Aventus

De school waar jij ’t maakt

Informatiebeveiliging en privacy beleid

Aventus

Versiebeheer

Versie	Datum	Auteur
1.0	18-09-2009	F.Y. Poon
2.0	25-04-2014	F.Y. Poon
3.0	03-07-2017	Vastgesteld door CVB
4.0 Wijzigingen n.a.v. AVG	24-09-2019	F.Y. Poon en N. Dutij
5.0	14-03-2023	Vastgesteld door CVB

1. Verantwoording en richtlijnen

1.1. Het belang van informatiebeveiliging en privacy, meer dan ICT

Privacy wordt voor studenten en medewerkers steeds belangrijker. Incidenten bij andere onderwijsinstellingen onderstrepen de noodzaak om goed en zorgvuldig met onze gegevens om te gaan. Informatiebeveiliging en privacy is niet meer enkel een aangelegenheid voor ICT, maar is voor al onze medewerkers een verantwoordelijkheid. Alleen samen kunnen wij onze school veilig houden.

Informatiebeveiliging en privacy is voor alle medewerkers relevant. Niet alleen in de digitale wereld, maar ook in de fysieke wereld is het belangrijk om goed om te gaan met gegevens van medewerkers, studenten en andere betrokkenen. Het uitlekken van documenten, het reageren op een phishing-mail of het kwijtraken van USB-sticks zijn alledaagse voorbeelden die schade kunnen toebrengen aan Aventus. In dit beleid omschrijven wij de uitgangspunten om Aventus veilig en AVG-proof te houden.

Het onderwijs is daarnaast in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan, met name ook van minderjarigen[1]. Informatiebeveiliging en privacy gaat niet alleen om digitale gegevens, maar ook om gegevens die op papier staan. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

1.2. Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.
Informatiebeveiliging richt zich op de volgende aspecten:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten volledig, juist en actueel zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades, boetes en imagoverlies.

1.3. Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:
Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens[2].

1.4. Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één geheel:

[1] Groene woorden worden in bijlage 3 (Verklarende woordenlijst) toegelicht

[2] Bewerkt artikel 2, lid 2 van de AVG.

IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis om informatiebeveiliging en privacy binnen Aventus te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

1.5. Doel

Het IBP- beleid heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen van wie Aventus persoonsgegevens verwerkt, waaronder studenten, hun ouders/verzorgers en medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het IBP-beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, studenten en hun ouders/verzorgers) wordt gerespecteerd en Aventus voldoet aan relevante wet- en regelgeving.

1.6. Reikwijdte

- Het IBP-beleid binnen Aventus geldt voor alle betrokkenen, te weten: medewerkers, studenten, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/ outsourcing).

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Aventus. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken (b.v. uitspraken van medewerkers, op (persoonlijke pagina's van) websites en of social media.). Onder dit beleid vallen ook alle (BYOD)-devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.

- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Aventus evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- Aventus laat door haar leveranciers ook persoonsgegevens verwerken, deze gegevens dienen door de leveranciers goed beschermd te worden conform ons IBP-beleid. Ons IBP-beleid eist dan ook dat wij verwerkersovereenkomsten afsluiten met onze leveranciers waar dit van toepassing is en hun diensten ook periodiek te beoordelen.

- IBP-beleid heeft binnen Aventus raakvlakken met:
  - *Algemene beleidsstukken rondom veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen.
  - *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.
  - *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen
  - *Medezeggenschap* van studenten, hun ouders/verzorgers en medewerkers.

1.7. Concretisering[3]

Aventus hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het **College van Bestuur** van Aventus neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de **verwerkingsverantwoordelijke**.

[3] Deze uitgangspunten zijn operationeel uitgewerkt en toegelicht in bijlage 1.

2. Aventus voldoet aan alle **relevante wet- en regelgeving**.

3. Bij Aventus is de verwerking van persoonsgegevens altijd gekoppeld aan een **specifiek doel** en gebaseerd op één van de **wettelijke grondslagen**. Een goede balans tussen het belang van Aventus om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming in- en herzien.

4. Aventus zal alle **betrokkenen helder en actief informeren** over de verwerkingen van hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, aanvullen, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit, afscherming en profilering van hun persoonsgegevens. Dit betekent dat wij met privacy-verklaringen onze betrokkenen informeren, maar ook dat alle organisatorische eenheden transparant in hun documenten informatie verschaffen over de omgang met gegevens aan betrokkenen.

5. Aventus legt alle **verwerkingen van persoonsgegevens** vast in een **dataregister** en zal deze up-to-date houden. Aventus voldoet hiermee aan de documentatieplicht, zoals benoemd in de AVG.

6. Binnen Aventus is het **veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van eenieder**. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.

7. Aventus is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het **eigendom** (auteursrecht) **toebehoort aan derden**. Medewerkers en studenten worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie door de afdeling HRM. Het intellectueel eigendom van ontwikkelde zaken door medewerkers (zoals ontwikkeld lesmateriaal, maar ook andersoortige systemen, methodes en documenten) blijft bij Aventus.

8. Aventus **classificeert informatie en informatiesystemen**. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.

9. Aventus sluit met **alle leveranciers van digitale middelen** (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken.

10. Aventus verwacht van alle **medewerkers, studenten, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen** met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Aventus heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. **Informatiebeveiliging en privacy is bij Aventus een continu kwaliteitsproces**, waarbij regelmatig (minimaal jaarlijks) wordt ge-audit of een self assessment wordt uitgevoerd en wordt gekeken of een aanpassing gewenst dan wel noodzakelijk is.

12. Aventus kijkt bij **wijzigingen** (denk ook aan uitfasering) in de infrastructuur of de **aanschaf van nieuwe (informatie)systemen** vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

13. Aventus neemt **passende organisatorische of technische (beveiligings-)maatregelen** om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.

14. Aventus zal alle **beveiligingsincidenten en datalekken** vastleggen, volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

15. Aventus kiest ten aanzien van informatiebeveiliging (**autorisatie en authenticatie**) voor de vooronderstelling "Alles is in principe verboden tenzij het uitdrukkelijk is toegelaten"[4] in plaats van de zwakkere regel "Alles is in principe toegelaten tenzij het uitdrukkelijk is verboden".

[4] Op basis van functie/rollen worden rechten door de leidinggevende toegekend. Een functioneel beheerder kent de rechten feitelijk toe. Bijvoorbeeld: een HR adviseur mag alleen de dossiers van de aan hem/haar toegewezen medewerkers inzien, als dat noodzakelijk is vanwege de opgedragen werkzaamheden.

2. Compliance

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

2.1. Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet Educatie en Beroepsonderwijs (WEB)
- Branche code Goed Bestuur MBO, MBO Raad
- Wet Inspectietoezicht
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Archiefwet
- Auteurswet
- Wetboek van Strafrecht
- Koppelingswet

Het internationale normenkader voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.
Aventus hanteert het Toetsingskader Informatiebeveiliging en Privacy dat ontwikkeld is door MBO-Raad (saMBO-ICT). Ook hanteert Aventus het NBA (Nederlandse Beroepsvereniging van Accountants) toetsingskader als self assessment tool.

2.2. Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens te weten:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld, inclusief de bewaartermijnen. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.

3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Transparantie**: de school legt aan betrokkenen (studenten, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast informatie, inzage, verbetering, aanvullen, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit, afscherming en profilering van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.

5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens volledig, juist en actueel zijn.

2.3. Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 2 geeft een overzicht van de diverse aanvullende besluiten rondom IBP. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

2.4. Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd op basis van het ROSA model.[5] Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses door de afdeling I&A. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitscriteria die van belang zijn.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden middels een centraal ingeregeld DPIA (Data Protection Impact Assessment). Vanaf de start van nieuwe (ICT)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

2.5. Incidenten en datalekken

Alle medewerkers die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings-)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings-)incidenten kunnen worden gemeld via het Selfserviceportal.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.
Studenten en externen kunnen kwetsbaarheden melden bij **Privacy@aventus.nl**.

2.6. Planning en controle

Dit IBP-beleid wordt jaarlijks gereviewed en eventueel bijgesteld door het bestuur. Hierbij wordt rekening gehouden met:

- de status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
- de actuele geinventariseerde risico's;
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan.

Daarnaast kent Aventus een jaarlijkse jaarplan voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het IBP-beleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen. Een en ander leidt tot een jaarplan IBP.

2.7. Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Naleving van ons IBP-beleid is een primaire verantwoordelijkheid van alle medewerkers binnen Aventus. Daarboven nemen de leidinggevenden en proceseigenaren hun verantwoordelijkheid om hun medewerkers aan te spreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, d.m.v. een instelling brede gedragscode, d.m.v. periodieke bewustwordingscampagnes, et cetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.
Mocht de naleving van dit beleid ernstig tekortschieten, dan kan Aventus de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

[5] https://www.edustandaard.nl/standaard_afspraken/certificeringsschema-informatiebeveiliging-en-privacy-rosa/certificeringsschema-informatiebeveiliging-en-privacy-rosa-v3-0/

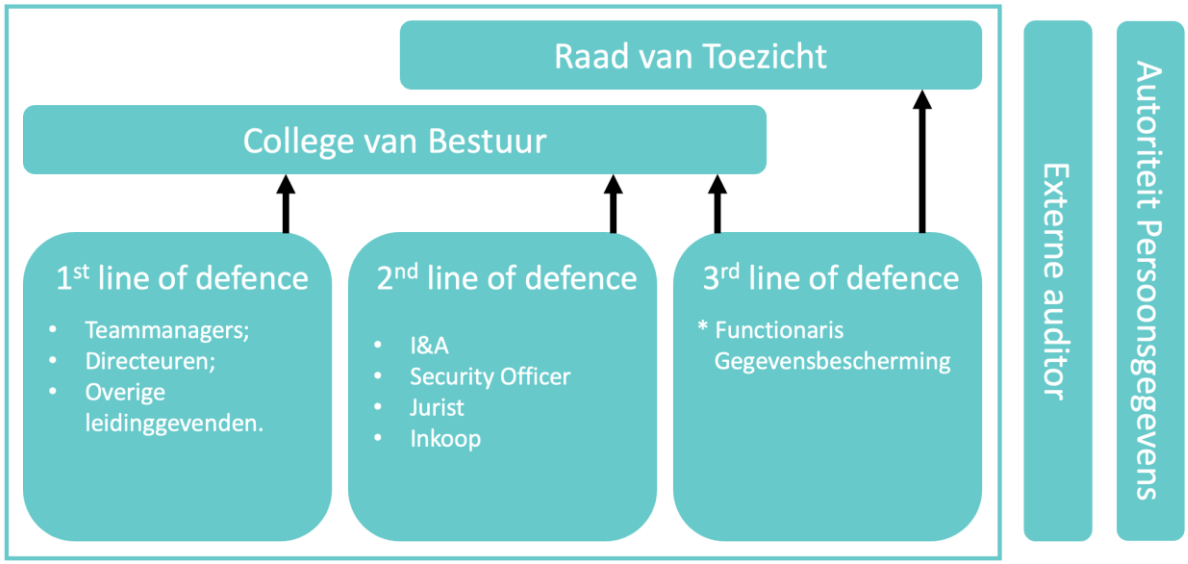
2.8. Logging en monitoring

Logging en monitoring door de afdeling I&A en de applicatie-eigenaar zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk. Aventus zal deze logging regelmatig beoordelen.

3. Governance

3.1. Rollen en verantwoordelijkheden

Aventus hanteert het three lines of defense model. De eerste lijn binnen dit model is cruciaal, immers de directeuren en teamleiders moeten erop toezien dat het IBP-beleid wordt nageleefd. Daartoe zijn alle leidinggevenden geschoold en zij zien erop toe dat al hun teamleden handelen volgens het vastgesteld IBP-beleid. Schematisch als volgt weergegeven.



3.2. De first line of defense: (leidinggevenden)

De eerste lijn bewaakt het IBP-beleid binnen hun eigen organisatorische onderdeel (bijvoorbeeld onderwijs). Onderwijsdirecteur, coördinatoren, teamleiders vormen de first line of defense als het gaat om de bescherming van persoonsgegevens. Zij voeren daarbij de volgende taken uit:

- toetsen dat nieuwe applicaties en functionele uitbreidingen van bestaande applicaties worden voorgelegd aan wijzigingsbeheer (onderdeel I&A);
- toetsen dat nieuwe of gewijzigde gegevensverwerkingen voldoen aan de AVG;
- toetsen dat een Verwerkersovereenkomst of een Gezamenlijk Verantwoordelijkenovereenkomst wordt afgesloten als persoonsgegevens worden overgedragen aan externe partijen. Verwerkersovereenkomsten worden enkel getekend door de directeur BVO of het College van Bestuur;
- beoordelen van incidenten rond persoonsgegevens en het intern melden daarvan als het vermoeden bestaat dat het gaat om een datalek;
- toetsen dat hun medewerkers voldoende geschoold zijn in het kader van de AVG;
- vastleggen van de extra taken en rollen van medewerkers en de daarbij behorende rechten binnen de bijbehorende systemen/processen.

3.3. De second line of defense: I&A, Jurist, Inkoop en Security Officer

De second line monitort de toepassing en naleving van het informatiebeveiligings- en privacybeleid, adviseert, gevraagd en ongevraagd, over informatiebeveiliging en privacybescherming en ondersteunt de first line. De second line ontwikkelt waar nodig beleid op het gebied van informatiebeveiliging en privacy, het College van Bestuur stelt dit beleid vast.

3.4. De third line of defense: de Functionaris voor Gegevensbescherming

Aventus heeft een interne toezichthouder op de verwerking van persoonsgegevens aangesteld. Deze toezichthouder wordt functionaris voor gegevensbescherming genoemd (hierna: "FG"). De FG zal door Aventus tijdig worden betrokken bij alle aangelegenheden waar persoonsgegevens bij komen kijken. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie binnen Aventus. Aventus heeft de FG aangemeld bij de nationale toezichthoudende autoriteit, de zogenaamde Autoriteit Persoonsgegevens.
De taken van de FG houden in:

- het informeren en adviseren van alle betrokken partijen over hun verplichtingen onder de AVG,
- het toezien op de naleving van de AVG en andere relevante privacywetgeving,
- het toezien op de naleving van dit IBP beleid door Aventus,
- het toezien op een Data Protection Impact Assessment,
- het behandelen van klachten over de toepassing van het privacyreglement,
- fungeren als eerste aanspreekpunt voor en samenwerken met de Autoriteit Persoonsgegevens.

3.5. De taken van de medewerkers

Onderwerp	1st line of defence	2nd line of defence	3rd line of defence
Applicaties	Verantwoordelijk leidinggevende toetst nieuwe applicaties bij I&A.	I&A controleert op ICT- en AVG-aspecten. Inkoop, jurist of security officer toetst of nieuwe applicaties passen binnen het inkoopbeleid.	De FG toetst of het juiste proces wordt uitgevoerd.
Autorisaties	Leidinggevenden hebben in kaart welke autorisaties hun medewerkers hebben en geven wijzigingen hiervan door.	I&A controleert of aangevraagde rechten voldoen aan het IBP-beleid.	De FG controleert of de autorisaties zijn ingericht op basis van *need-to-know* en *least privilege*.
Bewaartermijn	Leidinggevenden zijn verantwoordelijk voor het handhaven van de bewaartermijnen conform het Documentair StructuurPlan (DSP) binnen hun eigen organisatorische eenheid.	I&A / Jurist adviseert aan de hand van de het Documentair StructuurPlan (DSP) de 1st line over de geldende bewaartermijnen.	De FG ziet erop toe dat de bewaartermijnen worden nageleefd.
Naleving beleid	Leidinggevenden zien erop toe dat het beleid wordt uitgevoerd binnen hun organisatorische eenheid.	I&A, jurist en inkoop adviseert over probleempunten bij naleving beleid.	De FG toetst of de toegewezen taken worden uitgevoerd.
Datalekken	Medewerkers melden zelf intern een datalek via Selfservice. De leidinggevende draagt zorg voor bekendheid van de meldprocedure en scholing van haar medewerkers.	I&A maakt een inschatting van het datalek en betrekt de FG en onderneemt acties conform het beleid datalekken.	De FG besluit, na overleg met het CvB, om al dan niet het datalek bij de AP en/of de betrokkenen te melden.
Gegevensverwerkingen	Leidinggevenden zien erop toe dat gegevensverwerkingen voldoen aan de AVG. Dit betreft mede het intern als extern delen van gegevens.	I&A adviseert waar nodig over de mogelijkheden van de (voorgenomen) gegevensverwerking.	De FG toetst of de toegewezen taken worden nageleefd.

3.6. Implementatie beleid

Het College van Bestuur is verantwoordelijk voor de verwerkingen van persoonsgegevens binnen Aventus. Het College van Bestuur wordt aangemerkt als de verwerkingsverantwoordelijke in de zin van de wet AVG. De verantwoordelijkheid houdt kort samengevat in:

- dat de persoonsgegevens verwerkt worden in overeenstemming met de vastgestelde doelen van de verwerking, dat die doelen gerechtvaardigd zijn en dat de verwerking zorgvuldig gebeurt,
- dat hierover verantwoording kan worden afgelegd aan de Autoriteit Persoonsgegevens.

De feitelijke verwerking van persoonsgegevens wordt echter op allerlei lagen van Aventus uitgevoerd. Het is niet één instituut of dienst die effectief verantwoordelijk kan zijn voor alle persoonsgegevens die Aventus verwerkt.

3.7. Inpassing in de instellingsgovernance en afstemming met aanpalende beleidsterreinen

Om de samenhang in de organisatie met betrekking tot gegevensbescherming goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van verwerking van persoonsgegevens binnen de verschillende onderdelen op elkaar af te stemmen, is het belangrijk om gestructureerd overleg te voeren over het onderwerp privacy op verschillende niveaus.

Op strategisch niveau wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van privacyaspecten.

Op tactisch niveau wordt de strategie vertaald naar plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering.

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan. Het operationeel niveau wordt ingevuld door de leidinggevenden binnen hun organisatorische eenheid.

3.8. Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van persoonsgegevens uit te sluiten. Noodzakelijk is het om het bewustzijn voortdurend aan te scherpen, zodat bij Aventus kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordings-campagnes voor medewerkers, studenten en relaties. Verhoging van het bewustzijn is de verantwoordelijkheid van elke leidinggevende en wordt gefaciliteerd door I&A en Marketing en Communicatie. Daarnaast is HRM verantwoordelijk voor het faciliteren van scholing van de medewerkers .

3.9. Controle en naleving

Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens.

Mocht de naleving op de bescherming van data- en privacygegevens ernstig tekortschieten, dan kan Aventus de betrokken verantwoordelijke medewerkers een maatregel opleggen, binnen de kaders cao-mbo en de wettelijke mogelijkheden.

Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten Aventus maken het noodzakelijk om periodiek te bezien of men nog voldoende op koers zit met het beleid.

Bijlage 1: Verklarende woordenlijst

AVG:	Algemene Verordening Gegevensbescherming.
Beleid:	Beleid met betrekking tot het verwerken van persoonsgegevens door Aventus.
Betrokkene:	Een individueel en natuurlijk persoon op wie een persoonsgegeven betrekking heeft.
Datalek:	Een inbreuk in verband met persoonsgegevens, die leidt tot enige ongeoorloofde verwerking daarvan. Hier vallen zowel opzettelijke als onopzettelijke inbreuken onder.
Dataportabiliteit:	Het recht om persoonsgegevens en informatie over te dragen aan een nieuwe verwerker zonder technische problemen.
Dataregister:	De AVG spreekt van het Register van Verwerkingsactiviteiten, dit is een overzicht van de persoonsgegevens die verwerkt worden, met informatie over het doel daarvan, de grondslag daarvoor, de bewaartermijnen van de gegevens en bron of ontvanger van de gegevens. Aventus heeft drie centrale registers: dat voor studentgegevens, voor medewerkergegevens en voor relatiegegevens. Het dataregister is het Register van Verwerkingsactiviteiten aangevuld met de BIV-classificatie en de autorisatie matrix op hoofdlijnen.
DPIA:	Data Protection Impact Assessment (Gegevensbeschermingseffectbeoordeling): een beoordeling die helpt bij het identificeren van privacy risico's en de handvaten levert om deze risico's te verkleinen tot een acceptabel niveau. Soms ook wordt de term PIA gebruikt, Privacy Impact Assessment.
Functionaris voor Gegevensbescherming:	Interne toezichthouder en privacy adviseur aangesteld door het College van Bestuur, op grond van artikel 37 van de AVG, ook wel aangeduid als FG.
Kernsystemen:	De hoofdsystemen voor: SIS, HR, Financiën, Rooster, ELO, MIS, CRM, IDM, Office en ARBO.
Minderjarige:	Voor de AVG: iedere persoon die de leeftijd van 16 jaar nog niet heeft bereikt. Buiten de AVG geldt uiteraard jonger dan 18 jaar.
Niet-geautomatiseerde verwerking:	Voorbeelden: aangetekende stukken, pasjes die zichtbaar gedragen worden, klassenlijsten met foto's (smoelenboek), etc.
Persoonsgegeven:	Elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon.
Verwerker:	Een door Aventus ingeschakelde (derde) partij die ten behoeve van Aventus, en op basis van haar schriftelijke instructies, persoonsgegevens verwerkt, e.e.a. vastgelegd in een verwerkersovereenkomst.
Verwerking:	Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, afschermen, wissen of vernietigen van gegevens.
Verwerkingsverantwoordelijke:	College van Bestuur van Aventus dat het doel en de middelen van de verwerking van persoonsgegevens vaststelt.

Bijlage 2: Besluitenlijst

Deze besluitenlijst geeft een aantal besluiten van Aventus rondom IBP, maar deze besluitenlijst is niet limitatief. Er kunnen nog aanvullende beleidsstukken rondom IBP worden gehanteerd, bijvoorbeeld het beleid datalekken.

Besluit 1: Mobiele apparatuur.
Voor mobiele apparatuur geldt de 3 Treden regeling:
Trede 1 - Gebruik de applicatie

Persoonsgegevens worden zoveel als mogelijk opgeslagen in de applicaties.
Toelichting: persoonsgegevens in applicaties zijn in het algemeen goed beveiligd door toekenning van rollen en rechten en een persoonlijke account.

Trede 2 - Gebruik het Aventus opslag aanbod (bijvoorbeeld: SharePoint, Teams, OneDrive)

Het kan noodzakelijk zijn om persoonsgegevens verder te verwerken, terwijl dat niet in de hiertoe aangewezen applicatie kan. Voor de opslagen van dergelijke verder verwerkte gegevens kan het netwerk gebruikt worden.

Trede 3 - Gebruik encryptie

Is het lokaal opslaan van persoonsgegevens op eigen apparatuur (zoals de BYOD-apparatuur) onvermijdelijk dan geldt: gebruik wachtwoordbeveiliging en encryptie als je gegevens op bijvoorbeeld je eigen device of een USB-stick of een externe harde schijf plaatst.

Samenvattend:
- Persoonsgegevens worden opgeslagen in centrale versleutelde databases, indien dit niet mogelijk is dan encrypted opslaan op een device (bijv. usb).
- Aventus maakt gebruik van een versleutelprogramma (bijv. Bitlocker).
- Encryptie-sleutels worden opgeslagen bij I&A.

Besluit 2: Classificatiemodel.
Aventus hanteert het ROSA classificatiemodel en de uitkomsten van de classificatie worden openomen in het dataregister. Aventus classificeert de data in het dataregister, waarbij de uitkomsten worden gebruikt voor de beoordeling van applicaties.

Besluit 3: Bewaartermijnen.
Aventus hanteert het DSP (Documentair Structuur Plan) van de MBO Raad.

Besluit 4: Lidmaatschap IBP-netwerk, SCIRT en SCIPR.
Aventus is actief lid van communities op gebied van IBP, bijvoorbeeld MBO-Digitaal, IBP-Netwerk MBO-Digitaal, SCIPR en SCIRT.

Besluit 5: Muti-factor authenticatie
Voor applicaties met een hoge vertrouwelijkheid (conform ROSA Classificatiemodel) wordt gebruik gemaakt van Multi-factorauthenticatie.

Besluit 6: Responsible disclosure procedure.
Hackers kunnen (op ethisch verantwoorde wijze) kwetsbaarheden ontdekken in onze beveiliging. Daar kunnen we van leren en mogelijke schade voorkomen. Wij vragen aan de hacker om aan onderstaande regels te voldoen. Als een ethische hacker aan deze regels voldoet, zullen wij geen aangifte bij de politie doen.

Wat wij van de hacker eisen:
- *Geen openbaarmaking of wijziging van onze gegevens;*

- *Geen schade berokkenen aan Aventus op enige manier, waaronder het maken van een inbreuk op de beschikbaarheid, integriteit of vertrouwelijkheid van gegevens of systemen.*
- *Onze gegevens en/of de kwetsbaarheid niet delen met anderen;*
- *Ons zo snel mogelijk (maar uiterlijk binnen 24 uur) en zo volledig mogelijk informeren op **Privacy@aventus.nl**;*
- *Geen gebruik te maken van deze gegevens door bijvoorbeeld extracties te maken van de database of andere handelingen met de gegevens uit te voeren; dat de hacker de gegevens zo spoedig mogelijk en volledig verwijderd van zijn/haar systemen inclusief back-up voorzieningen;*
- *Aventus inzicht te geven in de wijze van hacken;*
- *Aventus inzicht te geven in de details van de gehackte informatie.*
- *Aventus keert geen beloningen uit aan de hackers.*

Wat wij de hacker beloven:
- *We ondernemen geen juridische stappen;*
- *We reageren binnen 5 werkdagen;*
- *We handelen dit vertrouwelijk af;*
- *We houden hem/haar op de hoogte.*

Dit beleid is gepubliceerd op de openbare website van Aventus.

Besluit 7: Clean desk, Clear screen.

Clear Screen:
Medewerkers dienen hun laptop, computers of andere (BYOD)-device te vergrendelen, zodra zij hun device achterlaten. Medewerkers dienen dit bijvoorbeeld te doen als zij een kop koffie gaan halen, naar het toilet gaan etc. Een device mag niet onvergrendeld toegankelijk zijn voor studenten en collega's of andere derden.

Technisch afdwingen:
I&A is verantwoordelijk om apparatuur die in beheer is van Aventus automatisch na maximaal 10 minuten inactiviteit te vergrendelen.

Clean desk:
Medewerkers zijn verplicht om privacygevoelige informatie en bedrijfskritische informatie in een afgesloten omgeving op te slaan. Medewerkers mogen dit niet op hun bureau onbeheerd laten liggen. Medewerkers zijn verplicht de aangewezen kasten te gebruiken voor de opslag van hun fysieke documenten en dienen deze kasten ook telkens af te sluiten.

De leidinggevende is verantwoordelijk voor een goede uitvoering van het clean-desk, Clear-screenbeleid.

Veilige papierafvoer en papierversnipperaars
Medewerkers zijn verplicht gebruik te maken van de afgesloten en beveiligde papiercontainers, indien zij fysieke documenten met persoonsgegevens willen weggooien. Aventus zal hiervoor iedere locatie voorzien van een papierversnipperaar of een mogelijkheid tot het veilig afvoeren van papier.

Besluit 8: Back-up van informatie.
Aventus heeft als back-up beleid het uitgangspunt dat de eisen worden overgenomen conform het ROSA-classificatiekader. Voor de kernsystemen van Aventus geldt aanvullend in ieder geval
- Een verplichting om afspraken vast te leggen in een Service Level Agreement;
- Een verplichting aan de zijde van de leverancier om tenminste 1 keer per dag een back-up te maken;
- De Recovery Point Objective is maximaal 1 uur;
- Viermaal per jaar dient leverancier een restore test uit te voeren;
- Afspraken van de leverancier dienen gecontroleerd te kunnen worden.

Besluit 9 Logging.
Aventus logt in ieder geval de werking en het gebruik van de top 10 aan kernsystemen. Logging wordt toegepast met de volgende doelstellingen:

- Ontdekken van fouten in soft- en hardware (security, IBP gerelateerd);
- Ontdekken van fouten door menselijk handelen (misbruik gerelateerd);
- Ontdekken van indringers (niet realtime, maar na analyse van logs);
- Ondersteunen bij forensisch onderzoek.

Algemeen
Het raadplegen van de technische logbestanden kan alleen door I&A Bij het toepassen van logging gelden de volgende regels:

- Het toepassen van logging is in ieder geval verplicht op onze kernsystemen.
- Het actief zijn van de logging-services wordt gemonitord.
- Logbestanden worden maximaal 3 maanden bewaard, tenzij een incident het noodzaakt om logging langer te bewaren. Specifieke logbestanden kunnen langer bewaard blijven bijv. t.b.v. een forensisch onderzoek.
- Er is een automatische en tijdige signalering van het vollopen van log-opslagruimte.
- Het handmatig verwijderen en wijzigen van logbestanden wordt gelogd.
- Er is geen logging van gegevens waarmee beveiliging kan worden doorbroken (wachtwoorden).
- Leveranciers moeten mogelijkheden bieden om logging te kunnen (laten) controleren.
- Logging van de kernsystemen wordt op basis van een deelwaarneming en regelmatig gecontroleerd op onregelmatigheden conform het informatiebeveiligings- en privacy beleid.

Te loggen gegevens
De volgende gegevens worden in ieder geval gelogd binnen de kernsystemen:

- het inloggen/uitloggen van een gebruiker;
- autorisatie-wijzigingen;
- het raadplegen/wijzigen van gevoelige gegevens, waarbij gegevens met een categorie Hoog op het dataregister van toepassing is.

Besluit 10: Calamiteitenplan ICT

- Het calamiteitenplan sluit aan bij het wettelijke calamiteitenplan van Aventus.
- Bij datalekken geldt het beleid datalekken van Aventus.