Beleid IBP

Beleid InformatieBeveiliging & Privacy

SiNTLUCAS
CREATING OPPORTUNITIES

Inhoud

1. VERANTWOORDING EN RICHTLIJNEN 4
1.1 Wat is informatiebeveiliging en privacy? 4
1.2 Het belang van informatiebeveiliging en privacy 4
1.3 Vervlechting informatiebeveiliging en privacy 4
1.4 Doel 5
1.5 Reikwijdte 5
1.6 Concretisering 5
2. COMPLIANCE 7
2.1 Relevante wet- en regelgeving 7
2.2 Basisregels bij het omgaan met persoonsgegevens 7
2.3 Ondersteunende richtlijnen en procedures 7
2.4 Classificatie en risicoanalyse 8
2.5 Beveiligingsincidenten en datalekken 8
2.6 Planning en controle 8
2.7 Naleving en sancties 8
2.8 Logging en monitoring 9
3. GOVERNANCE 10
3.1 Rollen en verantwoordelijkheden 10
3.2 De first line of defence: directeuren, managers, IV, Inkoop, FD en ICT 10
3.3 De second line of defence: manager Informatievoorziening, ISO en PO 10
3.4 De third line of defence: de Functionaris voor de Gegevensbescherming en Control 11
3.5 De taken van de medewerkers 11
3.6 Implementatie beleid 14
3.7 Persoonsgegevens 14
3.8 Verdeling van de verantwoordelijkheden 14
3.9 Inpassing in de instellingsgovernance en afstemming met aanpalende beleidsterreinen 14
3.10 Bewustwording en training 15
3.11 Controle en naleving 15
Bijlage 1: Ondersteunende documenten 16
Bijlage 2: Besluitenlijst 17
Bijlage 3: Verklarende woordenlijst 20

Auteur	Erwin Huggers
Versie	4.1
Versiedatum	17 juli 2023
Status document	Goedgekeurd CD 2 oktober 2023 / Instemming OR 13 december 2023
Opdrachtgever	Ruud Rabelink

1. Verantwoording en richtlijnen

1.1 Wat is informatiebeveiliging en privacy?

Informatiebeveiliging en privacy (afgekort tot IBP) is het geheel van maatregelen, richtlijnen en procedures voor informatie en informatiesystemen, gericht op het waarborgen van de beschikbaarheid, betrouwbaarheid en integriteit van informatie en systemen en het minimaliseren van schade. De drie kernbegrippen verhouden zich als volgt tot informatiebeveiliging:

- Beschikbaarheid: de mate waarin informatie en systemen op het gewenste moment toegankelijk zijn voor gebruikers.
- Vertrouwelijkheid: de mate waarin de toegang tot informatie en systemen beperkt is tot een vastgestelde groep van gebruikers.
- Integriteit: de mate waarin informatie en systemen geen fouten bevatten.

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving (AVG). 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*[1].

1.2 Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door onder andere 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[2]. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging en privacy door IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en bijvoorbeeld de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen, en schade in de persoonlijke levenssfeer van betrokkenen (leerlingen/studenten, ouders en medewerkers) te voorkomen.

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

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

[1] Bewerkt artikel 2, lid 2 van de AVG.
[2] Groene woorden worden in bijlage 3 (Verklarende woordenlijst) toegelicht

1.4 Doel

Informatiebeveiliging en privacy 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 SintLucas persoonsgegevens verwerkt, waaronder studenten/leerlingen, hun ouders/verzorgers en (gast)medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (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 (onder andere medewerkers, studenten/leerlingen en hun ouders/verzorgers) wordt gerespecteerd en SintLucas voldoet aan relevante wet- en regelgeving.

1.5 Reikwijdte

- Het IBP-beleid binnen SintLucas geldt voor alle betrokkenen, te weten: leerlingen/studenten, ouders/verzorgers, medewerkers, maar ook (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing) waarmee wordt samengewerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van SintLucas. Hieronder valt tevens de gecontroleerde informatie, die door de SintLucas zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop SintLucas kan worden aangesproken (bijvoorbeeld uitspraken van medewerkers, op (persoonlijke pagina's van) websites en of social media.). Onder dit beleid vallen ook alle 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 SintLucas 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.

- IBP-beleid heeft binnen SintLucas raakvlakken met:
  - *Integraal veiligheidsplan;* waarin een verbinding gemaakt wordt tussen Informatieveiligheid, Sociale veiligheid en Fysieke veiligheid met o.a. 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.
  - *ICT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen
  - *Medezeggenschap* van studenten, leerlingen en hun ouders/verzorgers en medewerkers.

1.6 Concretisering[3]

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

1. Het college van bestuur van SintLucas 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.
2. SintLucas voldoet aan alle relevante wet- en regelgeving.
3. Bij SintLucas is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen[4]. Een goede balans tussen het belang van

[3] Deze uitgangspunten zijn operationeel uitgewerkt en toegelicht in bijlage 1.
[4] In artikel 6 van de AVG staat dat de verwerking alleen rechtmatig is als er aan ten minste een van de grondslagen wordt voldaan. De grondslagen zijn toestemming, vitaal belang, wettelijke verplichting, overeenkomst, algemeen belang of gerechtvaardigd belang. Meer informatie op https://www.charlotteslaw.nl/de-6-grondslagen-van-de-avg/

SintLucas 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 te allen tijde hun toestemming in- en herzien.

4. SintLucas zal alle betrokkenen helder en actief informeren over de verwerkingen van hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen (medewerkers, studenten, leerlingen, externen) 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.
5. SintLucas legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. SintLucas voldoet hiermee aan de documentatieplicht, zoals benoemd in de AVG.
6. Binnen SintLucas 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. SintLucas 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 en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
8. SintLucas 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. SintLucas sluit met alle leveranciers van digitale (onderwijs)middelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken.
10. SintLucas verwacht van alle medewerkers, studenten, leerlingen, (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. SintLucas heeft hiervoor een gedragscode[5] geformuleerd, vastgesteld en geïmplementeerd.
11. Informatiebeveiliging en privacy is bij SintLucas 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. SintLucas 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. SintLucas 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. SintLucas zal alle beveiligingsincidenten en datalekken vastleggen, volgens een vast protocol[6] afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.
15. SintLucas kiest ten aanzien van informatiebeveiliging (autorisatie en authenticatie) voor de vooronderstelling "Standaard geen toegang tenzij het uitdrukkelijk is toegelaten"[7] in plaats van de zwakkere regel "Standaard toegang tenzij het uitdrukkelijk niet is toegestaan".

[5] Richtlijn verantwoord digitaal werken, te vinden in Weten & Regelen van MijnLucas
[6] Draaiboek beveiligingsincidenten en datalekken, te vinden in Weten & Regelen van MijnLucas
[7] 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. Beleid voor IAA, te vinden in Weten & Regelen van MijnLucas

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 Beroepsvorming (WEB).
- Branche code Goed Bestuur MBO, MBO Raad.
- Wet Inspectietoezicht.
- Algemene Verordening Gegevensbescherming (AVG).
- Archiefwet.
- Auteurswet.
- Wetboek van Strafrecht.
- Wijzigingswet Vreemdelingenwet: Koppelingswet.

Het NBA-normenkader (Nederlandse Beroepsvereniging van Accountants[8]) is leidend voor de te nemen beveiligingsmaatregelen. SintLucas hanteert dit normenkader dat gespecificeerd is door MBO Raad (MBO Digitaal) en neemt periodiek deel aan de peer-review georganiseerd vanuit MBO Digitaal.

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, leerlingen, 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 1 geeft een overzicht van de diverse aanvullende documenten. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

[8] Beter bekend is als NBA-LIO (en NOREA) Volwassenheidsmodel v.2.1, afkomstig van de Nederlandse Beroepsvereniging van Accountants en Ledengroep Intern en Overheidsaccountant

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. 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. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitscriteria die van belang zijn. Daarnaast maken we gebruik van de MORA om processen en gebruik van informatie te beschrijven.

Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf, via een centraal ingeregeld Pre-DPIA (Data Protection Impact Assessment), gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ICT-)projecten wordt rekening gehouden met informatiebeveiliging en privacy. De verantwoordelijkheid voor een goede classificatie en risicoanalyse ligt bij de 1st Line of Defense (en meer specifiek de proceseigenaren).

2.5 Beveiligingsincidenten 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[9].

Alle (beveiligings-)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings-)incidenten kunnen worden gemeld bij de ICT-Servicedesk of bij de Functionaris voor Gegevensbescherming (FG) via privacy@sintlucas.nl.

Periodiek wordende beveiligingsincidenten besproken en, waar nodig, aanvullende passende beleidsmaatregelen genomen.

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 SintLucas een jaarlijks verbeterplan 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 meerjaren roadmap 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 SintLucas. Daar boven 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, door een instelling brede gedragscode, door periodieke bewustwordingscampagnes, et cetera.

[9] Draaiboek beveiligingsincidenten en datalekken, te vinden in Weten & Regelen van MijnLucas

Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan SintLucas de betrokken verantwoordelijke medewerkers in het uiterste geval een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

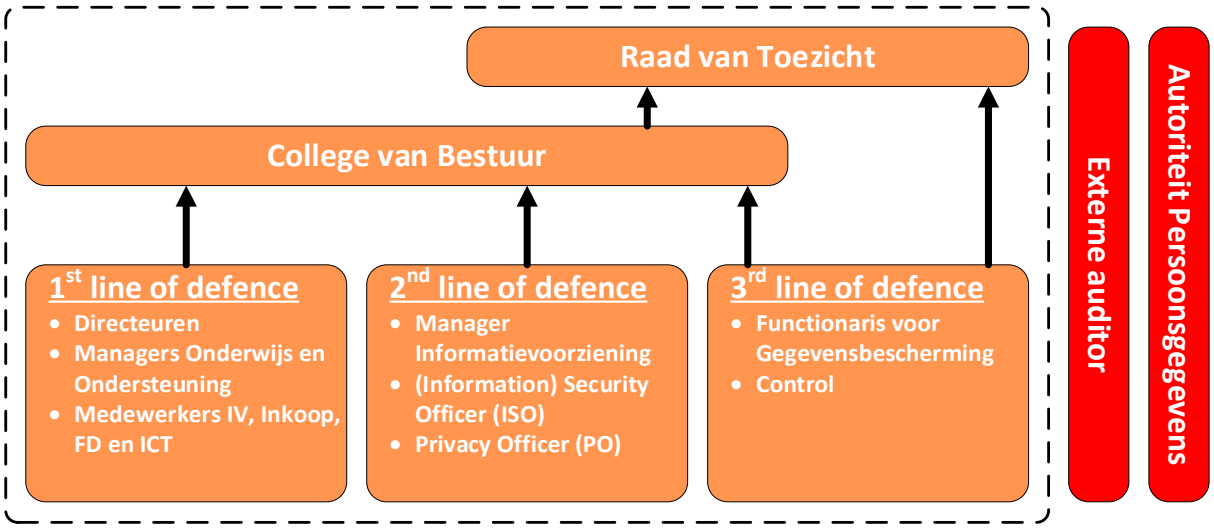
2.8 Logging en monitoring

Logging en monitoring door beheerders zorgt er voor 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. SintLucas zal deze logging regelmatig beoordelen.

3. Governance

3.1 Rollen en verantwoordelijkheden

SintLucas hanteert het 'three lines of defence'-model. De eerste lijn binnen dit model is cruciaal, immers de directeuren en managers onderwijs en managers bedrijfsvoering moeten er op toezien dat IBP-beleid en dus de AVG 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 defence: directeuren, managers, IV, Inkoop, FD en ICT

De eerste lijn bewaakt het IBP-beleid en dus het privacybeleid binnen hun eigen organisatorische onderdeel. Directeuren, managers onderwijs en bedrijfsvoering, IV[10], Inkoop, FD[11] en ICT vormen de first line of defence als het gaat om de bescherming van persoonsgegevens. Zij voeren de daarbij horende operationele taken uit, zoals:

- Toetsen dat geen andere verwerkingen plaatsvinden als vastgelegd in de dataregisters voor studenten/leerlingen, medewerkers en relaties.
- Toetsen dat een verwerkersovereenkomst of een gezamenlijk verantwoordelijkenovereenkomst wordt afgesloten als persoonsgegevens worden overgedragen aan externe partijen.
- Beoordelen van incidenten rond persoonsgegevens en het intern melden daarvan als het vermoeden bestaat dat het gaat om een datalek.

Directeuren en managers onderwijs en bedrijfsvoering voeren bovendien de volgende operationele taken uit:

- Toetsen dat hun medewerkers voldoende geschoold zijn in het kader van IBP en 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 defence: manager Informatievoorziening, ISO en PO

De experts op het gebied van informatiebeveiliging en privacybescherming werken samen en monitoren de toepassing en naleving van het informatiebeveiligings- en privacybeleid, adviseren, gevraagd en ongevraagd, over informatiebeveiliging en privacybescherming en ondersteunen de first line. Het team van experts zijn de manager Informatievoorziening, de Privacy Officer, en de (Information) Security Officer,.

[10] Informatievoorziening
[11] Facilitaire Dienst

De (Information) Security Officer en de Privacy Officer ontwikkelen waar nodig beleid op het gebied van informatiebeveiliging en privacy, in samenspraak met de manager Informatievoorziening en de FG. Het college van bestuur stelt dit voorgenomen beleid vast nadat het CD, de OR en MR hiermee ingestemd hebben.

3.4 De third line of defence: de Functionaris voor de Gegevensbescherming en Control

a) Functionaris voor de Gegevensbescherming

SintLucas heeft een interne toezichthouder op de verwerking van persoonsgegevens aangesteld. Deze toezichthouder wordt functionaris voor de gegevensbescherming genoemd (FG). De FG zal door SintLucas 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 SintLucas. SintLucas heeft de FG aangemeld bij de nationale toezichthoudende autoriteit: de Autoriteit Persoonsgegevens (AP).

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 SintLucas.
- Het toezien op een Data Protection Impact Assessment.
- Het behandelen van klachten over de verwerking van persoonsgegevens.
- Fungeren als eerste aanspreekpunt voor en samenwerken met de AP.

b) Control

Externe controles worden uitgevoerd door onafhankelijke accountants. Deze worden gepland en geformuleerd door control van SintLucas.

3.5 De taken van de medewerkers

Onderwerp	1st line of defence	2nd line of defence	3rd line of defence
Autorisaties	Management[12] brengt autorisaties in kaart (SOLL) en toetst dit bij de functioneel beheerders (IST). ❶ (stap 1)[13]	De expert-IBP controleert of het SOLL en IST autorisatie vergelijk is uitgevoerd. ❷ (stap 2)	De FG controleert of de autorisaties zijn ingericht op basis van *need-to-know* en *least privilege*. ❸ (stap 3)
Beleids-documenten	Directeur, manager, IV, Inkoop, FD en ICT zien er op toe dat de goedgekeurde kaders en richtlijnen uit de beleidsdocumenten worden uitgevoerd. ❷	De expert-IBP evalueert de beleidsdocumenten en bespreekt deze met de FG en dient ze in bij het cvb ter goedkeuring. ❶	De FG toetst de kwaliteit en de werking van het door het cvb goedgekeurde beleid. ❸
Bewaartermijn	Directeur, manager en FD zijn verantwoordelijk voor het handhaven van de bewaartermijnen conform het Documentair StructuurPlan (DSP). ❶	De expert-IBP adviseert aan de hand van de het Documentair StructuurPlan (DSP) de 1st line over de geldende bewaartermijnen. ❷	De FG ziet er op toe dat de bewaartermijnen worden nageleefd. ❸
Bewustwording	Directeuren en managers voeren het	De experts-IBP stellen een bewustwordingsprogramma	De FG toetst het gewenste kennisniveau

[12] Met management worden directeuren en (lijn)managers bedoeld.

[13] ❶, ❷, ❸, ❹, ❺ geven de volgorde/stappen aan waarin de acties genomen moeten worden.

Onderwerp	1st line of defence	2nd line of defence	3rd line of defence
	bewustwordingsprogramma uit of stellen een afgeleid opleidingsplan vast. ❶	op voor IBP-scholings- en awareness plannen en faciliteert ook centrale trainingen. ❷	aan de scholings- en awareness plannen en komt eventueel met aanbevelingen. ❸
DPIA's	Directeur, manager, IV, Inkoop, FD, ICT en projectleiders voeren een pré DPIA uit bij ieder nieuw ICT project. ❶ Directeur, teamleider, IM, FD, ICT en projectleider voeren een DPIA uit in opdracht van de FG. ❹	De PO of ISO komt op basis van de pré DPIA, uitgevoerd door de 1st line, tot een voorstel om al dan niet een DPIA uit te voeren en wordt betrokken bij de uitvoering van de DPIA. ❷	De FG besluit op basis van het voorstel van de PO of ISO of er een DPIA moet worden uitgevoerd en adviseert gevraagd of ongevraagd over de DPIA. ❸ De DPIA wordt slechts vastgesteld door het CvB na advies van de FG. ❺
Datalekken	Medewerkers melden zelf intern een vermoeden van een datalek via de ICT Servicedesk. Het management draagt zorg voor bekendheid van de meldprocedure en scholing van haar medewerkers. ❶	De PO informeert en adviseert de manager IV en ISO en het cvb over de gemelde datalekken. Bij een communicatie naar betrokkenen stelt de PO deze eventueel samen met Communicatie op. ❸	De FG adviseert het cvb inhoudelijk over het datalek, en om al dan niet het datalek bij de AP en/of de betrokkenen te melden. ❷
Dataregisters centraal	De in § 3.7 aangewezen verantwoordelijke directeuren (broneigenaren) voor de d bewaken de actualiteit van het dataregister. ❶	De expert-IBP adviseert en controleert op volledigheid, juistheid en actualiteit van de dataregisters. ❷	De FG toetst of het register van verwerkingen voldoet aan wet- en regelgeving. ❸
Door het management aangewezen uitvoerders	De manager wijst de deelprocesuitvoerders aan (bijv. examinering, roostering, stage, etc.). ❶	De expert-IBP toetst het toegewezen eigenaarschap aan de autorisatie. ❷	De FG toetst of het eigenaarschap beschreven is. ❸
Rechten van de betrokkenen	De manager ontvangt het verzoek van de PO en neemt deze in behandeling (controle door afdeling Onderwijsservice of afdeling HR). ❷	De PO is het eerste aanspreekpunt en volgt de vastgestelde procedure. De PO informeert de experts-IBP over de verzoeken. ❸	De FG staat de PO waar nodig bij en controleert periodiek de procedure. ❶
Verwerkersovereenkomsten	De betrokken directeur, manager, Inkoop, FD en ICT zorgt dat er een verwerkersovereenkomst is opgesteld en kan de experts IBP hiervoor advies vragen. De directeur, manager, Inkoop, FD en ICT stuurt de verwerkersovereenkomst	De expert-IBP adviseert bij de verwerkersovereenkomst na verzoek van de first line. ❷	De FG toetst de verwerkersovereenkomst op rechtmatigheid en volledigheid. Het cvb tekent na advies van de FG. ❸

Onderwerp	1st line of defence	2nd line of defence	3rd line of defence
	ter controle aan de PO. ❶		
Vragen van medewerkers betreffende IBP gerelateerde onderwerpen	De manager is het eerste aanspreekpunt voor vragen inzake informatiebeveiliging en privacy. Medewerkers kunnen de experts IBP ook zelf benaderen. ❶	De expert IBP adviseert de manager en/of medewerker. ❷	De FG controleert de gestelde vragen en de oplossingen. ❸
Controle			Controleert privacyreglementen en verklaringen, grondslagen en eisen, instellingen en beveiligingsmaatregelen. Controleert op overbodige verwerkingen en verwerkingen/maatregelen buiten EER ❶

3.6 Implementatie beleid

SintLucas is zowel verwerkingsverantwoordelijke als verwerker, zoals bedoeld in de AVG. Het college van bestuur heeft de taak toe te zien op de bescherming van persoonsgegevens volgens de geldende wet- en regelgeving.

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 SintLucas, als verwerkingsverantwoordelijke, kan aantonen persoonsgegevens te verwerken volgens geldende wet- en regelgeving.

3.7 Persoonsgegevens

Persoonsgegevens worden verwerkt in nagenoeg alle teams en afdelingen van SintLucas. Bijna elke medewerker van SintLucas is erbij betrokken en kan op de verwerking worden aangesproken.

3.8 Verdeling van de verantwoordelijkheden

SintLucas onderscheidt een viertal soorten verwerkingen van persoonsgegevens met daarbij benoemde broneigenaren:

- Onderwijsservice (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle mensen die bij SintLucas onderwijs volgen. Onderwijsservice is verantwoordelijk voor het Dataregister met student- en leerlingengegevens.
- HR (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle mensen die in opdracht van SintLucas werk verrichten. HR is verantwoordelijk voor het Dataregister van medewerkers.
- Communicatie (broneigenaar) is verantwoordelijk voor de verwerkingen van persoonsgegevens van alle mensen waarmee SintLucas centraal een relatie onderhoudt, zoals belangstellenden, sollicitanten, oud-werknemers, contactpersonen van de stageverlenende organisaties en leveranciers, potentials en alumni. Communicatie is verantwoordelijk voor het Dataregister van deze relaties.
- De opdrachtgever van onderzoek (broneigenaar) dat SintLucas uitvoert is verantwoordelijk voor de verwerkingen van persoonsgegevens in het kader van dat onderzoek. Een onderzoek wordt altijd afgestemd met het college van bestuur.

Deze toewijzing van verantwoordelijkheden houdt ook in dat elke manager die buiten de genoemde broneigenaren om, eigen persoonsgegevens verwerkt of verrijkt, zélf verantwoordelijk is voor die aanvullende persoonsgegevens. Zij dienen deze verwerkingen te melden bij de functionaris voor gegevensbescherming en te documenteren.

3.9 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 informatiebeveiliging en privacyaspecten. Het strategisch niveau wordt voorbereid door de ISO.

Op tactisch niveau wordt de strategie vertaald naar plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering. Het tactisch niveau wordt ingevuld door de manager Informatievoorziening en/of ISO en/of PO.

Op operationeel niveau worden de zaken besproken die de dagelijkse bedrijfsvoering aangaan. Het operationeel niveau wordt ingevuld door de directeur, manager, IV, Inkoop, FD en ICT.

3.10 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 SintLucas 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/leerlingen en relaties. Verhoging van het bewustzijn is de verantwoordelijkheid van elke leidinggevende en wordt gefaciliteerd door de experts IBP.

3.11 Controle en naleving

Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert gezamenlijk met de 2nd line en Control de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens.

Eventuele externe controles worden uitgevoerd door onafhankelijke accountants. Deze externe controles worden gepland en geformuleerd in een nauwe samenspraak met Control van SintLucas.

Mocht de naleving op de bescherming van data- en privacygegevens ernstig tekortschieten, dan kan SintLucas de betrokken verantwoordelijke medewerkers in het uiterste geval 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 SintLucas maken het noodzakelijk om periodiek te bezien of men nog voldoende op koers zit met het beleid.

Bijlage 1: Ondersteunende documenten

Deze bijlage bevat een aantal aanvullende documenten.

	IBP beleid Concretisering	SintLucas document	Bron
1	College van bestuur, verwerkingsverantwoordelijke	IBP-beleid SintLucas, hoofdstuk 3	MBO Raad, Kennisnet
2	Relevante wet- en regelgeving	IBP-beleid SintLucas, hoofdstuk 2	MBO Raad, Kennisnet
3	Specifiek doel en wettelijke grondslag	Dataregisters Toestemmingsverklaring	MBO Raad Eigen versie SintLucas
4	Betrokkenen helder en actief informeren	Privacy verklaring voor medewerkers en studenten	MBO Raad, Kennisnet
5	Verwerkingen van persoonsgegevens (dataregisters)	Dataregister medewerkers Dataregister studenten Dataregister relaties	MBO Raad, Kennisnet
6	Veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van eenieder	Privacyreglement medewerkers Privacyreglement studenten	Eigen versie SintLucas
7	Eigendom toebehoort aan derden	Auteursrecht	MBO Raad, Kennisnet
8	Classificeren informatie en informatiesystemen	BIV classificatie	MBO Raad, Kennisnet
9	Leveranciers van digitale onderwijsmiddelen	Model verwerkersovereenkomsten SintLucas	MBO Raad, Kennisnet, Surfnet
10	Medewerkers, studenten, (geregistreerde) bezoekers en externe relaties gedragen zich ‘fatsoenlijk’	10 grondregels SintLucas Handboek AVG voor medewerkers Gedragscode ICT-faciliteiten	Eigen versie SintLucas Bewerkte versie saMBO-ICT Eigen versie SintLucas
11	Informatiebeveiliging en privacy is een continu kwaliteitsproces	Self assessment op basis van ISO27001/2	MBO Raad, Kennisnet
12	Wijzigingen en aanschaf van nieuwe (informatie)systemen	Privacy by design/default DPIA	Fontys Hogescholen Rijksoverheid, Kennisnet en NOREA
14	Beveiligingsincidenten en datalekken	Draaiboek beveiligingsincidenten en datalekken SintLucas	Eigen versie SintLucas
15	Autorisatie en authenticatie (IAA)	Autorisatie- en authenticatiebeleid SintLucas	Eigen versie SintLucas
16	Verantwoord digitaal werken	Richtlijn verantwoord digitaal werken	Eigen versie SintLucas

Bijlage 2: Besluitenlijst

Besluit 20: Mobiele apparatuur.
Voor mobiele apparatuur geldt de 3 Treden regeling:

Trede 1 - Gebruik de applicatie (Magister, Afas, OnStage)
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 netwerk (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 én 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).
- SintLucas maakt gebruik van een versleutelprogramma (bijv. Bitlocker of FileVault) Encryptiesleutels worden opgeslagen bij ICT.

Besluit 21: Classificatiemodel
SintLucas hanteert het MORA classificatiemodel en de uitkomsten van de classificatie worden opgenomen in het dataregister.

Besluit 22: Bewaartermijnen
SintLucas hanteert het DSP (Documentair Structuur Plan) van de MBO Raad. (Te vinden in Weten & Regelen van MijnLucas).

Besluit 23: Lidmaatschap IBP-netwerk, SCIRT en SCIPR
SintLucas is actief lid van communities op gebied van IBP, bijvoorbeeld MBO-Digitaal, IBP-Netwerk MBO-Digitaal, SCIPR en SCIRT.

Besluit 24: Thuiswerken
Medewerkers mogen thuis alleen applicaties ontsluiten, die gegevens bevatten met de vertrouwelijkheid “Hoog”, als zij gebruik maken van multi factor authenticatie.

Besluit 25: Responsible disclosure procedure
Hackers kunnen (op ethisch verantwoorde wijze) kwetsbaarheden ontdekken in onze beveiliging. Daar kunnen we van leren en mogelijke schade voorkomen. Hieronder het beleid hoe SintLucas hier mee omgaat (communicatie, eventuele beloning) en wat de spelregels zijn voor de melder.

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.
- 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 security@sintlucas.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.

Wat wij de hacker beloven:

- We ondernemen geen juridische stappen.
- We reageren binnen 5 werkdagen (exclusief vakantie).
- We handelen dit vertrouwelijk af.
- We houden hem/haar op de hoogte.
- We bieden een beloning als de kwetsbaarheid nog niet bekend is bij SintLucas of leverancier. Afhankelijk van de ernst van het beveiligingsprobleem en de kwaliteit van de melding, kan die beloning variëren van een T-shirt tot cadeaubonnen voor maximaal 300 euro.

Dit beleid is gepubliceerd op de openbare website van SintLucas.

Besluit 26: Clear desk, clear screen.

Clear Screen:

Medewerkers dienen hun laptop, computers of andere 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 et cetera. Een device mag niet onvergrendeld toegankelijk zijn voor studenten/leerlingen en collega's of andere derden.

Technisch afdwingen:

IV is verplicht om apparatuur die in beheer is van SintLucas automatisch na maximaal 10 minuten inactiviteit te vergrendelen. De manager Informatievoorziening of ISO kan deze termijn verkorten als hij dat noodzakelijk acht voor de veiligheid. Van een BYOD-apparaat is het technisch afdwingen niet mogelijk, maar medewerkers hebben de plicht om zelfstandig hun scherm te vergrendelen als het apparaat niet wordt gebruikt door de medewerker.

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. De leidinggevende is verantwoordelijk voor een goede uitvoering van het clean-desk beleid. De directeur of (lijn)manager is verantwoordelijk en aanspreekpunt voor het bieden van een oplossing.

Papierversnipperaar en beveiligde containers:

Iedere locatie dient in het bezit gesteld te worden van papierversnipperaars of beveiligde containers voor de afvoer van vertrouwelijke informatie. Medewerkers zijn verplicht om privacygevoelige informatie en bedrijfskritische informatie (zie MijnLucas voor meer informatie) in deze papierversnipperaars of beveiligde containers te doen als papier wordt weggegooid. Facilitair is verantwoordelijk voor een goede uitvoering van dit beleid.

Besluit 27: Back-up van informatie

SintLucas heeft als back-up beleid het uitgangspunt dat de default-instellingen van de leverancier worden overgenomen. Voor de kernsystemen van SintLucas geldt aanvullend:

- 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.
- Twee maal per jaar dient leverancier een restore test uit te voeren.
- Afspraken van de leverancier dienen gecontroleerd te kunnen worden.

Besluit 28: Logging

SintLucas 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 ICT of medewerkers die hiertoe zijn gedelegeerd door ICT. 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 bijvoorbeeld voor 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 regelmatig gecontroleerd op onregelmatigheden door de broneigenaar conform het informatiebeveiligings- en privacybeleid.

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 29: Crisisplan Digitale Informatievoorziening

- Het crisisplan sluit aan bij het calamiteitenplan van SintLucas.
- Voor beveiligingsincidenten/datalekken geldt het draaiboek beveiligingsincidenten en datalekken. Bij een cybercrisis is er een crisisteam beschikbaar volgens het crisisplan Digitale Informatievoorziening.

Bijlage 3: Verklarende woordenlijst

AVG
Algemene Verordening Gegevensbescherming. Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

Beleid
Beleid met betrekking tot het beschermen van persoonsgegevens door SintLucas.

Betrokkene
Een natuurlijk persoon op wie een persoonsgegeven betrekking heeft.

Broneigenaar
Aangewezen directeur of manager die verantwoordelijk is voor persoonsgegevens van één of meerdere categorieën van Betrokkenen. De broneigenaar voert de persoonsgegevens in en zorgt voor de vernietiging. In de tussentijd leent hij ze uit aan de organisatorische eenheden binnen SintLucas. De organisatorische eenheden mogen dan de persoonsgegevens verrijken.

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. SintLucas heeft drie centrale registers: dat voor student- en leerlinggegevens, voor medewerker gegevens 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: StudentenInformatieSysteem, HR, Financiën, Rooster, Electronische LeerOmgeving, Stagesysteem, CRM, Identity- en AccesManagement, Office365.

Minderjarige
Voor de AVG geldt iedere persoon die de leeftijd van 16 jaar nog niet heeft bereikt.

Niet-geautomatiseerde verwerking
Voorbeelden: aangetekende stukken, pasjes die zichtbaar gedragen worden, klassenlijsten met foto's (smoelenboek), et cetera.

Persoonsgegeven
Elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon.

Privacy by Default
Een gegevensverwerking waarbij de standaardinstellingen van producten en diensten zo zijn ingesteld dat de privacy van betrokkenen maximaal wordt gewaarborgd. Dit betekent onder meer dat er zo min mogelijk gegevens worden gevraagd en verwerkt.

Privacy by Design
Al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) wordt ten eerste aandacht besteed aan privacy verhogende maatregelen. Ten tweede wordt rekening gehouden met dataminimalisatie: er worden zo min mogelijk persoonsgegevens verwerkt, alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking.

Verwerker
Een door SintLucas ingeschakelde (derde) partij die ten behoeve van SintLucas, 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
SintLucas, waarbij het college van bestuur door de wet is aangewezen als verantwoordelijke voor het vaststellen van het doel en de middelen van de verwerking.