waarop we binnen de EUR Inkopen.
- *Inkopen/Inkoop*	Alles waar een externe factuur tegenover staat. Het betreft dus alle diensten, werken en leveringen waarbij externe

	partijen producten leveren en/of werkzaamheden verrichten voor de EUR.
- *ISO*	Information Security Officer
- *Interne Audit & Review Functie*	onafhankelijke medewerker van de afdeling Corporate Planning & Control EUR die de kwaliteit en effectiviteit van processen onderzoekt.
- *JZ*	*de* Afdeling Juridische Zaken van de EUR
- *Lead DIM*	Aanpreekpunt van de discipline Documentary Information Management binnen het CIO Office
- *Mandaat*	de bevoegdheid om in naam van het College besluiten te nemen
- *Medewerker*	een natuurlijk persoon die werkzaamheden voor de EUR verrichten, al dan niet bezoldigd, en onder het interne beheer valt
- *Persoonsgegevens:*	alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); 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;
- *Privacybeleid*	Het beleid van de EUR ten aanzien van privacy waarin vorm en kaders worden gegeven ten behoeve van gegevensbescherming binnen de EUR
- *PO*	Privacy Officer
- *Portfoliomanagement*	de discipline Portfoliomanagement binnen het CIO Office
- *Privacy*	de discipline Privacy binnen het CIO Office
- *PJ*	Privacy Jurist
- *Rechten van Betrokkenen*	de rechten beschreven in de artikelen 15 tot en met 23 AVG die aan de betrokkenen worden toegekend
- *Recordmanager*	medewerker van Documentary Information Management
- *RASCI*	een matrix die wordt gehanteerd om de rollen en verantwoordelijkheden van de personen die bij een project of lijnwerkzaamheden betrokken zijn weer te geven (Responsible, Accountable, Supportive, Consulted, Informed)
- *Reglement:*	Information Governance Risk & Compliance Reglement. Dit Reglement waarin de inrichting en werkwijze binnen de EUR met betrekking tot Gegevensbescherming, Informatiebeveiliging en Archivering staat beschreven

- *Schriftelijk*:	Op schrift of "langs elektronische weg", zoals bedoeld in artikel 6:227a van het BW;
- *Security*	de discipline Informatiebeveiliging binnen het CIO Office
- *Security expert*	Medewerker van de Faculteit of Dienst die het aanspreekpunt is voor de ISO
- *Selectielijst*	lijst waarin is aangegeven of de archiefwaardige informatieobjecten voor blijvende bewaring dan wel voor vernietiging in aanmerking komen als ook de termijn.
- *Sourcing*	de discipline Sourcing binnen EDIS/CIO Office
- *Submandaat*	mandaat van een mandaat
- *Subvolmacht*	volmacht van een volmacht
- *Tenderboard*	Overleg(plat)vorm, bestaande uit verschillende Functionarissen met voldoende deskundigheid op specifieke kernexpertises en van de totale belangen van de EUR, ten behoeve van Aanbestedingen van de EUR.
- *Three Lines model*	model voor inrichting van de governance gebaseerd op "The IIA's Three Lines" gepubliceerd op 20 juli 2020 door The Institute of Internal[1]
- *Vernietigen*	Beheerst proces van verwijderen of wissen van een informatieobject zonder dat het informatieobject weer geconstrueerd kan worden.
- *Verwerken:*	een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via (geautomatiseerde) processen, 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;
- *Volmacht*	de bevoegdheid om namens het college rechtshandelingen uit te voeren
- *Werkplannen*	plannen die de Beheerseenheden jaarlijks opstellen over de geplande werkzaamheden ten aanzien van Gegevensbescherming, Informatiebeveiliging en Archivering
- *WHW*	Wet van 8 oktober 1992, houdende bepalingen met betrekking tot het hoger onderwijs en wetenschappelijk onderzoek
- *WOO*	Wet Open Overheid

2. De in dit Reglement voorkomende begrippen hebben, indien die begrippen ook voorkomen in de wet en hier niet zijn gedefinieerd, dezelfde betekenis als in de wet (WHW).

[1] https://www.iia.nl/kenniscentrum/vaktechnische-publicaties/publicatie/three-lines-model-updated---nl

3. Wanneer in dit Reglement de 'hij'- vorm wordt gebruikt, kan ook de 'zij'-vorm of 'die' vorm worden gelezen en vice versa.
4. Waar in dit Reglement een term in enkelvoud vermeld wordt, kan eveneens meervoud worden gelezen of vice versa.

Artikel 1.2 – Uitgangspunt Three Lines model

De verdeling van verantwoordelijkheden ten aanzien van Gegevensbescherming, Informatiebeveiliging en Archivering binnen de gehele EUR is op het Three Lines model gebaseerd, met als doel het bevorderen van een effectieve samenhang van werkzaamheden door een efficiënte samenwerking.

Artikel 1.2.1 – Eerste lijn

Het College is verantwoordelijk voor de Gegevensbescherming, Informatiebeveiliging en Archivering in de gehele organisatie. Daarnaast zijn de Beheerders van de Beheerseenheden verantwoordelijk voor hun eigen verwerkingsprocessen, en de daar aan gerelateerde aspecten Gegevensbescherming, Informatiebeveiliging en Archivering binnen het betreffende organisatieonderdeel.

Artikel 1.2.2 – Tweede lijn

De tweede lijn bestaat uit de staffunctionarissen die het management ondersteunen. De CIO zorgt ervoor dat de (C)ISO, de CPO, de PJ en DIM kaders, richtlijnen, toetsingskaders en procedures opstellen ten aanzien van Gegevensbescherming, Informatiebeveiliging en Archivering. Ten aanzien van Gegevensbescherming ondersteunen de POs de eerste lijn en adviseren, signaleren en rapporteren over de wijze waarop persoonsgegevens worden verwerkt door de Beheerseenheden. De ISOs ondersteunen de eerste lijn en adviseren, signaleren en rapporteren over de Informatiebeveiliging binnen de Beheerseenheden. DIM-medewerkers ondersteunen de eerste lijn en adviseren, signaleren en rapporteren over de Archivering binnen de Beheerseenheden.

Ten aanzien van Inkopen bij de EUR wordt het Inkoopbeleid EUR toegepast. Hierin zijn Gegevensbescherming, Informatiebeveiliging en Archivering aangemerkt als interne toetsingskaders voor iedere inkoop, waarbij de contracteigenaar verantwoordelijk is voor naleving hiervan en opvolging van de adviezen van de hiertoe verantwoordelijke functionarissen, namelijk de (C)ISO, (C)PO, DIM en de PJ, tenzij zij aantoonbare en gegronde redenen hebben om hiervan af te wijken. Hiervoor geldt het principe pas toe of leg uit.

Bij Inkopen die conform het EUR-Reglement aan de Tenderboard worden voorgelegd, toetst deze de verantwoording van de contracteigenaar omtrent het voldoen aan de interne toetsingskaders, het onderhavige Information GRC Reglement en de naleving van wet- en regelgeving.

Artikel 1.2.3 – Derde lijn

De derde lijn bestaat uit de FG en de Interne Audit & Review Functie. De FG en de Interne Audit & Review Functie zijn belast met het onderzoek naar de kwaliteit en de effectiviteit van processen ten aanzien van Gegevensbescherming, Informatiebeveiliging en Archivering.

Specifiek de FG adviseert de beheerders en het College gevraagd en ongevraagd over de verplichtingen op grond van de AVG.

Hoofdstuk II - Inleiding

Artikel 2.1 - Inleiding

Dit Reglement regelt, in aanvulling op de bevoegdheden zoals genoemd in het BBR-EUR, de taken, verantwoordelijkheden en bevoegdheden van het College, de Beheerders, de FG en andere functionarissen met betrekking tot Gegevensbescherming, Informatiebeveiliging en Archivering binnen de EUR en de rol van de CIO en CIO Office hierbij.

Artikel 2.2 - Toepasselijke wet- en regelgeving

1. De uitvoering van de in dit Reglement genoemde Beheerstaken geschiedt in overeenstemming met toepasselijk wet- en regelgeving. Toepasselijke wet- en regelgeving bestaat onder meer uit, maar is niet gelimiteerd tot:
    a. De AVG en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)
    b. Algemene Wet inzake Rijksbelastingen (AWR), specifiek art. 52 inzake de bewaarplicht
    c. Wet Open Overheid (WOO)
    d. Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW)
    e. Archiefwet 1995; specifiek artikel 41, en Archiefbesluit 1995, meer specifiek artikel 14
    f. Algemene wet bestuursrecht (Awb)
    g. Beleidsregels, gedragscodes en certificeringsmechanismen die door een bevoegde overheidsinstantie, waaronder de Autoriteit Persoonsgegevens, zijn vastgesteld, als ook zienswijzen van de FG, gedragscodes vanuit koepels als de UNL waaronder de gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek en de Code goed bestuur universiteiten
    h. Regelingen en beleid van de EUR.

Hoofdstuk III - Beheer omtrent Gegevensbescherming, Informatiebeveiliging en Archivering

Artikel 3.1 - Beheerstaken EUR

Het beheer omtrent Informatiehuishouding, meer specifiek de aspecten Gegevensbescherming, Informatiebeveiliging en Archivering omvat de Besluiten en rechtshandelingen, die bij of krachtens wet, te weten de Algemene Verordening Gegevensbescherming (AVG), Archiefwet, dan wel ingevolge het door het College vastgestelde beleid zijn voorgeschreven, doch in elk geval:

1. Het benoemen en ontslaan van de FG en zorgdragen voor de formele aanmelding bij de Autoriteit Persoonsgegevens
2. Het sluiten van overeenkomsten met verwerkers en (gezamenlijke) verwerkingsverantwoordelijken.

3. Het verlenen medewerking aan de Autoriteit Persoonsgegevens en de Inspectie Overheidsinformatie & Erfgoed
4. Het monitoren, evalueren, adviseren, rapporteren en bevorderen de bestendigheid van Gegevensbescherming, de weerbaarheid van Informatiebeveiliging en de duurzaamheid van Archivering door de Beheerseenheden
5. Het beschikbaar stellen van gelden en middelen aan de Beheerseenheden ten behoeve van Gegevensbescherming, Informatiebeveiliging en Archivering.
6. Het opstellen van beleid en kaders op het gebied van Gegevensbescherming, Informatiebeveiliging en Archivering, deze onderhouden en uitvoeren.
7. Het bijhouden van een register van verwerkingsactiviteiten in de zin van de AVG (registerplicht)
8. Het uitvoeren van DPIA's voorafgaand aan risicovolle verwerkingsactiviteiten
9. Het onder bepaalde omstandigheden voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit raadplegen van de Autoriteit Persoonsgegevens (voorafgaande raadpleging)
10. Het bij het inrichten van de informatiehuishouding rekening houden met de principes van ontwerp en standaardinstellingen van Privacy (privacy by design & default), van Security (security by design) en Archivering (Archivering by design)
11. Het treffen van passende beveiligingsmaatregelen met het oog op de bescherming van (persoons)gegevens en de informatiebeveiliging
12. Het registreren van datalekken, het melden van deze bij de Autoriteit Persoonsgegevens en betrokkenen (onder bepaalde omstandigheden)
13. Het respecteren en invullen van de rechten van betrokkene, waaronder ook wordt verstaan het nemen van Besluiten op grond van de AVG en de Awb
14. Het verzorgen van opleiding en het bevorderen van bewustwording van de EUR van haar Medewerkers conform de AVG, het Privacy-, Informatiebeveiligings- en Archiveringsbeleid
15. Het samenwerken met de Beheerseenheden om de doelmatigheid en uniformiteit op het gebied van Gegevensbescherming, Informatiebeveiliging en Archivering te bevorderen
16. Het inkopen van diensten, werken en leveringen, conform het opgestelde in het Inkoopbeleid, waarbij de inbedding van Gegevensbescherming, Informatiebeveiliging en Archivering wordt geborgd
17. Het duurzaam beheren van archiefwaardige informatieobjecten
18. Het houden van overzicht over in welke applicaties/systemen de archiefwaardige informatieobjecten zich bevinden en in welke processen deze worden gebruikt
19. Het tijdig vernietigen van archiefwaardige informatieobjecten bij het aflopen van de bewaartermijn
20. Het tijdig overbrengen van de permanent te bewaren archiefwaardige informatieobjecten naar het Nationaal Archief.

Artikel 3.2 – Voorbehouden College en EUR

Het College behoudt zich de volgende beslissingen en bevoegdheden voor:

1. Het benoemen en ontslaan van de FG en zorgdragen voor de formele aanmelding aan de Autoriteit Persoonsgegevens (AP)

2. Het sluiten van overeenkomsten die samenhangen met een hoofovereenkomst, waarvoor het College tekeningsbevoegd is
3. Het verlenen van medewerking aan de Autoriteit Persoonsgegevens en de Inspectie Overheidsinformatie & Erfgoed
4. Het monitoren en bevorderen van de bestendigheid van Gegevensbescherming, de weerbaarheid van Informatiebeveiliging en de duurzaamheid van Archivering door de Beheerseenheden
5. Het beschikbaar stellen van gelden en middelen aan de Beheerseenheden ten behoeve van Gegevensbescherming, Informatiebeveiliging en Archivering
6. Het (laten) opstellen van beleid en kaders op het gebied van Gegevensbescherming, Informatiebeveiliging en Archivering en deze onderhouden
7. Het (laten) houden van EUR breed overzicht over in welke applicaties/systemen de archiefwaardige informatieobjecten zich bevinden en in welke processen deze worden gebruikt
8. Het tijdig (laten) overbrengen van de permanent te bewaren archiefwaardige informatieobjecten naar het Nationaal Archief.

Artikel 3.3 - Toepasselijkheid BBR – EUR

De artikelen 11.10 Mandaat en Volmacht, 11.11 Submandaat en Subvolmacht en 11.12 Beheersinstructie uit het Bestuurs- en Beheersreglement Erasmus Universiteit Rotterdam 2023 (BBR-EUR 2022) zijn op dit Reglement overeenkomstig van toepassing.

Artikel 3.4 - Taken Beheerders

De navolgende Beheerstaken met betrekking tot het Beheer van de Gegevensbescherming, Informatiebeveiliging en Archivering, genoemd in artikel 3.1 van dit Reglement worden gemandateerd en in Volmacht gegeven aan de Beheerder:

1. Het maken van afspraken met verwerkers en (gezamenlijke) verwerkingsverantwoordelijken
2. Het verlenen van medewerking aan de Autoriteit Persoonsgegevens en de Inspectie Overheidsinformatie & Erfgoed
3. Het monitoren, evalueren, adviseren, rapporteren en bevorderen van de bestendigheid van Gegevensbescherming, de weerbaarheid van Informatiebeveiliging, de duurzaamheid van Archivering van de eigen Beheerseenheid
4. Het uitvoeren van het beleid, het werken binnen de kaders op het gebied van Gegevensbescherming, Informatiebeveiliging en Archivering en het voorleggen van afwijkingen hiervan aan de CIO
5. Het bijhouden van een register van verwerkingsactiviteiten in de zin van de AVG (registerplicht)
6. Het uitvoeren van DPIA's voorafgaand aan risicovolle verwerkingsactiviteiten.
7. Het onder bepaalde omstandigheden voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit raadplegen van de Autoriteit Persoonsgegevens (voorafgaande raadpleging)

8. Het bij het inrichten van de informatiehuishouding rekening houden met de principes van ontwerp en standaardinstellingen van Privacy (privacy by design & default), van security (security by design) en Archivering (archivering by design)
9. Het treffen van passende beveiligingsmaatregelen met het oog op de bescherming van (persoons)gegevens en de Informatiebeveiliging
10. Het registreren van datalekken, deze melden bij de FG en betrokkenen (onder bepaalde omstandigheden)
11. Het respecteren en invullen van de rechten van betrokkene
12. Het verzorgen van opleiding en bewustwording van de EUR van Medewerkers conform de AVG, het Privacy-, Informatiebeveiligings- en Archiveringsbeleid
13. Het samenwerken met de Beheerseenheden om de doelmatigheid en uniformiteit op het gebied van Gegevensbescherming, Informatiebeveiliging en Archivering te bevorderen
14. Het inkopen van diensten, werken en leveringen in, conform het opgestelde in het Inkoopbeleid, waarbij de inbedding van Gegevensbescherming, Informatiebeveiliging en Archivering wordt geborgd
15. Het duurzaam beheren van archiefwaardige informatieobjecten binnen de eigen Beheerseenheid
16. Het binnen de Beheerseenheid houden van overzicht over in welke applicaties/systemen de archiefwaardige informatieobjecten zich bevinden en in welke processen deze worden gebruikt
17. Het tijdig (laten) vernietigen van archiefwaardige informatieobjecten bij het aflopen van de bewaartermijn.

Artikel 3.5 - Taken (Interne) Audit & Review Functie

De navolgende taken met betrekking tot het Beheer van de Gegevensbescherming, Informatiebeveiliging en Archivering voert de Interne Audit en Review uit in opdracht van het College ten behoeve van de Beheerstaak, beschreven in artikel 3.2 lid 6:

1. Voert in samenspraak met de FG audits uit (of laat deze uitvoeren) ten einde de naleving van de AVG, het Privacy-, Informatiebeveiligings- en Archiveringsbeleid van de EUR te kunnen monitoren, evalueren en rapporteren
2. Ziet in samenspraak met de FG toe op de opvolging van de aanbevelingen uit de audits met betrekking tot de naleving van de AVG, het Privacy-, Informatiebeveiligings- en Archiveringsbeleid van de EUR.

Artikel 3.6 - Taken Functionaris Gegevensbescherming

De navolgende wettelijke taken met betrekking tot het Beheer van de Gegevensbescherming behoren op grond van artikel 39 AVG en de taken met betrekking tot het Beheer van de Gegevensbescherming en onderdelen van Informatiebeveiliging en Archivering, voor zover het Gegevensbescherming betreft, voert de FG uit in opdracht van het College ten behoeve van de Beheerstaak, beschreven in artikel 3.2 lid 6:

1. Informeert en adviseert desgevraagd en/of op eigen initiatief het College over de verplichtingen op grond van de AVG
2. Ziet toe als toezichthouder op de naleving van de AVG en het Privacy beleid van de EUR

3. Ziet toe op de uitvoering van Gegevensbescherming effectbeoordelingen (DPIA's) en adviseert over de volgende aspecten:
    a. of er een DPIA moet worden uitgevoerd
    b. op welke wijze de beoordeling wordt gedaan
    c. of de beoordeling intern wordt gedaan of wordt uitbesteed aan een externe partij
    d. welke waarborgen er moeten worden getroffen om de in de beoordeling gebleken risico's te beperken
    e. of de DPIA goed is gedaan en
    f. of de uitkomsten ervan voldoen aan de AVG
4. Treed op als contactpunt voor en werkt samen met de Autoriteit Persoonsgegevens
5. Vervult alleen andere taken en plichten wanneer deze niet tot een belangenconflict kunnen leiden
6. Ziet toe op opleiding en bewustwording van medewerkers ten aanzien van de AVG en het Privacy beleid van de EUR
7. Voert in samenspraak met de Interne Audit & Review Functie audits uit (of laat deze uitvoeren) ten einde de naleving van de AVG en het Privacy beleid van de EUR te kunnen monitoren, evalueren en rapporteren.

Artikel 3.7 - Taken Chief Information Officer

De navolgende taken met betrekking tot het Beheer van de Gegevensbescherming, Informatiebeveiliging en Archivering voert de CIO (of laat deze uitvoeren) in opdracht van het College uit ten behoeve van de Beheerstaken, beschreven in artikel 3.2 lid 6 t/m 11:

1. Monitort, evalueert, adviseert, rapporteert en bevordert EUR breed de bestendigheid van Gegevensbescherming, de weerbaarheid van Informatiebeveiliging en de duurzame Archivering binnen de Beheerseenheden
2. Geeft uitvoering aan het beschikbaar stellen van middelen ten einde de Beheerseenheden te faciliteren om beheerstaken ten aanzien van Gegevensbescherming, Informatiebeveiliging en Archivering te ondersteunen
3. Laat beleid, kaders en richtlijnen op het gebied van Gegevensbescherming, Informatiebeveiliging en Archivering opstellen en onderhouden, in samenhang met die van andere CIO Office disciplines
4. Houdt een de gehele organisatie omvattend overzicht van applicaties/systemen waarin archiefwaardige informatieobjecten zijn opgeslagen en in welke werkprocessen deze worden gebruikt
5. Houdt EUR breed overzicht over in welke applicaties/systemen de archiefwaardige informatieobjecten zich bevinden en in welke processen deze worden gebruikt
6. Laat de permanent te bewaren archiefwaardige informatieobjecten tijdig overbrengen naar het Nationaal Archief.

Hoofdstuk IV – Beheersinstructie CIO

Artikel 4.1 - Algemeen

Voor de uitvoering van de Beheerstaken die op grond van artikel 3.7 toekomen aan de CIO schakelt deze de CPO, CISO,PJ en DIM als autoriteit op hun expertisegebied in zoals beschreven in de onderstaande artikelen.

Artikel 4.2 - Taken Chief Information Security Officer

De navolgende Beheerstaken met betrekking tot het Beheer van de Informatiebeveiliging, die toebehoren aan de CIO, worden op grond van diens expertise toebedeeld aan de CISO:

1. Stelt het Informatiebeveiligingsbeleid in samenhang met het beleid van de andere CIO Office disciplines op en houdt dit bij
2. Draagt zorg voor organisatie brede richtlijnen, toetsingskaders, standaarden, methoden en technieken ten aanzien van Informatiebeveiliging
3. Organiseert het vakgebied Informatiebeveiliging en de benodigde expertise
4. Zorgt voor afstemming tussen Informatiebeveiliging met andere beveiligingsdomeinen (Gegevensbescherming, Beheerseenheid, fysieke beveiliging en continuiteitsmanagement)
5. Initieert en coördineert organisatie brede Informatiebeveiligingsactiviteiten en verbetertrajecten
6. Organiseert de afstemming, samenwerking en kennisdeling tussen de ISO's en de Security experts
7. Monitort, evalueert, adviseert en rapporteert omtrent het borgen van de kwaliteit van informatierisicoanalyses, -assessments, beveiligingsontwerpen en de beveiligingsoplossingen en -maatregelen
8. Monitort, evalueert, adviseert en rapporteert omtrent het borgen van Informatiebeveiligingsbewustzijn binnen de organisatie
9. Monitort, evalueert, adviseert en rapporteert omtrent de relevante risico's op het gebied van informatiebeveiliging voor de organisatie
10. Adviseert de Beheerders en Beheerseenheden over het voldoende voorbereid zijn op toekomstige Informatiebeveiligingsrisico's en ICT-beveiligingsrisico's
11. Monitort, evalueert, adviseert en rapporteert in hoeverre de organisatie compliant is met het Informatiebeveiligingsbeleid en wet- en regelgeving.
12. Ondersteunt de Interne Audit & Review functie bij het toezien op uitvoeren van de verbeterprogramma's of -maatregelen naar aanleiding van de resultaten van de audits met betrekking tot de naleving het informatiebeveiligingsbeleid van de EUR
13. Toetst of laat toetsen de Inkopen conform het gestelde in het Inkoopbeleid aan de toetsingskaders op het gebied van Informatiebeveiliging
14. Heeft een regelmatig overleg met het College, zijnde de portefeuillehouder Informatiebeveiliging, over de weerbaarheid van Informatiebeveiliging en het borgen de maatregelen van Informatiebeveiliging en de status van Informatiebeveiliging en incidenten. Verder presenteert deze verbetervoorstellen
15. Informeert College over de status van Informatiebeveiliging en incidenten en presenteert verbetervoorstellen

16. Grijpt in de systemen EUR breed of legt systemen geheel of gedeeltelijk stil als dit noodzakelijk is voor de Informatiebeveiliging (handhavingstaak) omdat continueren een (mogelijk) risico voor de EUR vormt
17. Informeert en legt verantwoording over de bovenstaande taken af aan de CIO met uitzondering van de taken 14, 15 en 16 waarvoor enkel een informatieverplichting geldt.

Artikel 4.3 - Taken Chief Privacy Officer

De navolgende Beheerstaken met betrekking tot het Beheer van de Gegevensbescherming die toebehoren aan de CIO, worden op grond van diens expertise toebedeeld aan de CPO:

1. Stelt het Privacy beleid op in samenhang met het beleid van de andere CIO Office disciplines en houd het bij
2. Zorgt voor organisatie brede richtlijnen, toetsingskaders, standaarden, werkinstructies en protocollen voor Gegevensbescherming
3. Organiseert het vakgebied Gegevensbescherming en de benodigde expertise
4. Zorgt voor afstemming tussen Privacy met andere domeinen (waaronder Inkoop, JZ, Beheerseenheden)
5. Organiseert de afstemming, samenwerking en kennisdeling tussen de POs
6. Monitort, evalueert, adviseert en rapporteert ten aanzien van de registers van verwerkingen en het beheer van de datakwaliteit
7. Initieert en coördineert in afstemming met de FG organisatie brede privacy-activiteiten en -projecten
8. Monitort, evalueert, adviseert en rapporteert (gevraagd en ongevraagd) over de Beheerseenheden omtrent het borgen de beginselen van gegevensverwerking, waaronder de Gegevensbescherming
9. Borgt van de kwaliteit van de assessments en privacy analyses, privacy by design / default-ontwerpen en oplossingen
10. Ondersteunt de Interne Audit & Review Functie en de FG bij het toezien op het uitvoeren van de verbeterprogramma's of -maatregelen naar aanleiding van de resultaten van de audits met betrekking tot de naleving de AVG en het Privacy beleid van de EUR
11. Toetst of laat toetsen de Inkopen conform het gestelde in het Inkoopbeleid aan de toetsingskaders op het gebied van Gegevensbescherming
12. Adviseert het College op diens verzoek omtrent het borgen van de beginselen van gegevensverwerking, waaronder de Gegevensbescherming
13. Bereid, in opdracht van het College, samen de PJ de overeenkomsten voor die het College zich heeft voorbehouden
14. Informeert en legt verantwoording over de bovenstaande taken af aan de CIO.

Artikel 4.4 - Taken Privacy Jurist

De navolgende Beheerstaken met betrekking tot het Beheer van de Gegevensbescherming die toebehoren aan de CIO, worden op grond van diens expertise toebedeeld aan de PJ:

1. Stelt juridische modellen op en houdt deze bij
2. Zorgt voor de inrichting van juridische processen die voldoen aan wettelijke eisen

3. Monitort, evalueert, adviseert en rapporteert omtrent de afhandeling van (AVG) verzoeken
4. Monitort, evalueert, adviseert en rapporteert omtrent de afhandeling van (AVG) overeenkomsten
5. Adviseert de CIO, CPO en FG over juridische vraagstukken
6. Ondersteunt en begeleidt de POs bij complexe juridische vraagstukken
7. Ondersteunt en begeleidt de POs bij complexe onderhandelingen
8. Bevordert het uniform werken op het juridische vlak door middel van de verbinding met de afdeling JZ
9. Bereid, in opdracht van het College, samen de CPO de overeenkomsten voor die het College zich heeft voorbehouden
10. Informeert en legt verantwoording over de bovenstaande taken af aan de CIO.

Artikel 4.5 - Taken Lead Documentary Information Management

De navolgende Beheerstaken met betrekking tot het zorg voor archiefwaardige informatieobjecten die toebehoren aan de CIO, worden op grond van diens expertise toebedeeld aan de Lead van DIM:

1. Stelt het Archiveringsbeleid op in samenhang met het beleid van de andere CIO Office disciplines en houd het bij
2. Stelt een beheersregime voor de documentaire informatiehuishouding op
3. Zorgt voor organisatie brede richtlijnen, toetsingskaders, standaarden, werkinstructies en protocollen voor de documentaire informatiehuishouding van de EUR
4. Organiseert het vakgebied Archivering en de daarvoor benodigde expertise
5. Monitort, evalueert, adviseert en rapporteert omtrent de zorg voor Archiefwaardige Informatieobjecten
6. Zorgt voor afstemming tussen Archivering en de andere domeinen (waaronder Privacy, Informatiebeveiliging, Inkoop)
7. Adviseert de Beheerders met betrekking tot (documentaire) informatiehuishouding
8. Ondersteunt de Beheerders met betrekking tot het tijdig vernietigen van de archiefwaardige informatieobjecten bij het aflopen van de bewaartermijn
9. Brengt de permanent te bewaren Archiefwaardige Informatieobjecten tijdig over naar het Nationaal Archief
10. Informeert en legt verantwoording over de bovenstaande taken af aan de CIO.

Hoofdstuk V – Verantwoordelijkheden

Artikel 5.1 – Verantwoordelijkheden algemeen

De verdere verdeling van de verantwoordelijkheden op basis van de “Three Lines” model is noodzakelijk om te zorgen voor compliance en beperking van de risico’s ten aanzien van Gegevensbescherming, Informatiebeveiliging en Archivering te realiseren. De inzet van alle bestuurslagen, Beheerders en Medewerkers van de universiteit is hiervoor nodig. De verschillende taken, rollen en verantwoordelijkheden zijn in de RASCI Responsibility Matrix Algemeen (bijlage 1), de RASCI Responsibility Matrix Beheerstaken (bijlage 2) en de RASCI Matrix Rolverdeling (Bijlage 3) vastgelegd en worden hieronder verder uitgewerkt. Bij

afwijkingen tussen de rollen en verantwoordelijkheden geldt hetgeen in de RASCI Matrix Rolverdeling is opgenomen.

Artikel 5.2 – Verantwoordelijkheid College

1. Het College is "accountable" voor de naleving van de AVG en de Archiefwet.
2. Het College stelt op basis van de jaarlijkse verantwoording de mate van optimalisatie van Information Risk & Compliance van de Beheerseenheden vast
3. Het College stelt op basis van de ingediende Werkplannen van de Beheerseenheden jaarlijks een programma vast over de optimalisatie van Information Risk & Compliance
4. Het College stelt middelen en ondersteuning beschikbaar om te voldoen aan wet- en regelgeving ten aanzien van Gegevensbescherming, Informatiebeveiliging en Archivering
5. Het College treft in redelijkheid de maatregelen of sancties als beheerders (een Faculteitsbestuur of directie van een Dienst) in gebreke is met betrekking tot de wet- en regelgeving ten aanzien van Gegevensbescherming, Informatiebeveiliging en Archivering of dit Reglement.

Artikel 5.3 – Verantwoordelijkheid Beheerders

1. De Beheerders zijn als bestuurder van de Beheerseenheid "responsible" voor de uitvoering van het vastgestelde Privacy- , Informatiebeveiligings- en Archiveringsbeleid .
2. De Beheerders zullen de aan hen toebedeelde verantwoordelijkheden en beheerstaken binnen de Beheerseenheid beleggen in een Beheersinstructie (met een daarbij behorende RASCI Matrix Beheerstaken en RASCI Matrix Rolverdeling Beheerseenheid)
3. Beheerders stemmen de toepassing van de AVG, het Informatiebeveiligingsbeleid, de Archiefwet en de WOO af met andere Beheerseenheden, zodat dubbel werk voorkomen wordt en de uniformiteit bevorderd wordt
4. Beheerders voeren het beleid uit en werken binnen de gestelde kaders, bij afwijking contacteren zij de CIO
5. Beheerders stellen jaarlijks een werkplan op waarin Information Risk & Compliance voor de domeinen onderwijs, bedrijfsvoering en wetenschappelijk onderzoek worden uitgewerkt in concrete maatregelen en acties
6. Beheerders stellen een PO aan of nemen PO diensten af van de centrale pool om de toepassing van dit Reglement ten aanzien van Gegevensbescherming binnen diens Beheerseenheid te coördineren
7. Beheerders leggen jaarlijks verantwoording af aan het College, waarin zij inzicht geven in de realisatie van de voorgenomen acties en maatregelen van het ingediende werkplan. Een afschrift van deze rapportage wordt gedeeld met de FG en de CIO.

Artikel 5.4 – Verantwoordelijkheid Chief Information Officer

1. De CIO is "responsible" voor uitvoering (laten) geven aan de opdrachten vanuit het College bij het uitvoeren en naleven van de geldende wetgeving (o.a. AVG, Archiefwet) en het komen tot Information Risk & Compliance

2. De CIO geeft sturing aan het CIO Office waaronder de disciplines Privacy, Security en DIM teneinde de strategische doelen van de EUR middels integrale samenhang en visie vorm te geven
3. De CIO (laat) relevante audits op de auditkalender plaatsen op verzoek van de disciplines Privacy, Security en DIM, naast die van andere disciplines van CIO Office
4. De CIO legt jaarlijks verantwoording af aan het College over de optimalisatie van Gegevensbescherming, Informatiebeveiliging en Archivering. Een afschrift van deze rapportage wordt gedeeld met de FG en de Beheerders.

Artikel 5.5 – Verantwoordelijkheid Chief Information Security Officer

1. De CISO is " responsible" voor de opdrachten vanuit het College, "supportive" voor wat betreft de uitvoering van de opdrachten van de CIO en "consulted" ten aanzien van de ISO's bij hun ondersteuning van de Beheerseenheden bij het uitvoeren en naleven van het Informatiebeveiligingsbeleid.
2. De CISO coördineert de EUR brede verbetertrajecten en projecten die op basis van de door de Beheerders opgestelde Werkplannen door het College zijn vastgesteld.
3. De CISO geeft sturing aan de ISO's daar waar het om de toepassing van beleid en kaders die door het College zijn bekrachtigd
4. De CISO heeft het recht om, na instemming van het College, in te grijpen in alle systemen dan wel deze stil te leggen als dit noodzakelijk voor de Informatiebeveiliging (handhavingstaak).

Artikel 5.6 – Verantwoordelijkheid Chief Privacy Officer

1. De CPO is "supportive" voor wat betreft de uitvoering van de opdrachten van de CIO en "consulted" ten aanzien van de POs bij hun ondersteuning van de Beheerseenheden bij het uitvoeren en naleven van de AVG
2. De CPO coördineert de EUR brede verbetertrajecten en projecten die op basis van de door de Beheerders opgestelde Werkplannen door het College zijn vastgesteld
3. De CPO geeft sturing aan de POs daar waar het om de toepassing van beleid en kaders die door het College zijn bekrachtigd
4. De CPO informeert de FG over grote of risicovolle Gegevensbeschermingsvraagstukken
5. Als de uitoefening van zijn taken hem hiertoe nopen, informeert, rapporteert of escaleert de CPO rechtstreeks aan/naar het College en informeert de CIO.

Artikel 5.7 – Verantwoordelijkheid Information Security Officer

1. De ISO is "supportive" ten aanzien van de taken en verantwoordelijkheden van de CISO
2. De ISO adviseert de Beheerders bij het uitvoering geven aan het EUR Informatiebeveiligingsbeleid.

Artikel 5.8 – Verantwoordelijkheid Privacy Officers

1. De POs zijn "supportive" jegens de Beheerders bij het naleven van de Gegevensbescherming van de Beheerseenheden
2. De POs zijn "supportive' jegens de CPO bij het uitvoering geven aan de EUR brede projecten en het beleid en kaders.

Artikel 5.9 – Verantwoordelijkheid Privacy Jurist

1. De PJ is "consulted" als er grote of risicovolle juridische vraagstukken spelen. Verder is de PJ "responsible" voor de taken als hierboven beschreven in artikel 4.4.

Artikel 5.10 – Verantwoordelijkheid Lead Documentary Information Management

1. De Lead DIM is "supportive" voor wat betreft de uitvoering van de opdrachten van de CIO en "consulted" ten aanzien van het adviseren van de Beheerseenheden over het uitvoeren en naleven van de Archiefwet
2. De Lead DIM coördineert de EUR brede verbetertrajecten en projecten die op basis van de door de Beheerders opgestelde Werkplannen door het College zijn vastgesteld
3. De Lead DIM informeert de Interne Audit & Review Functie of FG over grote of risicovolle risicomanagementvraagstukken resp. grote of risicovolle Gegevensbeschermingsvraagstukken
4. Als de uitoefening van zijn taken hem hiertoe nopen informeert, rapporteert of escaleert de Lead DIM rechtstreeks naar het College en informeert de CIO.

Artikel 5.11 – Verantwoordelijkheid Recordmanagers

1. De Recordmanagers zijn "supportive' jegens de Lead DIM bij het uitvoering geven aan de EUR brede projecten en het beleid en kaders
2. De Recordmanagers zijn "supportive" jegens de Beheerders bij het naleven van de Archiefwet door de Beheerseenheden.

Artikel 5.12 – Verantwoordelijkheid Interne Audit & Review Functie

1. De Interne Audit & Review Functie wordt "informed" over alle zaken die onder het toezicht van deze functie valt
2. De Interne Audit & Review Functie wordt geïnformeerd over grote of risicovolle risicomanagementvraagstukken waarop de functie toezicht houdt. Daarnaast is de Interne Audit & Review Functie "responsible" voor de taken als hierboven beschreven in artikel 3.5.

Artikel 5.13 – Verantwoordelijkheid Functionaris Gegevensbescherming

1. De FG wordt "informed" over zaken die onder het toezicht van deze functie valt.
2. De FG wordt geconsulteerd als er grote of risicovolle Gegevensbeschermings-vraagstukken spelen en geïnformeerd over de grote of risicovolle Gegevensbeschermingsvraagstukken die onder zijn toezicht vallen. Daarnaast is deze functie "responsible voor de taken als hierboven beschreven in artikel 3.6.

Artikel 5.14 – Verantwoordelijkheid Medezeggenschap

1. De Universiteitsraad is "accountable" voor de uitvoering van Information Risk & Compliance binnen de Raad
2. De Universiteitsraad wordt "consulted" over regelingen omtrent het verwerken alsmede de bescherming van persoonsgegevens van de personen die in de onderneming werkzaam zijn in verband met het instemmingsrecht.
3. De Universiteitsraad wordt "consulted" over regelingen inzake voorzieningen die gericht zijn op of geschikt zijn voor het registreren of controleren van aanwezigheid, gedrag of prestaties van de personen die in de onderneming

werkzaam zijn (ofwel personeelsvolgsystemen) in verband met het instemmingsrecht.

4. De Universiteitsraad wordt "informed" over regelingen omtrent het verwerken alsmede de bescherming van persoonsgegevens van de personen die zijn ingeschreven als student.
5. De Universiteitsraad wordt "informed" over regelingen inzake voorzieningen die zijn gericht op of geschikt zijn voor het registeren of controleren van aanwezigheid, gedrag en prestaties van studenten (ofwel studentvolgsystemen).

Artikel 5.15 – Verantwoordelijkheid Commissie

1. De Commissie is "responsible" voor de uitvoering van de AVG, Infomatiebeveiligingsbeleid, de Archiefwet binnen de Commissie.
2. Indien het een onafhankelijke Commissie betreft, is zij "accountable" voor Information Risk & Compliance binnen deze Commissie.

Artikel 5.16 – Verantwoordelijkheid Medewerker

1. Iedere Medewerker van de EUR is "supportive" jegens de Beheerders. Ze dragen zorg voor de toepassing van geldend beleid en maatregelen ten aanzien van Gegevensbescherming, Informatiebeveiliging en Archivering met betrekking tot de eigen activiteiten.

Hoofdstuk VI - Positie Functionaris Gegevensbescherming, Chief Information Security Officer en Interne Auditor

Artikel 6.1 – Onafhankelijkheid Functionaris Gegevensbescherming

1. De FG is geplaatst bij de afdeling JZ. De FG is voor zover het de uitvoering van zijn taken betreft niet hiërarchisch ondergeschikt aan de Directeur JZ, noch aan de Directeur ABD, secretaris van het College.
2. De FG ontvangt geen instructies met betrekking tot de uitvoering van zijn taken.
3. De FG wordt niet ontslagen of gestraft voor de uitvoering van zijn taken.
4. De FG brengt jaarlijks rechtstreeks verslag uit aan het College over de stand van zaken met betrekking tot de naleving van de AVG door de EUR.
5. De FG brengt direct verslag uit aan het College, in geval van overtredingen van de AVG.
6. Het College zorgt ervoor dat de FG naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

Artikel 6.2 – Onafhankelijkheid Chief Information Security Officer

1. De CISO is binnen de EUR geplaatst in de eenheid CIO Office. De CISO is voor zover het signaleringstaken en de handhavingstaken betreft niet hiërarchisch ondergeschikt aan de CIO
2. De CISO ontvangt geen instructies met betrekking tot de uitvoering van zijn signalerings- en handhavingstaken
3. De CISO wordt niet door de CIO ontslagen of gestraft voor de uitvoering van deze signalerings- en handhavingstaken

4. De CISO brengt jaarlijks rechtstreeks verslag uit aan het College over de stand van zaken met betrekking tot de naleving van het Informatiebeveiligingsbeleid door de EUR.
5. De CISO brengt direct verslag uit aan het College over de risico's van de Informatiebeveiliging
6. Het College zorgt ervoor dat de CISO naar behoren en tijdig wordt betrokken bij alle aangelegenheden die verband houden met de Informatiebeveiliging.

Artikel 6.3 – Onafhankelijkheid Interne Audit & Review Functie

1. De Interne Audit & Review Functie heeft een onafhankelijke en onpartijdige positie binnen de EUR. De positie van de Audit & Review Functie is vastgesteld in de Audit Charter.

Hoofdstuk VII - Slot- en overgangsbepalingen

Artikel 7.1 - Interpretatie

In gevallen verband houdend met de in dit Reglement geregelde onderwerpen, waarin dit Reglement niet voorziet of ingeval dit Reglement aanleiding geeft tot meervoudige interpretatie, beslist het College.

Artikel 7.2 - Beheer Reglement

Dit Reglement is in beheer bij: EDIS/CIO Office

Artikel 7.3 - Vertaling

Wanneer dit Reglement is vertaald en zich er een geval van strijdigheid tussen de vertaling en de Nederlandse versie voordoet, prevaleert de Nederlandse versie.

Artikel 7.4 - Publicatie

Het College plaatst dit Reglement op de website van de EUR.

Artikel 7.5 - Inwerkingtreding

Dit Reglement treedt, na de goedkeuring van het College, in werking, op 1 januari 2023.

Artikel 7.6 - Citeertitel

Dit Reglement wordt aangehaald als: Information Governance Risk & Compliance Reglement.
Dit Reglement wordt afgekort als: Information GRC Reglement.

Artikel 7.7 - Geldend recht

Op dit Reglement is uitsluitend Nederlands recht van toepassing.

Bijlage 1 – RASCI Responsibility Matrix Algemeen

Bijlage behorende bij art. 5.1 van dit Reglement.

Afkorting	Betekenis	Nederlands	Functie
Responsible	Verantwoordelijk voor de uitvoering	Verantwoordelijk	BE
Accountable	Bevoegd om beslissingen te nemen. Er kan maar een persoon Accountable zijn. CvB is Accountable / eindverantwoordelijk in de zin de de Avg. Vwb interne procesafspraken kan Accountable / eindverantwoordelijkheid ook anderen liggen.	Eindverantwoordelijk	CvB
Supporting	Wordt geraadpleegd ter ondersteuning	Ondersteunend	CPO, (C)ISO, PO / Procesbeheerders / onderzoekers /medewerkers
Consulting	Wordt vooraf geraadpleegd	Geraadpleegd	FG / JZ / PJ / Inkoop
Informed	Wordt achteraf geinformeerd	Geinformeerd	Medezeggenschapsorganen, betrokkenen / externe toezichthouders / IA

afk.	betekenis
CvB	College van Bestuur
IA	(Interne) Audit & Review Functie: Sec toezicht , alleen consulted over processen
FG	Functionaris Gegevensbescherming: Toezicht: Adviestaken:
CIO	Chief Information Officer
CPO	Chief Privacy Officer
PO	Privacy Officer
PJ	Privacy Jurist
CISO	Chief Information Security Officer
BE	Beheerseenheid
Inkoop	Afdeling Inkoop
ISO	Information Security Officer
MC	Marketing & Communicatie

Bijlage 2 – RASCI Responsibility Matrix Beheerstaken

Bijlage behorende bij art. 5.1 van dit Reglement.

		Beheerstaken	R	A	S	C	I
INFORMATION	1	Het benoemen en ontslaan van de FG en zorgdragen voor de formele aanmelding bij de Autoriteit Persoonsgegevens (AP)	CvB	CVB		FG, PJ, CPO, CISO	BE, JZ, CIO, M
	2a	Het sluiten van overeenkomsten die samenhangen met een hoofovereenkomst, waarvoor het College tekeningsbevoegd is	CIO	CvB	CPO, PJ	FG, ISO, CISO	
	2b	Het maken van afspraken met verwerkers en (gezamenlijke) verwerkingsverantwoordelijken	BE	CvB	PO	PJ	
	3a	Het verlenen van medewerking aan de Autoriteit Persoonsgegevens	CVB, BE	CVB	CPO, PO, CISO, ISO	FG, PJ	
	3b	Het verlenen van medewerking aan de Inspectie Overheidsinformatie en Erfgoed (Min. OCW)	CVB	CVB	DIM	A, CPO, CISO, IM, IM	BE, CIO
	4	Het monitoren en bevorderen van de bestendigheid van Gegevensbescherming, de weerbaarheid van Informatiebeveiliging en de duurzaamheid van Archivering door de Beheerseenheden	CIO, BE	CVB	PO, CPO, CISO, DIM	FG, IA	
	5	Het beschikbaar stellen van gelden en middelen aan de Beheerseenheden ten behoeve van Gegevensbescherming, Informatiebeveiliging en Archivering	CvB	CvB	CPO, CISO, PJ, DIM		BE, FG
	6a	Het (laten) opstellen van beleid en kaders op het gebied van Gegevensbescherming, Informatiebeveiliging en Archivering en deze onderhouden	CIO	CVB	CPO, CISO, DIM	PJ, FG,	BE, CIO
	6b	Het uitvoeren van het beleid, het werken binnen de kaders op het gebied van Gegevensbescherming, Informatiebeveiliging en Archivering en het voorleggen van afwijkingen hiervan aan de CIO	BE	CVB	PO, ISO, DIM	CPO, CISO, PJ, FG	
	7	Het bijhouden van een register van verwerkingsactiviteiten in de zin van de AVG (registerplicht)	BE	CVB	PO	FG, PJ, CPO	
	8	Het uitvoeren van DPIA's voorafgaand aan risicovolle verwerkingsactiviteiten	BE	CVB	PO	FG, PJ, CPO, CISO	CISO

		Beheerstaken	R	A	S	C	I	
GRC REGLEMENT	9	Het onder bepaalde omstandigheden voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit raadplegen van de Autoriteit Persoonsgegevens (voorafgaande raadpleging)	BE	CVB	PO	FG		
	10	Het bij het inrichten van de informatiehuishouding rekening houden met de principes van ontwerp en standaardinstellingen van Privacy (privacy by design & default), van Security (security by design) en Archivering (Archivering by design)	BE	CVB	PO, ISO, DIM	FG, PJ, CISO	M	
	11	Het treffen van passende beveiligingsmaatregelen met het oog op de bescherming van (persoons)gegevens en de informatiebeveiliging	BE	CVB	PO, ISO, DIM	FG, CISO, CPO	M	
	12	Het registreren van datalekken, het melden van deze bij de Autoriteit Persoonsgegevens en betrokkenen (onder bepaalde omstandigheden)	BE	CVB	PO	FG, PJ, CPO, ISO, CISO	AP	
	13	Het respecteren en invullen van de rechten van betrokkene	BE	CVB	PO	FG, PJ		
	14	Het verzorgen van opleiding en het bevorderen van bewustwording van de EUR van haar Medewerkers conform de AVG, het Privacy-, Informatiebeveiligings- en Archiveringsbeleid	BE	CVB	PO, ISO, DIM	CPO, FG, PJ, CISO, IM	CPO, CISO	
	15	Het samenwerken met de Beheerseenheden om de doelmatigheid en uniformiteit op het gebied van Gegevensbescherming, Informatiebeveiliging en Archivering te bevorderen	BE	CVB	PO, ISO, DIM	CPO, PJ, CISO, IM	FG, CIO	
	16	Het inkopen van diensten, werken en leveringen, conform het opgestelde in het Inkoopbeleid, waarbij de inbedding van Gegevensbescherming, Informatiebeveiliging en Archivering wordt geborgd	BE	CVB	PO, ISO, DIM	Inkoop *, CPO, CISO, PJ	CIO	*Tenderboard kan worden ingeschakeld door inkoop-/ aanbestedings-adviseur obv Reglement Tenderboard
	17	Het duurzaam beheren van archiefwaardige informatieobjecten	BE	CVB	DIM	A, IM, CPO, CISO, Lead DIM	CIO, M	
	18	Het houden van overzicht over in welke applicaties/systemen de archiefwaardige informatieobjecten zich bevinden en in welke processen deze worden gebruikt	BE	CvB	DIM	A, IM, Lead DIM	CIO, CPO, CISO	
	19	Het tijdig vernietigen van archiefwaardige informatieobjecten bij het aflopen van de bewaartermijn	BE	CVB	DIM	A, IM, CPO, CISO, Lead DIM, TB, FB	BE, M	
	20	Het tijdig overbrengen van de permanent te bewaren archiefwaardige informatieobjecten naar het Nationaal Archief	CIO	CVB	DIM	IM, CPO, PJ, JZ, BE, Lead DIM	M	

Bijlage 3 – RASCI Responsibility Matrix Taakverdeling

Bijlage behorende bij art. 5.1 van dit Reglement.

	Categorie		Activiteit	R	A	S	C	I
	2. Overeenkomsten (AVG)	1	Bepalen of en zo ja welke overeenkomst nodig is	BE	CvB	PO	PJ, CPO, FG	
		2	Uitwerken bijlage specificatie verwerkingen	BE	CvB	PO	PJ, CPO, FG	
		3	Uitwerken bijlage contactgegevens	BE	CvB	PO	PJ, CPO, FG	
		4	Uitwerken bijlage informatiebeveiliging	ISO	CvB	PO	PJ, CPO, FG	
		5	Onderhandelen met wederpartij over inhoudelijk aanpassen modelovereenkomsten	BE	CVB	PO	PJ	
		6	Ondertekenen definitieve overeenkomst	BE	CVB			
		7	Ondertekenen definitieve overeenkomst die samenhangt met hoofdovereenkomst waarvoor het CvB tekeningsbevoegd is	CVB	CVB			
		8	Archiveren definitieve overeenkomst	BE	CVB			
		9	Evalueren overeenkomsten	BE	CVB	PO, PJ		FG, CPO, PJ
	3a. Contact AP **3b Contact Inspectie** **Overheidsinformatie & Erfgoed**	10	Contact, overleg en samenwerking met AP Contact, overleg en samenwerking met Inspectie	FG FG/IA	CVB CVB	BE BE, DIM	PJ, CPO A, IM CPO, CISO	PJ, CPO BE
R	**4. Toezicht**	11	Privacy compliance control framework opstellen en bijhouden	CIO	CVB	CPO, PJ	FG	BE, IA
O		12	Interne audits (laten) uitvoeren	FG / IA	CVB		CPO, PJ, CISO, PO	BE
L		13	Implementeren maatregelen die blijkens een audit nodig zijn	BE	CVB	CIO, CPO, PJ, CISO, PO		FG
V		14	Toezien op implementatie maatregelen die blijkens een audit nodig zijn	FG / IA	CVB		BE	
E	**5. Financieen**	15	Gelden en middelen beschikbaar stellen centraal	CVB	CVB		FG, CPO, CISO, PJ	
		16	Indienen begroting mbt gelden en middelen bij CVB	BE	CvB	PO	FG, CPO, CISO, PJ	
		17	Gelden en middelen beschikbaar stellen decentraal	BE	CvB			
		18	Jaarlijkse verantwoording uitgaven aan CVB	BE	CvB	PO		
R	**6a. Beleid**	19	EUR-breed privacy-beleid opstellen en bijhouden (richtlijnen, procedures, reglementen etc.)	CIO / CPO	CVB	PJ	FG, CIO	BE
D		20	Toezien op de naleving van EUR-breed beleid ten aanzien van gegevensbeschermingsbeleid en informatiebeveiligingsbeleid	FG	CVB	BE, CPO, CISO		IA
E		21	Privacy compliance control framework opstellen en bijhouden	CIO / CPO	CVB		FG, PO	BE, IA
L		22	Informatiebeveiligingsbeleid opstellen en bijhouden	CIO / CISO	CVB	ISO	FG	BE, IA
I	**6b. Wet- en Regelgeving**	23	Voldoen aan geldende privacy wet- en regelgeving	BE	CvB	PO	PJ	FG
N		24	EUR-brede impact nieuwe privacy wet- en regelgeving bepalen	CPO, PJ	CVB	PO	FG	BE
		25	Implementeren nieuwe privacy wet- en regelgeving voor eigen eenheid	BE	CVB	PO	CPO, PJ	
G		26	Toezien op de naleving van privacy wet- en regelgeving	FG	CVB	CISO, CIO, CPO		
	6c. Juridische modellen en standaarddocumenten	27	Modellen opstellen en bijhouden	CIO/PJ	CvB		FG	PO, JZ
		28	Modellen binnen de EUR beschikbaar stellen en toelichten	CIO/PJ	CvB	CPO	FG	PO, JZ
	7. Register van verwerkingen	29	Bijhouden structuur register	CPO	CVB	BE	FG	PO
		30	Inventariseren en registreren verwerkingen in register	BE	CVB	PO		FG
		31	Beoordelen en bijhouden van de inhoud van het register (faculteits- of Dienstniveau)	BE	CvB	PO		FG
I		32	Toezien op inhoudelijke kwaliteit register (EUR-breed)	FG	CVB	CPO, PJ, BE, CISO		BE, IA
N	**8. DPIA**	33	Beleid DPIA opstellen, bijhouden en toezien op naleving daarvan (model, proces, toepassingscriteria, goedkeuring etc.)	CIO / CPO	CVB	PO	PJ, FG	PJ, PO, BE
F		34	Beoordelen of een DPIA noodzakelijk is	BE	CVB	PO	CPO, PJ, FG	
		35	DPIA uitvoeren	BE	CVB	PO	CPO, PJ, FG	
O		36	DPIA goedkeuren (nader te specificeren in beleid)	FG	CVB	CPO, PJ, PO	BE	BE
		37	Voorafgaande raadpleging AP	FG	CVB		BE	PJ, CPO
R		38	Implementeren maatregelen die blijkens een DPIA nodig zijn	BE	CVB	PO, PJ, CPO, CIO		FG
		39	Toezien op implementatie maatregelen die blijkens een DPIA nodig zijn	FG	CVB	CISO, CPO	BE	IA
M		40	DPIA archiveren	BE	CVB			
		41	DPIA's evalueren	BE	FG	PO	CPO, PJ	BE

	Categorie		Activiteit	R	A	S	C	I
A	9. Voorafgaande raadpleging	42						
T	10a. Privacy by design	43	Toegangsrechten Privacy periodiek nagaan	PO, ISO	CvB		CISO, CPO	FG
I		44	Periodiek toezien op toegangsrechten	FG / CISO	CVB		CIO	
		45	Implementeren van P & S in bestaande werkprocessen					
		46	Privacy by Design/ Privacy by Default toepassen	BE	CVB	PO	FG	
		47	Toezicht op Privacy by Design en Default	FG	CVB		CIO, CISO	PO, BE, CVB
	11. Beveiligingsmaatregelen	48	Praktisch informatiebeveiligingsadvies	(C)ISO	CvB	FG, CPO, PJ, CIO		
		49	Uitvoering geven aan IB-beleid en IB-advies	BE	CvB		CISO, ISO	
I	11. Beveiligingsmaatregelen	48	Praktisch informatiebeveiligingsadvies	(C)ISO	CvB	FG, CPO, PJ, CIO		
		49	Uitvoering geven aan IB-beleid en IB-advies	BE	CvB		CISO, ISO	
O	12. Datalekken	50	(Vermoeden) melden aan servicedesk IT	BE	CvB	PO	CPO, PJ	FG, CERT
		51	Inventariseren feiten en omstandigheden	FG, CERT	CVB		BE	CISO
N		52	Juridische beoordelen van feiten en omstandigheden	FG	CvB	PJ		BE, CIO
		53	CvB adviseren of er gemeld moet worden of niet aan AP	FG	FG	PJ		
		54	Besluiten of er gemeld moet worden aan AP	CVB	CVB		FG	FG
		55	Melden aan AP	FG	CVB			CIO, CISO, CPO, PJ
		56	Bepalen of er gecommuniceerd moet worden aan betrokkenen	CVB	CVB	PJ	FG	CIO, CISO, CPO, PJ
		57	Communicatie opstellen richting betrokkenen	BE	CVB		FG, WV	
G		58	Communicatie goedkeuren	CVB	CVB		FG, WV	
		59	Communicatie verzenden aan betrokkenen	BE	CvB	PO	FG, WV	CVB, FG, CISO, WV
R		60	Evalueren datalekken	FG	CVB			CPO, PO, CVB,BE , CISO, CIO
C		61	Archiveren besluiten en communicatie	BE	CVB	PO		
	13. Rechten van betrokkenen	62	Beoordelen verzoek	FG	CVB	PO	PJ	
		63	Afhandelen verzoek	BE	CVB	PO	PJ	FG
		64	Registreren verzoek	BE	CVB	PO		
		65	Opstellen antwoord op verzoek	BE	CVB	PO	PJ	
		66	Ondertekenen besluit (Awb)	CVB	CVB		FG, PJ	BE
R		67	Verzenden antwoord op verzoek	BE	CVB	PO		FG
		68	Processen m.b.t. rechten van betrokkenen opstellen en onderhouden	CIO / PJ, CPO, JZ	CVB	PO	FG	BE, PO, FG
E	14. Bewustmaking en opleiding	69	EUR-brede (bewustzijns)campagnes	CIO, CPO, PJ, CISO	CVB		FG, MC	BE
		70	Opleidingen PO	CPO, PJ	CVB		FG, CISO	BE
G		71	Trainingen (onderdelen Beheerseenheden) geven	BE	CvB	PO, CPO, PJ, MC	FG	
L	15. Samenwerking Beheerseenheden	72	Bevorderen efficiency & uniformiteit	BE	CvB	CPO, CISO	PJ	FG
	16. Inkopen	73	Koopt diensten, werken en leveringen in, conform het opgestelde in het Inkoopbeleid, waarbij de inbedding van Gegevensbescherming en Informatiebeveiliging wordt geborgd	BE	CVB	PO	FG, CISO, PJ, Inkoop *, JZ	
E	17. Beheer archiefwaardige informatieobjecten	74		BE	CVB	DIM,	A, IM, CPO, CISO	CIO, M
M	18. Overzicht houden van de archiefwaardige informatieobjecten	75		BE	CvB	DIM,	IM, A, Lead DIM	CIO, CPO, CISO
E	19. Vernietiging archiefwaardige informatieobjecten	76		BE	CVB	DIM,	A, IM, CPO, CISO, Lead DIM, TB, FB	BE, M
N	20. Overbrengen naar Nationaal Archief	77		CIO	CvB	DIM	IM, CPO, CISO, Lead DIM, PJ, JZ, BE	M
T								