Bijlage: tabel met KPI's

KPI`s op het vlak van Privacy

1	**KPI: Beleid**
	Algemeen privacybeleid opgesteld
	Lijnmanagement verantwoordelijkheden
	Deze kpi ziet toe op opzet en bestaan van actueel privacybeleid. Het privacybeleid geeft de kaders weer die gesteld worden op de rechtmatige verwerking van persoonsgegevens door het college.
2	**KPI: Processen**
	Werkprocessen vaststellen
	Bewaartermijnen
	Geautomatiseerde besluitvorming
	Deze kpi ziet toe op opzet, bestaan en werking van processen binnen de primaire afdelingen waarbinnen persoonsgegevens verwerkt worden.
3	**KPI: Organisatorische inbedding**
	Passende instructies omgang persoonsgegevens
	Uitvoeren DPIA
	Aanstellen FG
	Juridische kennis
	Middelen voor privacybescherming
	Privacy by design en Privacy by default
	Deze kpi ziet toe op opzet, bestaan en werking van de benodigde organisatorische en privacy gerichte maatregelen ter borging van (de verwerking van) privacy gevoelige gegevens.
4	**KPI: Rechten van betrokkenen**
	Register van verwerkingen
	Processen rechten van betrokkenen
	Informeren van betrokkenen
	Communicatieplan
	Toepassing rechten van btrokkenen
	Deze kpi ziet toe op opzet, bestaan en werking van de uitvoering van de privacyrechten van betrokkenen zoals vastgelegd in de AVG.
5	**KPI: Samenwerking**
	Doorgifte verwerkingen buiten de EER
	Privacy eisen wetgeving en contracten
	Deze kpi ziet toe op opzet, bestaan en werking van de borging van de afspraken met betrekking tot de samenwerking met derde partijen
6	**KPI: Beveiliging**
	Inzicht in privacy incidenten
	Privacy specifieke beveiligingsincidenten
	Deze kpi ziet toe op opzet, bestaan en werking van de beveiligingsmaatregelen op het gebied van privacy.
7	**KPI: Verantwoording**
	Informeren OR en btrokkenen
	Privacy en Cookieverklaring
	Deze kpi ziet toe op opzet, bestaan en werking van instrumenten op het gebied van verantwoording op de rechtmatigheid van de verwerking van persoonsgegevens.

KPI`s op het vlak van Informatiebeveiliging

8	**KPI: Beleid en organisatie**

	Beleid opgesteld
	Beleidsregels voor informatiebeveiliging
	Beoordeling van het informatiebeveiligingsbeleid
	De kpi op beleid kent een score toe aan opzet, bestaan en werking van het informatiebeveiligingsbeleid, aansturing door het management, communicatie naar de medewerkers en toetsing op doeltreffendheid conform bedrijfseisen en relevante wetgeving.
9	**KPI: Organisatie**
	Rollen en verantwoordelijkheden bij informatiebeveiliging
	Scheiding van taken
	Contact met overheidsinstanties
	Informatiebeveiliging in projectbeheer
	Beleid voor mobiele apparatuur
	De kpi voor organisatie scoort opzet, bestaan en werking waar het gaat om de definitie van de rollen en verantwoordelijkheden in een beheerkader inclusief het toepassen van functiescheiding, om de implementatie van informatiebeveiliging te beheersen.
10	**KPI: Personeel en toegang**
	Personeel
	Screening
	Arbeidsvoorwaarden
	Directieverantwoordelijkheden
	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
	Disciplinaire procedure
	De kpi op het vlak van personeel scoort opzet, bestaan en werking voor wat betreft de eisen die aan personeel worden gesteld voorafgaand en tijdens het dienstverband, denk aan contractuele afspraken en kennis, vaardigheden en scholing, om te waarborgen dat zij geschikt zijn voor hun rol.
11	**KPI : Toegang**
	Beleid voor toegangsbeveiliging
	Toegang tot netwerken en netwerkdiensten
	Registratie en afmelden van gebruikers
	Gebruikers toegang verlenen
	Beheren van speciale toegangsrechten
	Beheer van geheime authenticatie-informatie van gebruikers
	Beoordeling van toegangsrechten van gebruikers
	Toegangsrechten intrekken of aanpassen
	Geheime authenticatie-informatie gebruiken
	Beperking toegang tot informatie
	Beveiligde inlogprocedures
	Systeem voor wachtwoordbeheer
	Speciale systeemhulpmiddelen gebruiken
	Toegangsbeveiliging op programmabroncode
	Fysieke toegangsbeveiliging
	Fysieke beveiligingszone
	Kantoren, ruimten en faciliteiten beveiligen
	Beschermen tegen bedreigingen van buitenaf

	Werken in beveiligde gebieden
	Laad- en loslocatie
	Plaatsing en bescherming van apparatuur
	Nutsvoorzieningen
	Beveiliging van bekabeling
	Onderhoud van apparatuur
	Verwijdering van bedrijfsmiddelen
	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein
	Veilig verwijderen of hergebruiken van apparatuur
	Onbeheerde gebruikersapparatuur
	Clear desk'- en 'clear screen'-beleid
	De kpi voor toegang geeft een waarde aan opzet, bestaan en werking van de maatregelen die toe zien op het toegang verlenen van de juiste persoon tot de juiste beveiligingszone, de juiste data en de juiste applicatie om onbevoegde toegang te voorkomen.
12	**KPI: Bedrijfsmiddelen en informatiesystemen**
	Bedrijfsmiddelen
	Inventariseren van bedrijfsmiddelen
	Eigendom van bedrijfsmiddelen
	Aanvaardbaar gebruik van bedrijfsmiddelen
	Teruggeven van bedrijfsmiddelen
	Classificatie van informatie
	Informatie labelen
	Behandelen van bedrijfsmiddelen
	Beheer van verwijderbare media
	Verwijderen van media
	Media fysiek overdragen
	De kpi op het vlak van bedrijfsmiddelen geeft een score aan de mate waarin het beheer van bedrijfsmiddelen zoals informatie, media en apparatuur bestaat en werkt zodat zij passend beschermd worden.
13	**Informatiesystemen:**
	Analyse en specificatie van informatiebeveiligingseisen
	Toepassingen op openbare netwerken beveiligen
	Transacties van toepassingen beschermen
	Beleid voor beveiligd ontwikkelen
	Procedures voor wijzigingsbeheer met betrekking tot systemen
	Technische beoordeling van toepassingen na wijzigingen besturingsplatform
	Principes voor engineering van beveiligde systemen
	Beveiligde ontwikkelomgeving
	Uitbestede softwareontwikkeling
	Testen van systeembeveiliging
	Systeemacceptatietests
	Bescherming van testgegevens
	De kpi voor informatiesystemen geeft een waarde aan de mate waarin het beheer van het verkrijgen, beheren en gebruiken van software systemen bestaat en werkt zodat informatie systemen gedurende hun hele levenscyclus veilig zijn om te gebruiken.
14	**KPI: Bedrijfsvoering, communicatiebeveiliging, cryptografie**

	Bedrijfsvoering:
	Gedocumenteerde bedieningsprocedures
	Wijzigingsbeheer
	Capaciteitsbeheer
	Scheiding van ontwikkel-, test- en productieomgevingen
	Beheersmaatregelen tegen malware
	Back-up van informatie
	Gebeurtenissen registreren
	Beschermen van informatie in logbestanden
	Logbestanden van beheerders en operators
	Kloksynchronisatie
	Software installeren op operationele systemen
	Beheer van technische kwetsbaarheden
	Beperkingen voor het installeren van software
	Beheersmaatregelen betreffende audits van informatiesystemen
	De kpi voor bedrijfsvoering scoort de mate waarin het dagelijkse technische beheer van de IT omgeving in opzet, bestaan en werking correct en veilig wordt uitgevoerd ter voorkoming van verlies en beschadiging van gegevens.
15	**KPI: Communicatiebeveiliging**
	Beheersmaatregelen voor netwerken
	Beveiliging van netwerkdiensten
	Scheiding in netwerken
	Beleid en procedures voor informatietransport
	Overeenkomsten over informatietransport
	Elektronische berichten
	Vertrouwelijkheids- of geheimhoudingsovereenkomst
	De kpi voor communicatiebeveiliging geeft een waarde aan de opzet, bestaan en werking van het digitale transport van informatie door onze informatie verwerkende faciliteiten
16	**KPI: Cryptografie**
	Beleid inzake het gebruik van cryptografische beheersmaatregelen
	Sleutelbeheer
	De kpi voor cryptografie geeft een score aan de opzet, bestaan en werking van het beheer van de digitale sleutels die wij gebruiken om de vertrouwelijkheid, authenticiteit en integriteit van onze informatie te beschermen.
17	**KPI: Incidenten en continuïteit**
	Incidenten
	Verantwoordelijkheden en procedures
	Rapportage van informatiebeveiligingsgebeurtenissen
	Rapportage van zwakke plekken in de informatiebeveiliging
	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen
	Respons op informatiebeveiligingsincidenten
	Lering uit informatiebeveiligingsincidenten
	Verzamelen van bewijsmateriaal

	De kpi op het vlak van informatiebeveiligingsincidenten heeft een waarde aan de mate waarin opzet, bestaan en werking van het beheer van incidenten consistent en doeltreffend is in het verbeteren van de informatiebeveiliging.
18	**KPI: Continuïteit**
	Informatiebeveiligingscontinuïteit plannen
	Informatiebeveiligingscontinuïteit implementeren
	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren
	De kpi voor bedrijfscontinuiteit geeft een score aan de opzet, bestaan en werking van de maatregelen die de beschikbaarheid en veiligheid van de informatie verwerkende faciliteiten moeten bewerkstellingen.
19	**KPI: Leveranciersrelaties en naleving**
	Leveranciersrelaties
	Informatiebeveiligingsbeleid voor leveranciersrelaties
	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
	Toeleveringsketen van informatie- en communicatietechnologie
	Monitoring en beoordeling van dienstverlening van leveranciers
	Beheer van veranderingen in dienstverlening van leveranciers
	De kpi voor leveranciersrelaties geeft een score aan de mate waarin de opzet, bestaat en werking van een passend informatiebeveiligingsniveau van leveranciers is geborgd die toegang hebben tot bedrijfsmiddelen van onze organisatie
20	**KPI: Naleving**
	Vaststellen van toepasselijke wetgeving en contractuele eisen
	Intellectuele-eigendomsrechten
	Beschermen van registraties
	Privacy en bescherming van persoonsgegevens
	Voorschriften voor het gebruik van cryptografische beheersmaatregelen
	Onafhankelijke beoordeling van informatiebeveiliging
	Naleving van beveiligingsbeleid en –normen
	Beoordeling van technische naleving
	De kpi op het vlak van naleving geeft een score aan de mate waarin de opzet, bestaan en werking van de informatiebeveiliging verzekert dat dit wordt uitgevoerd in overeenstemming met de beleidsregels van de organisatie en geldende verplichtingen van contractuele, wettelijke of regelgevende aard.