

	Onderwerp	Verwijzing WvS/Bus	Beheersmaatregel	Toelichting	Aantoonbaarheid	Voorreitelde toetsaank Oorzaak en Bestaan	Voorreitelde toetsaank Werkings
Wp-G1	Verstrekking aan derden en registratie	Wps artikel 1.7 lid 2, 2.6 en 8 Wps artikel 1.11 lid 2 Wps Artikel 2.29 lid 2 t/m 4 Wps Artikel 2.31 lid 11	Het Zorg- en Veiligheidsbuis heeft procedures ingericht die borgen bij het verstrekken van resultaten aan een derde wordt getoetst dat dit noodzakelijk is voor een van de doelen genoemd in art. 1.7 lid 2 WGS en dat de verstrekking vooraf door de RAC op rechtmatigheid is goetst. Daarnaast is geborgd dat bij gegevensuitwisseling tussen samenwerkingsverbanden uitsluitend gegevens worden verstrekt die op grond van artikel 1.10 Bp zijn toegestaan, waarbij in beginsel wordt voldaan met informatie over welke deelnemers bij de verwerking betrokken zijn of zijn geweest, tenzij aanvullende gegevens aantoonbaar noodzakelijk zijn.	Verstrekking aan derden (niet zijnde incidentele deelnemers of aangewezen deelnemers), dit zijn externe partijen die geen onderdeel zijn van het Zorg- en Veiligheidsbuis en niet als incidentele deelnemers aan een casus deelnemen. Het delen van informatie met deze partijen gebeurt alleen in uitzonderlijke situaties en in de praktijk komt dit zelden voor. Het gaat hierbij bijvoorbeeld om het delen van resultaten van een casus, zoals een plan van aanpak. Dit mag alleen als op rechtmatigheid is goetst (RAC) en de verstrekking noodzakelijk is. Belangrijk om te weten is dat partijen die tijdelijk worden betrokken bij een casus (incidentele deelnemers) niet als derden worden gezien. Zij maken voor de specifieke casus tijdelijk onderdeel uit van ZVH en vallen dus onder een andere werkwijze.	Log elke individuele verstrekking aan een derde apart vast in een verstrekkingen registratie. Indien een verstrekking aan een derde zich heeft voorgedaan betreft de bewijspaat de onderliggende casusinformatie waarin de verschillende verplichte aspecten zoals opgenomen in xxx (n.t.t. factsheet of periodieke review). Log per verstrekking duidelijk vast in het casusdossier: a. waarom informatie is gedeeld; b. hoeveel informatie is gedeeld; c. met welke externe partij dit is gedeeld; d. waarom de informatie is gedeeld; e. wat het RAC advies was; en of er sprake was van een wettelijke verplichting.	Voorreitelde toetsaank Oorzaak en Bestaan Opzet Stel vast dat het ZVH beschikt over vastgesteld beleid en/of procedures voor verstrekking aan derden. Bepaal of het beleid actueel is (bijv. door te controleren op vaststellatium, verbeterplan en/of periodieke review). Stel vast dat het beleid minimaal de volgende onderwerpen bevat: a. Afzonderlijke registratie van verstrekkingen; b. Verplichte vastlegging in een casusdossier; c. Vastlegging zoals opgenomen in aantoonbaarheidsdoelen. Stel vast dat het beleid voorschrijft dat zonder deze vastlegging geen verstrekking plaatsvindt. Bestaan Stel vast of gedurende de beoordelingsperiode verstrekkingen aan derden hebben plaatsgevonden, a. indien geen verstrekkingen hebben plaatsgevonden, documenteer deze non-occurrence. Indien wel verstrekkingen hebben plaatsgevonden, beoordeel of hiervan de vereiste vastlegging en RAC-toetsing aanwezig zijn. Trek b.v.b., een overzicht van verstrekkingen een steekproef en controleer de verstrekkingen of de volgende onderdelen zijn opgenomen in het casusdossier zoals opgenomen in het aantoonbaarheidsdoelen; Werkings Voor een steekproef uit op basis van het register van verstrekkingen aan andere samenwerkingsverbanden en selecteer casusdossiers die hierin zijn opgenomen, stel vast dat: a. voorafgaand aan gegevensdeling een noodzaak- en doelmatigheids toets heeft plaatsgevonden; b. deze afweging expliciet is vastgelegd in het dossier (bijv. casusoverzichts of wegement); c. uitsluitend noodzakelijke gegevens zijn gedeeld en niet voor andere doelen worden gebruikt; d. de gegevensuitwisseling en afwegingen volledig en herleidbaar zijn vastgelegd in de dossiervorming.	
	Verstrekking aan samenwerkingverbanden	Wps artikel 1.7 lid 8 Wps artikel 2.25 Wps artikel 2.28 lid 1 t/m 4	Het Zorg- en Veiligheidsbuis heeft procedures ingericht die borgen dat bij gegevensuitwisseling met een ander ZVH alleen plaatsvindt als voldaan is aan het bepaalde in art. 2.28 WGS. Het Zorg- en Veiligheidsbuis heeft procedures ingericht die borgen dat bij gegevensuitwisseling met andere WGS-samenwerkingsverbanden uitsluitend gegevens worden verstrekt die op grond van artikel 1.10 Bp zijn toegestaan, waarbij in beginsel wordt voldaan met informatie over welke deelnemers bij de verwerking betrokken zijn of zijn geweest. Tenzij aanvullende gegevens aantoonbaar noodzakelijk zijn. Gegevensverstrekking vindt uitsluitend casusgericht plaats na toetsing op doelbinding, noodzaakelijkheid en proportionaliteit en is beperkt tot het beoogde doel, herleidbaar is niet toegestaan. Persoonsgegevens worden alleen verwerkt voor zover noodzakelijk voor de uitvoering en afstemming van wettelijke taken van de deelnemende partijen.	Erst wordt een bekendheidscheck uitgevoerd, waarbij alleen beperkte identificerende gegevens worden verstrekt, in een ander ZVH alleen plaatsvindt als voldaan is aan het bepaalde in art. 2.28 WGS. Bij uitsluiting met een ander ZVH, wordt dit noodzakelijk zijn voor het doel van de ZVH (art. 2.25 WGS), door de casusaanpak. Bij uitsluiting met een ander WGS-samenwerkingsverband, moet het noodzakelijk zijn voor het doel van het ontvangende samenwerkingverband. Tussen ZVH's kan de ook inhoudelijke informatie betreffen, terwijl richting het REC de uitsluiting beperkt blijft tot afstemmingsinformatie. Bij uitsluiting met een ander ZVH tijdens de behandeling van een casus, is een voorafgaande bekendheidscheck niet altijd vereist. Bijvoorbeeld bij overdracht naar een andere regio wordt informatie gedeeld conform de geldende procedure (factsheet 07).	Bij uitsluiting met een ander Zorg- en Veiligheidsbuis: 1. Voer in het casusdossier een bekendheidscheck uit, tenzij dit niet nodig is, bijvoorbeeld bij overdracht van een casus aan een andere regio. 2. Maak aantoonbaar dat dit wordt vastgelegd in het casusdossier en/of registratiesysteem (bijv. PDAV/Geo), inclusief met welk ZVH gegevens zijn gedeeld en welke gegevens zijn verstrekt, conform factsheet 07 Gegevensuitwisseling. 3. Maak aantoonbaar dat per gegevensuitwisseling wordt geregistreerd met welke partij (ander ZVH of REC, REC of ICDO) gegevens worden gedeeld en welk type informatie wordt gedeeld (bekendheidscheck en bij REC), evt. afstemmingsinformatie of inhoudelijke casusinformatie, bijvoorbeeld via een registratiedatum of log in het casusmanagementstelsel, conform factsheet 07 Gegevensuitwisseling. 4. Borg dat voorafgaand aan gegevensdeling wordt beoordeeld of de verstrekking noodzakelijk is voor het doel van het ontvangende samenwerkingverband de casus, en toon aan dat deze afweging expliciet wordt vastgelegd in het casusdossier of in besluitvorming (bijv. casusoverzichts of wegementen), conform factsheet 05 Werkprocessen. WvS-zaak Bij uitsluiting met andere WGS-samenwerkingsverband 1. Voer in het casusdossier een bekendheidscheck uit. 2. Zorg dat per gegevensuitwisseling wordt beoordeeld welke gegevens op grond van artikel 1.10 Bp mogen worden verstrekt, in toon aan dat deze afweging en onderbouwing (met name bij meer dan bestaatsgegevens) wordt vastgelegd in het casusdossier of besluiten (bijv. casusoverzichts of wegementen), conform factsheet 05 Werkprocessen. 3. Maak aantoonbaar dat per gegevensuitwisseling wordt geregistreerd met welke partij (REC of ICDO) gegevens worden gedeeld en welk type informatie wordt gedeeld (bekendheidscheck en bij REC), evt. afstemmingsinformatie, bijvoorbeeld via een registratiedatum of log in het casusmanagementstelsel, conform factsheet 07 Gegevensuitwisseling. 4. Borg dat voorafgaand aan gegevensdeling wordt beoordeeld of de verstrekking noodzakelijk is voor het doel van het ontvangende samenwerkingverband, en toon aan dat deze afweging expliciet wordt vastgelegd in het casusdossier of in besluitvorming (bijv. casusoverzichts of wegementen), conform factsheet 05 Werkprocessen.	Bestaan Stel vast dat voor gegevensuitwisseling documentatie aanwezig is waarvan blijkt: a. met welk samenwerkingverband gegevens zijn gedeeld; b. welke gegevens zijn gedeeld; c. waarom de gegevensuitwisseling noodzakelijk was; d. dat de gegevensuitwisseling noodzakelijk was voor het doel bepaald in de WvS/Bp; e. dat de gegevensuitwisseling is geregistreerd. Stel vast dat format, registraties of dossiers beschikbaar zijn waarin de vereiste vastleggingen worden opgenomen. Opzet Stel vast dat het ZVH beschikt over vastgesteld beleid en/of procedures voor het uitvoeren van privacy audits, en dat hiervan minimaal is opgenomen: a. frequentie (minimaal eenmaal per vier jaar); b. scope (WGS/Bp en AVG); c. rol en verantwoordelijkheden (staatsorgaan, FG, RAC); d. omvang met bevindingen, herentree en rapportage. Bestaan Stel vast dat de middelen een jaarplan, auditplan of bestuurlijk vastgesteld auditplan aantoonbaar is dat privacy audits eenmaal per vier jaar wordt uitgevoerd. Stel vast dat de uitkomsten van deze toetsen worden vastgelegd in auditrapporten, controlelijsten of besluitvormingsdocumentatie (bijv. management- of casusdossiers). Stel vast dat de resultaten aantoonbaar worden geprojecteerd en besproken binnen het Zorg- en Veiligheidsbuis, door het beoordelen van notulen, rapportages en andere stukken (bijv. staatsorgaan, RAC of managementoverleg). Stel vast dat op basis van de uitkomsten verbetermaatregelen zijn bepaald en vastgelegd, en dat opvolging inschakelt, door het beoordelen van acties, verbetermaatregelen en voortgangrapportages. Opzet Stel vast dat beleid, procesen en procedures zijn ingericht voor het uitvoeren van periodieke (bijv. maandelijks, kwartaalwijd) nalevingsbeoordelingen van privacywetgeving, door het beoordelen van vastgelegde beleidsdocumenten, werkstructuur en procesbeschrijvingen. Stel vast dat rollen en verantwoordelijkheden voor toezicht en coördinatie van nalevingsbeoordelingen zijn bepaald, door het beoordelen van governance-documentatie, functieschetsingen en mandaten. Bestaan Beoordeel de bestuurlijke afspraken en besluiten actueel en geldig zijn vastgesteld, door het beoordelen van governance-documenten en bestuurlijke afspraken, waarbij wordt vastgesteld dat herzieningsdata en besluitvorming zijn vastgelegd. Verifieer dat de gezamenlijke verwerkingsverantwoordelijkheid van de deelnemers expliciet is uitgewerkt, door het beoordelen van bestuurlijke afspraken, convenanten of reglementen, waarbij wordt vastgesteld dat rollen, verantwoordelijkheden en besluitvorming zijn vastgesteld conform factsheet 04) Beoordeel of afspraken zijn vastgesteld na uitvoerbare werkstructuur en beleid, door het beoordelen van privacybeleid en werkprocessen, waarbij wordt vastgesteld dat deze aansluiten op de praktijk (conform factsheet 05 Werkprocessen).	
Wp-G2	Beoordeling van naleving privacywetgeving	Wps artikel 1.10 lid 1 t/m 3 Bp artikel 1.18 lid 1 t/m 3	Het samenwerkingverband laat periodiek privacy-audits uitvoeren op naleving van WGS en AVG en deelt de resultaten met de Autoriteit Persoonsgegevens. Het samenwerkingsverband laat de eerste privacy-audit uiterlijk binnen twee jaar na de inwerkingtreding van de wet te zijn uitgevoerd. Indien uit de audit blijkt dat niet wordt voldaan aan de bij of krachtens de WGS geldende vereisten, wordt binnen drie jaar na afronding van de audit een herentree uitgevoerd op de onderdelen die niet voldoen. De resultaten van de audit en eventuele herentree worden verstrekt aan de Autoriteit Persoonsgegevens. De privacy-audit wordt uitgevoerd door een onafhankelijke en deskundige autoriteit met aantoonbare kennis van auditmethodes en van het functioneren van het Zorg- en Veiligheidsbuis (ZVH). De auditor rapporteert de uitkomsten aan de rechtmatigheidscommissie (RAC), de opdrachtgever en de (coördinerende) functionarissen voor gegevensbescherming.	Het Zorg- en Veiligheidsbuis laat de naleving van de bij of krachtens de WGS gestelde regels en de Algemene verordening gegevensbescherming periodiek toetsen door middel van het uitvoeren van privacy-audits, ten minste eenmaal per vier jaar. Aangezien de Wp op 1 maart 2023 in werking is getreden, dient de eerste privacy-audit uiterlijk binnen twee jaar na de inwerkingtreding van de wet te zijn uitgevoerd. Indien uit de audit blijkt dat niet wordt voldaan aan de bij of krachtens de WGS geldende vereisten, wordt binnen drie jaar na afronding van de audit een herentree uitgevoerd op de onderdelen die niet voldoen. De resultaten van de audit en eventuele herentree worden verstrekt aan de Autoriteit Persoonsgegevens. De privacy-audit wordt uitgevoerd door een onafhankelijke en deskundige autoriteit met aantoonbare kennis van auditmethodes en van het functioneren van het Zorg- en Veiligheidsbuis (ZVH). De auditor rapporteert de uitkomsten aan de rechtmatigheidscommissie (RAC), de opdrachtgever en de (coördinerende) functionarissen voor gegevensbescherming.	WvS-zaak Zorg dat het ZVH periodiek privacy-audits uitvoert op de naleving van de WGS, de daarop gebaseerde regelgeving en de AVG, en maak aantoonbaar dat dit ten minste eenmaal per vier jaar plaatsvindt. Bijvoorbeeld, binnen één jaar na afronding van de audit een herentree wordt uitgevoerd op de onderdelen die niet voldoen. Borg dat de resultaten van de audit en eventuele herentree worden verstrekt aan de Autoriteit Persoonsgegevens, voor zover dit op grond van de WGS/Bp vereist is. Maak aantoonbaar dat de privacy-audit wordt uitgevoerd door een onafhankelijke en deskundige autoriteit met aantoonbare kennis van auditmethodes en van het functioneren van het Zorg- en Veiligheidsbuis. Borg dat de audit de uitkomsten van de rechtmatigheidscommissie (RAC), de opdrachtgever en de (coördinerende) functionarissen voor gegevensbescherming. Waarborg dat de uitkomsten van de audit worden vastgelegd en dat de opvolging hiervan periodiek wordt gemonteerd. Bijvoorbeeld via een activiteits-, voortgangrapportage of verbeterregister. WGS-zaak Borg dat procesen en procedures zijn ingericht om de naleving van privacywetgeving periodiek te toetsen, en maak aantoonbaar dat deze zijn vastgelegd in beleid, werkstructuur of procesbeschrijvingen conform de WGS/Bp en factsheet 05 Werkprocessen. Zorg dat deze toetsen plaatsvinden via interne audits, compliance checks en rapportages, en toon aan dat de uitkomsten worden vastgelegd in auditrapporten, controlelijsten of besluitvormingsdocumentatie binnen het management- of casusdossier. Maak aantoonbaar dat de resultaten van deze toetsen worden geprojecteerd en besproken binnen het Zorg- en Veiligheidsbuis. Dit kan op basis van deze beoordelingen verbetermaatregelen worden bepaald en opgevolgd, en toon aan dat de voortgang en opvolging inschakelt zijn via een activiteits-, verbeterregister of voortgangrapportages. Borg dat toezicht en coördinatie van nalevingsbeoordelingen zijn bepaald (bijv. via FG of deelnemers), en maak aantoonbaar dat deze rolverdeling is vastgelegd in governance-documenten, functieschetsingen of mandaten, conform factsheet 04 Coördinerende functionarissen gegevensbescherming en factsheet 04 Deelnemers.	Bestaan Stel vast dat de middelen een jaarplan, auditplan of bestuurlijk vastgesteld auditplan aantoonbaar is dat privacy audits eenmaal per vier jaar wordt uitgevoerd. Stel vast dat de uitkomsten van deze toetsen worden vastgelegd in auditrapporten, controlelijsten of besluitvormingsdocumentatie (bijv. management- of casusdossiers). Stel vast dat de resultaten aantoonbaar worden geprojecteerd en besproken binnen het Zorg- en Veiligheidsbuis, door het beoordelen van notulen, rapportages en andere stukken (bijv. staatsorgaan, RAC of managementoverleg). Stel vast dat op basis van de uitkomsten verbetermaatregelen zijn bepaald en vastgelegd, en dat opvolging inschakelt, door het beoordelen van acties, verbetermaatregelen en voortgangrapportages. Opzet Stel vast dat beleid, procesen en procedures zijn ingericht voor het uitvoeren van periodieke (bijv. maandelijks, kwartaalwijd) nalevingsbeoordelingen van privacywetgeving, door het beoordelen van vastgelegde beleidsdocumenten, werkstructuur en procesbeschrijvingen. Stel vast dat rollen en verantwoordelijkheden voor toezicht en coördinatie van nalevingsbeoordelingen zijn bepaald, door het beoordelen van governance-documentatie, functieschetsingen en mandaten. Bestaan Beoordeel de bestuurlijke afspraken en besluiten actueel en geldig zijn vastgesteld, door het beoordelen van governance-documenten en bestuurlijke afspraken, waarbij wordt vastgesteld dat herzieningsdata en besluitvorming zijn vastgelegd. Verifieer dat de gezamenlijke verwerkingsverantwoordelijkheid van de deelnemers expliciet is uitgewerkt, door het beoordelen van bestuurlijke afspraken, convenanten of reglementen, waarbij wordt vastgesteld dat rollen, verantwoordelijkheden en besluitvorming zijn vastgesteld conform factsheet 04) Beoordeel of afspraken zijn vastgesteld na uitvoerbare werkstructuur en beleid, door het beoordelen van privacybeleid en werkprocessen, waarbij wordt vastgesteld dat deze aansluiten op de praktijk (conform factsheet 05 Werkprocessen).	
Wp-G3	Beoordeling van naleving privacywetgeving	Wps artikel 1.10 lid 1 t/m 3 Bp artikel 1.18 lid 1 t/m 3 Bp artikel 2.19	Het Zorg- en Veiligheidsbuis heeft procesen en procedures ingericht om: a. jaarlijks de naleving te beoordelen van privacybeleid en -procedures, verplichtingen en geldende wet- en regelgeving, Service Level Agreements, door het Zorg- en Veiligheidsbuis opgestelde normen en andere overeenkomsten; b. periodieke beoordelingen te documenteren, zoals interne auditrapporten, auditrapporten, compliance checks en afleveringen ("sign-offs") van het management; c. te rapporteren over de resultaten van deze conformiteitsbeoordelingen en daaruit voortvloeiende verbeteracties tijdig te implementeren; d. op de hoogte te blijven van, en te anticiperen op (veranderingen in) toepasselijke wet- en regelgeving.	Deze norm geeft invulling aan artikel 1.10 lid 1 t/m 3 WGS en artikel 1.18 lid 1 t/m 3 BGS en ziet op het structureren borgen van nalevingsbeoordelingen binnen het Zorg- en Veiligheidsbuis. De overnemerdeelnemers richten hiervoor processen en procedures in om periodiek te toetsen of de gegevensverwerking voldoet aan wet- en regelgeving en gemaakte afspraken doormiddel van een self-assessment door het samenwerkingverband. De FG heeft hierbij geen verplichting om toezicht te houden, maar kan desgewenst worden betrokken. De resultaten worden gedocumenteerd en geprojecteerd, en vormen de basis voor het tijdig doorvoeren van verbetermaatregelen en het houden op wijzigingen in wet- en regelgeving.	Borg dat procesen en procedures zijn ingericht om de naleving van privacywetgeving periodiek te toetsen, en maak aantoonbaar dat deze zijn vastgelegd in beleid, werkstructuur of procesbeschrijvingen conform de WGS/Bp en factsheet 05 Werkprocessen. Zorg dat deze toetsen plaatsvinden via interne audits, compliance checks en rapportages, en toon aan dat de uitkomsten worden vastgelegd in auditrapporten, controlelijsten of besluitvormingsdocumentatie binnen het management- of casusdossier. Maak aantoonbaar dat de resultaten van deze toetsen worden geprojecteerd en besproken binnen het Zorg- en Veiligheidsbuis. Dit kan op basis van deze beoordelingen verbetermaatregelen worden bepaald en opgevolgd, en toon aan dat de voortgang en opvolging inschakelt zijn via een activiteits-, verbeterregister of voortgangrapportages. Borg dat toezicht en coördinatie van nalevingsbeoordelingen zijn bepaald (bijv. via FG of deelnemers), en maak aantoonbaar dat deze rolverdeling is vastgelegd in governance-documenten, functieschetsingen of mandaten, conform factsheet 04 Coördinerende functionarissen gegevensbescherming en factsheet 04 Deelnemers.	Bestaan Stel vast dat de middelen een jaarplan, auditplan of bestuurlijk vastgesteld auditplan aantoonbaar is dat privacy audits eenmaal per vier jaar wordt uitgevoerd. Stel vast dat de uitkomsten van deze toetsen worden vastgelegd in auditrapporten, controlelijsten of besluitvormingsdocumentatie (bijv. management- of casusdossiers). Stel vast dat de resultaten aantoonbaar worden geprojecteerd en besproken binnen het Zorg- en Veiligheidsbuis, door het beoordelen van notulen, rapportages en andere stukken (bijv. staatsorgaan, RAC of managementoverleg). Stel vast dat op basis van de uitkomsten verbetermaatregelen zijn bepaald en vastgelegd, en dat opvolging inschakelt, door het beoordelen van acties, verbetermaatregelen en voortgangrapportages. Opzet Stel vast dat beleid, procesen en procedures zijn ingericht voor het uitvoeren van periodieke (bijv. maandelijks, kwartaalwijd) nalevingsbeoordelingen van privacywetgeving, door het beoordelen van vastgelegde beleidsdocumenten, werkstructuur en procesbeschrijvingen. Stel vast dat rollen en verantwoordelijkheden voor toezicht en coördinatie van nalevingsbeoordelingen zijn bepaald, door het beoordelen van governance-documentatie, functieschetsingen en mandaten. Bestaan Beoordeel de bestuurlijke afspraken en besluiten actueel en geldig zijn vastgesteld, door het beoordelen van governance-documenten en bestuurlijke afspraken, waarbij wordt vastgesteld dat herzieningsdata en besluitvorming zijn vastgelegd. Verifieer dat de gezamenlijke verwerkingsverantwoordelijkheid van de deelnemers expliciet is uitgewerkt, door het beoordelen van bestuurlijke afspraken, convenanten of reglementen, waarbij wordt vastgesteld dat rollen, verantwoordelijkheden en besluitvorming zijn vastgesteld conform factsheet 04) Beoordeel of afspraken zijn vastgesteld na uitvoerbare werkstructuur en beleid, door het beoordelen van privacybeleid en werkprocessen, waarbij wordt vastgesteld dat deze aansluiten op de praktijk (conform factsheet 05 Werkprocessen).	
RDV1	Gegevensverwerking	Wps artikel 2.24 lid 1 en 2 Wps artikel 2.27 lid 1 t/m 5 Wps 2.30 lid 1 en 2 Wps artikel 2.31 lid 3 en 5 Bp artikel 1.2 lid 1 t/m 4 Bp artikel 1.3 t/m 3 Bp artikel 1.4 lid 1 en 2 Bp artikel 1.6 lid 1 en 2 Bp artikel 2.37 lid 1	De deelnemende partijen opereren binnen de vastgestelde territoriale werkgebieden, waarbij rol en verantwoordelijkheden en governance-structuren voor privacy, conformiteits, rechten van betrokkenden en besluitvorming expliciet zijn vastgelegd en gedocumenteerd. De overnemerdeelnemers zijn gezamenlijk verantwoordelijk voor de gegevensverwerking en nemen hierover de formele besluiten. De bestuurlijke afspraken zijn op hoofdlijnen (aggregeerd) beschreven en worden, waar nodig, nadier uitgewerkt. Deze afspraken vormen het uitgangspunt en worden aangevuld met regionale of lokale uitwerkingen, zoals een privacybeleid, om de praktische toepasbaarheid en aantoonbaarheid te borgen.	De samenwerking binnen het ZVH is formeel vastgelegd in bestuurlijke afspraken tussen de deelnemende partijen. De overnemerdeelnemers zijn gezamenlijk verantwoordelijk voor de gegevensverwerking en nemen hierover de formele besluiten. De bestuurlijke afspraken zijn op hoofdlijnen (aggregeerd) beschreven en worden, waar nodig, nadier uitgewerkt. Deze afspraken vormen het uitgangspunt en worden aangevuld met regionale of lokale uitwerkingen, zoals een privacybeleid, om de praktische toepasbaarheid en aantoonbaarheid te borgen.	Borg dat de bestuurlijke afspraken en besluiten over de samenwerking binnen het ZVH actueel en geldig zijn, en maak aantoonbaar dat deze periodiek worden herzien en vastgesteld door de staatsorgaan, bijvoorbeeld via vastgelegde governance-documenten, herzieningsdata en besluitvorming. Zorg dat de gezamenlijke verwerkingsverantwoordelijkheid van overnemerdeelnemers voor gegevensverwerking en besluitvorming expliciet is uitgewerkt, en toon aan dat deze is vastgelegd in bestuurlijke afspraken, convenanten of reglementen conform factsheet 04 Deelnemers aan het samenwerkingverband. Borg dat de afspraken zijn vastgesteld na uitvoerbare werkstructuur en beleid (bijv. privacybeleid en werkprocessen), en maak aantoonbaar dat deze aansluiten op de praktijk conform factsheet 05 Werkprocessen.	Bestaan Beoordeel de bestuurlijke afspraken en besluiten actueel en geldig zijn vastgesteld, door het beoordelen van governance-documenten en bestuurlijke afspraken, waarbij wordt vastgesteld dat herzieningsdata en besluitvorming zijn vastgelegd. Verifieer dat de gezamenlijke verwerkingsverantwoordelijkheid van de deelnemers expliciet is uitgewerkt, door het beoordelen van bestuurlijke afspraken, convenanten of reglementen, waarbij wordt vastgesteld dat rollen, verantwoordelijkheden en besluitvorming zijn vastgesteld conform factsheet 04) Beoordeel of afspraken zijn vastgesteld na uitvoerbare werkstructuur en beleid, door het beoordelen van privacybeleid en werkprocessen, waarbij wordt vastgesteld dat deze aansluiten op de praktijk (conform factsheet 05 Werkprocessen).	
Wp-G4.1	Autorisatiebeheer	Wps artikel 2.24 lid 1 en 2 Wps artikel 2.27 lid 1 t/m 5 Wps artikel 2.31 lid 11 Bp artikel 1.2 lid 1 t/m 4 Bp artikel 1.3 t/m 3 Bp artikel 1.4 lid 1 en 2 Bp artikel 1.6 lid 1 en 2 Bp artikel 2.37 lid 1	Het Zorg- en Veiligheidsbuis borgt de toegang tot persoonsgegevens uitsluitend wordt verleend aan geautoriseerde gebruikers op basis van hun rol, taak en betrokkenheid bij een casus. Het Zorg- en Veiligheidsbuis beschikt over een actuele autorisatiematraris waarin per rol is vastgelegd: • welke gegevens toegankelijk zijn; • welke handelingen mogen worden uitgevoerd; • wie verantwoordelijk is voor het toekennen, wijzigen en intrekken van autorisaties. Autorisaties worden verleend volgens het need-to-know-principe en worden periodiek beoordeeld om vast te stellen dat de toegewezen rechten nog passen en noodzakelijk zijn voor de uitvoering van de werkzaamheden binnen het Zorg- en Veiligheidsbuis. Wijzigingen in functies, taken of uitsluitendreding leiden tijdig tot aanpassing of intrekking van autorisaties.	Binnen het Zorg- en Veiligheidsbuis wordt toegang tot persoonsgegevens beperkt tot personen die deze gegevens nodig hebben voor de uitvoering van hun werkzaamheden binnen een specifieke casus. Het Zorg- en Veiligheidsbuis kent hierover een autorisatiebeleid waarin is vastgelegd hoe autorisaties worden aangevraagd, toegewezen, gewijzigd en ingetrokken. Autorisaties worden toegewezen op basis van functies, taken en betrokkenheid bij een casus (need-to-know-principe). In een autorisatiematraris is vastgelegd welke gebruikers of gebruikersrollen toegang hebben tot welke gegevens en functionaliteiten. Het Zorg- en Veiligheidsbuis voert periodiek controles uit op de toegewezen autorisaties om vast te stellen dat toegangsrechten nog passen en noodzakelijk zijn. Wijzigingen in functies, taken of uitsluitendreding leiden tijdig tot aanpassing of intrekking van autorisaties.	Borg dat toegang tot persoonsgegevens uitsluitend plaatsvindt op basis van geautoriseerde rollen en bevoegdheden, en maak aantoonbaar dat het ZVH beschikt over een actuele autorisatiematraris waarin minimaal rollen, toegangsrechten en toegewezen gegevensverwerkingen zijn vastgelegd. Zorg dat procedures zijn ingericht voor het aanvragen, toekennen, wijzigen en intrekken van autorisaties, en maak aantoonbaar dat deze procedures zijn vastgelegd en worden toegepast. Borg dat de autorisaties zijn gebaseerd op het need-to-know-principe, en toon aan dat uitsluitend toegang wordt verleend tot gegevens die noodzakelijk zijn voor de uitvoering van de werkzaamheden binnen een casus. Borg dat de afspraken zijn vastgesteld na uitvoerbare werkstructuur en beleid (bijv. privacybeleid en werkprocessen), en maak aantoonbaar dat deze aansluiten op de praktijk conform factsheet 05 Werkprocessen. Zorg dat wijzigingen in functies, taken of uitsluitendreding tijdig tot aanpassing of intrekking van autorisaties, en toon aan dat dit aantoonbaar wordt geregistreerd.	Bestaan Verrifieer dat een actuele autorisatiematraris aanwezig is, door het beoordelen van autorisatieoverzichten en beleidsdocumentatie, waarbij wordt vastgesteld dat rollen en toegangsrechten expliciet zijn vastgelegd. Stel vast dat de procedures aanwezig zijn voor het aanvragen, wijzigen en intrekken van autorisaties, door het beoordelen van werkstructuur, formulieren en registraties. Controleer of periodieke autorisatiereviews worden uitgevoerd en vastgesteld, door het beoordelen van reviewrapporten, controlelijsten of overige documentatie. Stel vast dat registraties aanwezig zijn van toegewezen, gewijzigde en ingetrokken autorisaties. Werkings Voor een steekproef uit op gebruikersaccounts, autorisaties en autorisatieoverzichten en beoordeel of: a. toegewezen autorisaties aansluiten op de functie, rol en betrokkenheid van de gebruiker bij een casus; b. uitsluitend toegang bestaat tot persoonsgegevens die noodzakelijk zijn voor de uitvoering van de werkzaamheden (need-to-know-principe); c. autorisaties overeenkomen met de vastgelegde autorisatiereviews; d. wijzigingen in functies, taken of uitsluitendreding tijdig hebben geleid tot wijziging of intrekking van autorisaties; e. periodieke autorisatiereviews daadwerkelijk zijn uitgevoerd en eventuele afwijkingen aantoonbaar zijn opgevolgd.	
Wp-G4.2							

RRED1	Afakening rollen & verantwoordelijkheden	Wps artikel 1.4 lid 2 en lid 3 Wps artikel 2.24 lid 1 en 2 Wps artikel 2.27 lid 1 t/m 5 Wps artikel 2.31 lid 4 Bp: artikel 1.1 lid 2 Bp: artikel 1.2 lid 1 t/m 4 Bp: artikel 1.3 t/m 3 Bp: artikel 1.4 lid 1 en 2 Bp: artikel 2.21 lid 1 en 3	Het Zorg- en Veiligheidshuis, stelt bij elke verwerking van persoonsgegevens vast en documenteert of zij verwerker of verwerkingsverantwoordelijke is.	Binnen het Zorg- en Veiligheidshuis (ZVH) is de verwerking van persoonsgegevens ingericht op basis van de activiteiten zoals in de WGS zijn vastgelegd. In de wet is expliciet bepaald welke activiteiten plaatsronden en welke partijen daarbij betrokken zijn en welke rol zij vervullen. De WGS schriftelijk voor welke activiteiten binnen het Zorg- en Veiligheidshuis zijn toegestaan, welke gegevens daarvoor gebruikt mogen worden en welke partijen daarbij betrokken zijn. Daarbij wordt ook per activiteit bepaald welke rol een partij heeft, zoals: 1. gezamenlijk verwerkingsverantwoordelijke; 2. uitvoerende partij; 3. of ondersteunende partij. Het Zorg- en Veiligheidshuis is volgens de wet geen rechtspersoon of entiteit. Er is daarom geen sprake van gegevensverwerking door één afzonderlijke entiteit, maar van gezamenlijke gegevensverwerking binnen het Zorg- en Veiligheidshuis. Dit betekent dat de betrokken partijen in veel gevallen optreden als gezamenlijk verwerkingsverantwoordelijken.	Borg dat per activiteit binnen het ZVH is vastgesteld welke persoonsgegevens worden verwerkt, welke partijen hierbij betrokken zijn en welke rol zij vervullen (gezamenlijk verwerkingsverantwoordelijke, uitvoerende of ondersteunende partij), en maak aantoonbaar dat dit is vastgelegd in een actueel overzicht (bijv., verwerkingsregister, procesbeschrijving of conversant) conform de WGS en factsheet 04 Deelnemers. Zorg dat de gezamenlijke verantwoordelijkheid voor gegevensverwerking binnen het Zorg- en Veiligheidshuis expliciet is ingericht en toegepast, en toon aan dat besluitvorming en verwerking plaatsvinden conform de werkwijze van het Veiligheidshuis zijn via causaleiden, besluitvorming en werkprocessen, conform factsheet 05 Werkprocessen.	Opzet - Bepaal of beleid, processen en procedures zijn ingericht voor het vastleggen van gegevensverwerking per activiteit binnen het Zorg- en Veiligheidshuis, door het beoornden van beleidsdocumenten, procesbeschrijvingen en werkstructuuren, waarbij is opgenomen welke gegevens worden verwerkt, welke partijen betrokken zijn en welke rol zij vervullen. Betaan - Beoornd of per activiteit binnen het ZVH is vastgesteld welke persoonsgegevens worden verwerkt en welke partijen daarbij betrokken zijn, door het beoornden van het verwerkingsregister en procesbeschrijvingen, waarbij wordt vastgesteld dat rollen (bijv., gezamenlijk verwerkende, uitvoerende partij) expliciet zijn opgenomen (conform factsheet 04).	Werking - Voor een steekproef uit op het verwerkingsregister of beoornd de bestuurlijke afpakken en stel vast: a. de uitvoering van gegevensverwerkingen aansluit op de vastgelegde activiteiten en rollen; b. de betrokken partijen handelen conform de vastgelegde rolverdeling (bijv., gezamenlijk verwerkende partij); c. verwerkingen en besluitvorming per casus of activiteit herleidbaar zijn vastgelegd (bijv., in werkprocessen); d. de toepassing in de praktijk in lijn is met de vastgelegde afpakken en werkprocessen (conform factsheet 05).
RRED3	Afakening rollen & verantwoordelijkheden	Wps artikel 1.4 lid 2 en lid 3 Wps artikel 2.24 lid 1 en 2 Wps artikel 2.27 lid 1 t/m 5 Wps artikel 2.31 lid 4 Bp: artikel 1.1 lid 2 Bp: artikel 1.2 lid 1 t/m 4 Bp: artikel 1.3 t/m 3 Bp: artikel 1.4 lid 1 en 2 Bp: artikel 2.21 lid 1 en 3	(a) In de gevallen dat het Zorg- en Veiligheidshuis als verwerkingsverantwoordelijke optreedt, doet deze een overeenkomst met de verwerkers waarin de verantwoordelijkheden van de verwerker met betrekking tot privacy en bescherming van persoonsgegevens zijn vastgelegd. Indien het Zorg- en Veiligheidshuis als gezamenlijke verwerkingsverantwoordelijke optreedt, worden afspraken gemaakt met de andere verwerkingsverantwoordelijke.	Het Zorg- en Veiligheidshuis heeft de verwerkingsactiviteiten per wet toegewezen gekregen en de deelnemers treden in alle gevallen op als gezamenlijk verwerkingsverantwoordelijke. Derhalve is individuele verantwoordelijkheid niet van toepassing. Binnen de WGS worden rollen en verantwoordelijkheden voor gegevensverwerking vooraf vastgesteld binnen het kader van het Zorg- en Veiligheidshuis. Verwerkingsovereenkomsten en afspraken tussen (gezamenlijke) verwerkingsverantwoordelijken vormen een nadere contractuele uitwerking hiervan en dienen in lijn te zijn met het gezamenlijke doel, de governance en de wettelijke kaders. Deze afspraken worden operationeel geboord per "thuis", bijvoorbeeld via afzonderlijke dienstverleningsovereenkomsten (DVO's), waarin de relevante verplichtingen en verantwoordelijkheden zijn vastgelegd.	Borg dat binnen het Zorg- en Veiligheidshuis afspraken zijn vastgesteld over rollen en verantwoordelijkheden voor gegevensverwerking, en maak aantoonbaar dat deze zijn opgenomen in bestuurlijke afspraken, convenanten of reglementen, conform factsheet 04 Deelnemers aan het Zorg- en Veiligheidshuis. Zorg dat per activiteit duidelijk is welke partijen betrokken zijn bij de gegevensverwerking en welke rol zij vervullen (gezamenlijk verwerkingsverantwoordelijk, uitvoerende of ondersteunend), en toon aan dat dit is vastgelegd in procesbeschrijvingen, werkspraken of het verwerkingsregister.	Opzet - Beoornd of beleid, processen en procedures zijn ingericht voor het vastleggen van rollen en verantwoordelijkheden binnen het Zorg- en Veiligheidshuis, door het beoornden van bestuurlijke afspraken, convenanten en governance-documentatie, waarbij is opgenomen dat rollen vooraf worden vastgesteld conform de WGS. Betaan - Stel vast dat rollen en verantwoordelijkheden expliciet zijn vastgesteld, door het beoornden van bestuurlijke afspraken, convenanten of reglementen (conform factsheet 04). - Stel vast dat per activiteit is vastgesteld welke partijen betrokken zijn en welke rol zij vervullen, door het beoornden van procesbeschrijvingen, werkspraken of het verwerkingsregister.	Werking Niet van toepassing. De norm ziet op de formele vastlegging van rollen en verantwoordelijkheden binnen het Zorg- en Veiligheidshuis. De effectiviteit wordt beoornd door middel van de opzet- en bestaansdelen, waarbij wordt vastgesteld dat de rollen en verantwoordelijkheden aantoonbaar zijn vastgesteld in bestuurlijke afspraken, overeenkomsten en/of het verwerkingsregister.
RRED4	Afakening rollen & verantwoordelijkheden	Wps artikel 1.4 lid 2 en lid 3 Wps artikel 2.24 lid 1 en 2 Wps artikel 2.27 lid 1 t/m 5 Wps artikel 2.31 lid 4 Bp: artikel 1.1 lid 2 Bp: artikel 1.2 lid 1 t/m 4 Bp: artikel 1.3 t/m 3 Bp: artikel 1.4 lid 1 en 2 Bp: artikel 2.21 lid 1 en 3	Het Zorg- en Veiligheidshuis belast een of meerdere personen met de verantwoordelijkheid voor de coördinatie van de privacybeheersing. De taken, bevoegdheden en verantwoordelijkheden van deze persoon(en) worden duidelijk omschreven en gereguleerd herin.	Binnen de WGS en het BGS is vermeld dat rollen, taken en verantwoordelijkheden rond gegevensverwerking duidelijk worden belegd. In de bestuurlijke afspraken is dit uitgewerkt via specifieke rollen (zoals netwerkmanager, procesregisseur en coördinerend FG), maar zonder expliciete aanwijzing van één centrale privacyverantwoordelijke. De verantwoordelijkheid voor privacybeheersing ligt daarmee bij de gezamenlijke inrichting van deze rollen en bij de stuurgroep en gezamenlijk verwerkingsverantwoordelijken. Taken, bevoegdheden en verantwoordelijkheden zijn vastgesteld en worden periodiek geëvalueerd en geactualiseerd.	Borg dat rollen, taken en verantwoordelijkheden voor privacybeheer en gegevensverwerking duidelijk zijn belegd binnen het ZVH, en maak aantoonbaar dat deze zijn vastgelegd in bestuurlijke afspraken, functiebeschrijvingen of een rol en verantwoordelijkhedenoverzicht. Zorg dat deze rolverdeling is uitgewerkt in concrete rollen (zoals netwerkmanager, procesregisseur en coördinerend FG), en toon aan dat per rol taken, bevoegdheden en verantwoordelijkheden zijn vastgesteld en toegepast in de werkwijze en besluitvorming. - Waarborg dat de verantwoordelijkheid voor privacybeheer ligt bij de gezamenlijke verwerkingsverantwoordelijken en de stuurgroep, en maak aantoonbaar dat deze governance is ingericht en functioneert via besluitvorming, overlegstructuren en rapportages. - Borg dat rollen en verantwoordelijkheden periodiek worden geëvalueerd en geactualiseerd, en toon aan dat deze actualisaties plaatsvinden via herzieningen van documenten, evaluatie of besluitvorming binnen de stuurgroep.	Opzet - Stel vast dat beleid, processen en procedures zijn ingericht voor het vastleggen van rollen, taken en verantwoordelijkheden voor privacybeheer, door het beoornden van bestuurlijke afspraken, functiebeschrijvingen en rol- en verantwoordelijkhedenoverzichten. id. Betaan - Stel vast dat rollen en verantwoordelijkheden expliciet zijn uitgewerkt, door het beoornden van governance-documenten, waarbij per rol taken, bevoegdheden en verantwoordelijkheden zijn vastgelegd. - Stel vast dat een centrale privacyrol (bijv., FG/coördinerend FG) is aangewezen, door het beoornden van functiebeschrijvingen en mandaten. - Stel vast dat rollen en verantwoordelijkheden periodiek worden geëvalueerd en geactualiseerd, door het beoornden van herzieningen van documenten en besluitvorming binnen de stuurgroep.	Werking - Trek een steekproef uit documentatie en controleer: a. of de coördinerend FG betrokken is bij privacyvraagstukken en afstemming; b. of besluitvorming plaatsvindt conform de vastgelegde governance-structuur; c. of wijzigingen en actualisaties aantoonbaar worden doorgevoerd en vastgelegd.
RRED6	Afakening rollen & verantwoordelijkheden	Wps artikel 1.4 lid 2 en lid 3 Wps artikel 2.24 lid 1 en 2 Wps artikel 2.27 lid 1 t/m 5 Wps artikel 2.31 lid 4 Bp: artikel 1.1 lid 2 Bp: artikel 1.2 lid 1 t/m 4 Bp: artikel 1.3 t/m 3 Bp: artikel 1.4 lid 1 en 2 Bp: artikel 2.21 lid 1 en 3	Indien vereist door wet- en regelgeving wijst de het Zorg- en Veiligheidshuis een Coördinerend Functionaris Gegevensbescherming (FG) aan en belast die met advies over en toezicht op de verwerking van persoonsgegevens, in overeenstemming met de eisen die de wet aan de functie van FG stelt.	De deelnemers van het Zorg- en Veiligheidshuis wijzen één van de functionarissen voor gegevensbescherming van de deelnemende overheidsinstellingen of overheidsorganen aan als coördinerend functionaris voor gegevensbescherming (FG), die zorgdraagt voor de afstemming en coördinatie van de privacykansen binnen het Zorg- en Veiligheidshuis.	- Stel vast dat een coördinerend functionaris gegevensbescherming (FG) is aangewezen , conform factsheet 02 Coördinerend functionaris gegevensbescherming. - Controleer dat de rol, taken en verantwoordelijkheden van de coördinerend FG staan opgenomen de bestuurlijke afspraken en dat deze zijn afgestemd met de deelnemers. - Stel vast dat de coördinerend FG betrokken is bij toezicht en afstemming op privacy binnen het Zorg- en Veiligheidshuis, conform factsheet 02 Coördinerend functionaris gegevensbescherming.	Opzet - Stel vast dat beleid, processen en procedures zijn ingericht voor het aanwijzen van een coördinerend FG en het vastleggen van diens rol, door het beoornden van bestuurlijke afspraken, functiebeschrijvingen en governance-documentatie (conform factsheet 02). Betaan - Stel vast dat een coördinerend FG formeel is aangewezen, door het beoornden van benoemingsbesteden of bestuurlijke afspraken. - Stel vast dat rollen, taken en verantwoordelijkheden van de coördinerend FG zijn vastgesteld, door het beoornden van functiebeschrijvingen en governance-documentatie.	Werking - Trek een steekproef uit documentatie en controleer: a. of de coördinerend FG betrokken is bij privacyvraagstukken en afstemming; b. of afstemming en coördinatie aantoonbaar zijn vastgelegd (bijv., in notulen of documentatie); c. of de rol in de praktijk wordt uitgevoerd conform de vastgelegde afspraken.
Wp-GS	Nationaliteit	Wps artikel 2.29 lid 1 Wps artikel 2.25 Bp: artikel 1.9	Het Zorg- en Veiligheidshuis borg dat persoonsgegevens waaruit nationaliteit blijkt, uitsluitend worden verwerkt indien dit noodzakelijk is voor de uitvoering van de bij of krachtens de WGS aangewezen activiteiten en deze verwerking wettelijk is toegestaan. Aanverweten en deelnemers worden geïnformeerd over de wettelijke bepalingen die gelden voor de verwerking van gegevens waaruit nationaliteit blijkt. Indien dergelijke gegevens binnen een casus worden verwerkt, vindt dit uitsluitend plaats voor zover dit noodzakelijk is voor de uitvoering van de wettelijke taak van het Zorg- en Veiligheidshuis	De Wp stelt aanvullende eisen aan de verwerking van persoonsgegevens waaruit nationaliteit blijkt. Binnen het Zorg- en Veiligheidshuis mogen nationaliteit worden verwerkt indien: - Noodzakelijk is voor de uitvoering van de wettelijke taken van het samenwerkingsovereenkomst. - De norm beoogt niet op dossierniveau per persoonsgegevens wordt vastgelegd tot welke categorie dit behoort. Het uitgangspunt is dat deelnemers en registers bekend zijn met de voorwaarden waaronder gegevens waaruit nationaliteit blijkt mogen worden verwerkt en deze voorwaarden toepassen binnen de reguliere casusbehandeling en werkprocessen	- Zorg dat in beleid, werkstructuuren of factsheet aandacht wordt besteed aan de voorwaarden voor verwerking van persoonsgegevens waaruit nationaliteit blijkt. - Maak aantoonbaar dat medewerkers en deelnemers worden geïnformeerd over deze voorwaarden, bijvoorbeeld via instructies, opleidingen, factsheet of werkprocessen. - Indien persoonsgegevens waaruit nationaliteit blijkt zijn verwerkt, moet aantoonbaar zijn dat dit heeft plaatsgevonden in het kader van een wettelijke taak van het Zorg- en Veiligheidshuis.	Opzet - Stel vast dat beleid, werkstructuuren of factsheet aandacht besteden aan de verwerking van persoonsgegevens waaruit nationaliteit blijkt. - Stel vast dat deelnemers worden geïnformeerd over de voorwaarden waaronder deze gegevens mogen worden verwerkt. Betaan - Verifieer dat documentatie aanwezig is waarin voorwaarden voor verwerking van persoonsgegevens waaruit nationaliteit blijkt zijn opgenomen. - Stel vast dat deze voorwaarden onderdeel uitmaken van de werkwijze, instructies of opleidingen van het Zorg- en Veiligheidshuis.	Werking - Trek een steekproef uit documentatie en controleer: a. of de gegevens die gedeeltelijk de beoogde/verrekenbare persoonsgegevens waaruit nationaliteit blijkt zijn verwerkt; - Indien hiervan geen sprake is, leg dit vast als non-occurrence - Indien hiervan wel sprake is, beoornd aan de hand van een steekproef of de verwerking plaatsvindt in het kader van een wettelijke taak van het Zorg- en Veiligheidshuis en niet verder ging dan noodzakelijk.
FD01	Identificatie en classificatie van persoonsgegevens	Wps artikel 2.29 lid 1 Bp: artikel 1.9	Het Zorg- en Veiligheidshuis identificeert en documenteert verwerking van persoonsgegevens aan de hand van een gedocumenteerd proces, en classificeert persoonsgegevens als zodanig. Dit omvat tevens de betrokken verwerkingsprocessen, toegepaste systemen en de gegevensverwerking door of namens deelnemers en andere betrokken deelnemers binnen het Zorg- en Veiligheidshuis.	Deze norm geeft invulling aan artikel 2.29 lid 1 WGS en artikel 1.9 BGS en ziet op het structureel identificeren en classificeren van persoonsgegevens. Het Zorg- en Veiligheidshuis hanteert hiervoor een gedocumenteerd proces, waarmee verwerkingen, betrokken processen, systemen en partijen systematisch worden vastgelegd en actueel gehouden.	- Borg dat verwerkingen van persoonsgegevens worden geïdentificeerd en gedocumenteerd via een gestructureerd proces, en maak aantoonbaar dat dit is vastgelegd in procesdocumentatie of het verwerkingsregister, conform factsheet 05 Werkprocessen. - Stel vast dat persoonsgegevens worden geïdentificeerd (incl. soort gegevens en grondslag) en actueel worden gehouden, conform de werkstructuuren XX en L.B factsheet beleid. - Leg vast dat ook de bijbehorende processen, systemen en betrokken partijen zijn beschreven en herleidbaar zijn binnen het verwerkingsregister. - Leg vast dat deze registratie periodiek wordt gecontroleerd en bijgewerkt.	Opzet - Stel vast dat beleid, processen en procedures zijn ingericht voor het identificeren en documenteren van verwerkingen van persoonsgegevens, en het classificeren van persoonsgegevens (incl. soort gegevens en grondslag), door het beoornden van bijvoorbeeld procesdocumentatie, werkstructuuren en het verwerkingsregister. Betaan - Stel vast dat verwerkingen van persoonsgegevens aantoonbaar zijn geïdentificeerd en gedocumenteerd, door het beoornden van het verwerkingsregister en/of procesdocumentatie, waarbij wordt vastgesteld dat per verwerking minimaal doel, categorie verwerking en verantwoordelijke partij zijn vastgelegd. - Stel vast dat persoonsgegevens zijn geïdentificeerd (incl. soort gegevens en grondslag) en actueel worden gehouden, door het beoornden van het verwerkingsregister en onderliggende werkstructuuren, waarbij wordt vastgesteld dat classificatie is opgenomen (bijv., type gegevens, grondslag en gevoeligheid) en dat een actualisatieproces is ingericht. - Stel vast dat de bijbehorende processen, systemen en betrokken partijen zijn vastgelegd en herleidbaar zijn binnen het verwerkingsregister, door het beoornden van het verwerkingsregister en gerelateerde documentatie, waarbij wordt vastgesteld dat per verwerking de relevante processen, gebruikte systemen en deelnemende partijen expliciet zijn opgenomen.	Werking - Voor een steekproef uit op het verwerkingsregister en stel vast dat: a. verwerkingen van persoonsgegevens volledig en actueel zijn vastgelegd; b. persoonsgegevens correct zijn geïdentificeerd (incl. soort gegevens en grondslag); c. bijbehorende processen, systemen en betrokken partijen herleidbaar zijn vastgelegd; d. het verwerkingsregister periodiek wordt gecontroleerd en bijgewerkt, door actualisatielasten, versies en controle-activiteiten te beoornden.
FD04	Identificatie en classificatie van persoonsgegevens	Wps artikel 2.29 lid 1 Bp: artikel 1.9	(a) Het Zorg- en Veiligheidshuis houdt een register bij van de verwerkingsactiviteiten met daarin de kenmerken van deze activiteiten (rechtsgeldig, doel, categorieën van gegevens en betrokkenen, oorzaken, doorgiften, en waar mogelijk beveiligingsmaatregelen). De juistheid en volledigheid van dit register wordt jaarlijks beoornd.	Deze norm geeft invulling aan artikel 2.29 lid 1 WGS en artikel 1.9 BGS en ziet op het bijhouden van een actueel register van verwerkingsactiviteiten/Procesbeschrijving binnen het Zorg- en Veiligheidshuis. Het Zorg- en Veiligheidshuis houdt een register bij waarin de kenmerken van de gegevensverwerking in het kader van complexe casuïstiek zijn vastgelegd, waaronder doel, categorieën gegevens en betrokken partijen. De juistheid en volledigheid van dit register wordt periodiek beoornd.	Borg dat een actueel register van verwerkingsactiviteiten wordt bijgehouden, en maak aantoonbaar dat dit register (of een gelijkwaardig document) is vastgesteld en beheerd binnen het ZVH, conform factsheet 05 Werkprocessen; specifiek en formaliseer het te gebruiken document indien dit nog niet eenduidig is vastgesteld. - Stel vast dat per verwerking de belangrijkste kenmerken zijn vastgelegd zoals doel, grondslag, categorieën gegevens, betrokken partijen en beveiligingsmaatregelen. - Waarborg dat de juistheid en volledigheid van het register periodiek (minimaal jaarlijks) wordt gecontroleerd en bijgewerkt. - Borg dat het verwerkingsregister wordt gebruikt als basis voor de uitvoering en controle van gegevensverwerkingen.	Opzet - Stel vast dat beleid, processen en procedures zijn ingericht voor het bijhouden van een actueel verwerkingsregister, door het beoornden van beleid, procesbeschrijvingen en werkstructuuren, waarbij is vastgesteld hoe het register wordt ingericht, beheerd en bijgehouden. Betaan - Stel vast dat per verwerking de belangrijkste kenmerken zijn vastgelegd, door het beoornden van het verwerkingsregister, waarbij wordt vastgesteld dat minimaal doel, grondslag, categorieën persoonsgegevens, betrokken partijen en beveiligingsmaatregelen zijn opgenomen. - Stel vast dat het verwerkingsregister periodiek wordt gecontroleerd en bijgewerkt, door het beoornden van versies, actualisatielasten en/of vastgelegde controle-activiteiten.	Werking - Voor een steekproef uit op eerste casusoverzichten en stel vast dat de volgende betrouwbaarheid is opgenomen: a. de informatie die vertrouwelijk wordt aangemerkt; b. hoe geheimhouding onderdeel is van deelname aan het ZVH; d. hoe naleving van de geheimhoudingsplicht wordt gecontroleerd.
	Vertrouwelijkheid & geheimhouding	Wps artikel 1.11 lid 1 t/m 3 Wps artikel 2.24 lid 1 en 2 Wps artikel 2.27 lid 1 t/m 4 Wps artikel 2.31 lid 4 Bp: artikel 1.2 lid 1 t/m 3 Bp: artikel 1.3 t/m 3 Bp: artikel 1.4 lid 1 en 2 Bp: artikel 2.21 lid 2	Er is geborgd dat eenieder die betrokken is bij de werkzaamheden van het Zorg- en Veiligheidshuis gehouden is tot geheimhouding van persoonsgegevens en andere gegevens waarvan het vertrouwelijke karakter redelijkerwijs bekend is of vermoed kan worden, behoudens wettelijke uitzonderingen. Deze geheimhoudingsplicht is formeel vastgelegd en de naleving hiervan wordt periodiek gecontroleerd.	Binnen het Zorg- en Veiligheidshuis (ZVH) is geborgd dat alle deelnemers voorafgaand aan een samenwerking expliciet worden gewezen op de geheimhoudingsplicht. Dit gebeurt door het beschikbaar stellen en toelichten van de geldende spelregels, bijvoorbeeld via een factsheet of instructiedocument, waarbij deelnemers voorafgaand aan deelname aantoonbaar akkoord geven. Het Zorg- en Veiligheidshuis legt vast hoe deze bevestigingsplicht is ingericht en zorgt dat deze wettelijke structuur en aantoonbaar wordt toegepast, bijvoorbeeld via een afwijking, paraaf of digitale bevestiging. De naleving hiervan kan periodiek, bijvoorbeeld jaarlijks via een steekproef, worden getoetst. Voor specifieke deelnemers (zoals hoofdbestuurlijke deelnemers) kan een uitzondering gelden indien de geheimhoudingsplicht al via de eigen beheerorganisatie is geborgd. In dat geval neemt het Zorg- en Veiligheidshuis hierover een expliciet standpunt in en legt dit formeel vast.	Borg dat alle deelnemers voorafgaand aan deelname aan het casusoverleg aantoonbaar worden gewezen op de geldende geheimhoudingsplicht, inclusief de reikwijdte en uitzonderingen. Maak dit inzichtelijk via bijvoorbeeld onderliggende beleidsdocumentatie of digitale bevestiging of registratie in het systeem. - Leg vast hoe de bevestiging van de geheimhoudingsplicht is ingericht en uitgevoerd binnen het ZVH, en toon aan dat deze wettelijke structuur en uniform wordt toegepast (bijvoorbeeld via werkstructuuren en procesbeschrijvingen). Onderbouw dat naleving periodiek wordt getoetst, bijvoorbeeld jaarlijks via een steekproef of interne controle. - Stel vast hoe wordt omgegaan met uitzonderingsituaties, zoals deelnemers waarvan de geheimhoudingsplicht via het beheerorganisatie is geborgd. Onderbouw dat het Zorg- en Veiligheidshuis hierover een expliciet standpunt inneemt en dit formeel vastlegt (bijvoorbeeld in bestuurlijke afspraken of beleid).	Opzet - Stel vast dat beleid, procedures, convenanten of deelnemersafspraken zijn vastgesteld waarin de geheimhoudingsplicht is opgenomen. - Bepaal of hiern minimaal is vastgelegd: a. welke personen onder de geheimhoudingsplicht vallen; b. welke informatie als vertrouwelijk wordt aangemerkt; c. hoe geheimhouding onderdeel is van deelname aan het ZVH; d. hoe naleving van de geheimhoudingsplicht wordt gecontroleerd. Betaan - Stel vast dat deelnemers aantoonbaar de geheimhoudingsplicht hebben geaccepteerd, door het beoornden van onderliggende verklaringen, registraties of digitale bevestigingen. - Stel vast dat deze wettelijke structuur is ingericht, door het beoornden van werkstructuuren en procesbeschrijvingen, waarbij wordt vastgesteld dat toepassing verplicht is gesteld. - Stel vast dat uitzonderingen op de geheimhoudingsplicht expliciet zijn vastgelegd, door het beoornden van bestuurlijke afspraken of beleid.	Werking - Voor een steekproef uit op eerste casusoverzichten en stel vast dat de volgende vertrouwelijkheid is opgenomen: a. de informatie die vertrouwelijk wordt aangemerkt; b. hoe geheimhouding onderdeel is van deelname aan het ZVH; d. hoe naleving van de geheimhoudingsplicht overeenkomstig de vastgelegde werkwijze onder de aandacht van deelnemers wordt gebracht.

	Vertrouwelijkheid & geheimhouding	Wps artikel 1.11 lid 1 t/m 3	(a) Indien binnen- en Veiligheidsbusholdings oplossen van derden/leveranciers verwerf of proces aan dienstverleners uitbestedt en de verwerking van persoonsgegevens (gedeeltelijk) extern plaatsvindt, worden formele overeenkomsten aan de die derden over verplichten de nodige vertrouwelijkheid te betrekken en een beschermingsniveau te waarborgen dat gelijk is aan dat van de het samenwerkingsverband
TPA01	Vertrouwelijkheid & geheimhouding	Wps artikel 1.11 lid 1 t/m 3	Het Zorg- en Veiligheidsbusholdings zorg dat in de overeenkomsten eveneens de volgende verplichtingen voor de andere partij zijn opgenomen: a. vertrouwelijkheid- en geheimhouding; b. beveiligingsmaatregelen; c. medewerking bij het behandelen van verzoeken van betrokkenen en de uitoefening van rechten van de betrokkenen; d. informatieovereenkomst (bijv. in het geval van geplande uitwisseling van informatie); e. informatieovereenkomst en medewerking bij informatie in verband met persoonsgegevens; f. bewaartijdens en verwijdering van gegevens; g. geen verdere uitbesteding zonder toestemming van de entiteit; h. aansprakelijkheid en vrijwaring. Het Zorg- en Veiligheidsbusholdings evalueert periodiek de prestaties en de naleving van de verplichtingen door derden/leveranciers en neemt waar nodig corrigerende acties af die deze evalueert voortvloeien.
TPA02	Vertrouwelijkheid & geheimhouding	Wps artikel 1.11 lid 1 t/m 3 Bp artikel 1.10 lid 2	Het Zorg- en Veiligheidsbusholdings doet afpakken over vertrouwelijkheid en geheimhouding zijn vastgesteld en bevestigd eventuele afpakken van afwikkelingen binnen de governance-structuur (bijv. casuïstiek van RAC). Het Zorg- en Veiligheidsbusholdings doet afpakken over vertrouwelijkheid en geheimhouding zijn vastgesteld en bevestigd eventuele afpakken van afwikkelingen binnen de governance-structuur (bijv. casuïstiek van RAC).
TPA03	Behandeling van privacyincidenten en inbreuken	Wps artikel 1.4 lid 4 Bp artikel 1.4 lid 2 en 3 Bp artikel 1.2 lid 1 t/m 4	Het Zorg- en Veiligheidsbusholdings heeft een formele proces vastgesteld en getijmgepast dat is gericht op het beheer van privacyincidenten en inbreuken in verband met persoonsgegevens. De verantwoordelijkheid van medewerkers om de aangewezen privacy officer of FG in te lichten wanneer er sprake is van een privacyincident of een mogelijke inbreuk in verband met persoonsgegevens. De privacy officer (of, indien van toepassing de security officer) beoordeelt of het een privacygerelateerd incident betreft, indien en inbreuk in verband met persoonsgegevens heeft plaatsgevonden, documenteert de privacy officer of FG dit aan de inbreuk, de gevolgen en, bij benadering, het aantal persoonsgegevens (verzamelingen) en betrokkenen in kwestie. De privacy officer instelt en coördineert de nodige correctieve maatregelen en bepaalt welke personen hierbij betrokken dienen te worden en welke belanghebbenden moeten worden geïnformeerd zoals de verantwoordelijkheid van de betroffene of de betroffene, of de toezichthouder als de betroffene verantwoordelijkheid is. De privacy officer of FG houdt toezicht op de voortgang van de corrigerende maatregelen en levert het management in, indien van toepassing, de verantwoordelijkheid van de toezichthouder.
PI01	Behandeling van privacyincidenten en inbreuken	Wps artikel 1.4 lid 4 Bp artikel 1.4 lid 2 en 3 Bp artikel 1.2 lid 1 t/m 4	Het Zorg- en Veiligheidsbusholdings heeft een formele proces vastgesteld en getijmgepast dat is gericht op het beheer van privacyincidenten en inbreuken in verband met persoonsgegevens. De verantwoordelijkheid van medewerkers om de aangewezen privacy officer of FG in te lichten wanneer er sprake is van een privacyincident of een mogelijke inbreuk in verband met persoonsgegevens. De privacy officer (of, indien van toepassing de security officer) beoordeelt of het een privacygerelateerd incident betreft, indien en inbreuk in verband met persoonsgegevens heeft plaatsgevonden, documenteert de privacy officer of FG dit aan de inbreuk, de gevolgen en, bij benadering, het aantal persoonsgegevens (verzamelingen) en betrokkenen in kwestie. De privacy officer instelt en coördineert de nodige correctieve maatregelen en bepaalt welke personen hierbij betrokken dienen te worden en welke belanghebbenden moeten worden geïnformeerd zoals de verantwoordelijkheid van de betroffene of de betroffene, of de toezichthouder als de betroffene verantwoordelijkheid is. De privacy officer of FG houdt toezicht op de voortgang van de corrigerende maatregelen en levert het management in, indien van toepassing, de verantwoordelijkheid van de toezichthouder.
PI03	Behandeling van privacyincidenten en inbreuken	Wps artikel 1.4 lid 4 Bp artikel 1.4 lid 2 en 3 Bp artikel 1.2 lid 1 t/m 4	Het Zorg- en Veiligheidsbusholdings heeft een formele proces vastgesteld en getijmgepast dat is gericht op het beheer van privacyincidenten en inbreuken in verband met persoonsgegevens. De verantwoordelijkheid van medewerkers om de aangewezen privacy officer of FG in te lichten wanneer er sprake is van een privacyincident of een mogelijke inbreuk in verband met persoonsgegevens. De privacy officer (of, indien van toepassing de security officer) beoordeelt of het een privacygerelateerd incident betreft, indien en inbreuk in verband met persoonsgegevens heeft plaatsgevonden, documenteert de privacy officer of FG dit aan de inbreuk, de gevolgen en, bij benadering, het aantal persoonsgegevens (verzamelingen) en betrokkenen in kwestie. De privacy officer instelt en coördineert de nodige correctieve maatregelen en bepaalt welke personen hierbij betrokken dienen te worden en welke belanghebbenden moeten worden geïnformeerd zoals de verantwoordelijkheid van de betroffene of de betroffene, of de toezichthouder als de betroffene verantwoordelijkheid is. De privacy officer of FG houdt toezicht op de voortgang van de corrigerende maatregelen en levert het management in, indien van toepassing, de verantwoordelijkheid van de toezichthouder.
PI04	Behandeling van privacyincidenten en inbreuken	Wps artikel 1.4 lid 4 Bp artikel 1.4 lid 2 en 3 Bp artikel 1.2 lid 1 t/m 4	Het Zorg- en Veiligheidsbusholdings heeft een formele proces vastgesteld en getijmgepast dat is gericht op het beheer van privacyincidenten en inbreuken in verband met persoonsgegevens. De verantwoordelijkheid van medewerkers om de aangewezen privacy officer of FG in te lichten wanneer er sprake is van een privacyincident of een mogelijke inbreuk in verband met persoonsgegevens. De privacy officer (of, indien van toepassing de security officer) beoordeelt of het een privacygerelateerd incident betreft, indien en inbreuk in verband met persoonsgegevens heeft plaatsgevonden, documenteert de privacy officer of FG dit aan de inbreuk, de gevolgen en, bij benadering, het aantal persoonsgegevens (verzamelingen) en betrokkenen in kwestie. De privacy officer instelt en coördineert de nodige correctieve maatregelen en bepaalt welke personen hierbij betrokken dienen te worden en welke belanghebbenden moeten worden geïnformeerd zoals de verantwoordelijkheid van de betroffene of de betroffene, of de toezichthouder als de betroffene verantwoordelijkheid is. De privacy officer of FG houdt toezicht op de voortgang van de corrigerende maatregelen en levert het management in, indien van toepassing, de verantwoordelijkheid van de toezichthouder.
PI05	Behandeling van privacyincidenten en inbreuken	Wps artikel 1.4 lid 4 Bp artikel 1.4 lid 2 en 3 Bp artikel 1.2 lid 1 t/m 4	Het Zorg- en Veiligheidsbusholdings heeft een formele proces vastgesteld en getijmgepast dat is gericht op het beheer van privacyincidenten en inbreuken in verband met persoonsgegevens. De verantwoordelijkheid van medewerkers om de aangewezen privacy officer of FG in te lichten wanneer er sprake is van een privacyincident of een mogelijke inbreuk in verband met persoonsgegevens. De privacy officer (of, indien van toepassing de security officer) beoordeelt of het een privacygerelateerd incident betreft, indien en inbreuk in verband met persoonsgegevens heeft plaatsgevonden, documenteert de privacy officer of FG dit aan de inbreuk, de gevolgen en, bij benadering, het aantal persoonsgegevens (verzamelingen) en betrokkenen in kwestie. De privacy officer instelt en coördineert de nodige correctieve maatregelen en bepaalt welke personen hierbij betrokken dienen te worden en welke belanghebbenden moeten worden geïnformeerd zoals de verantwoordelijkheid van de betroffene of de betroffene, of de toezichthouder als de betroffene verantwoordelijkheid is. De privacy officer of FG houdt toezicht op de voortgang van de corrigerende maatregelen en levert het management in, indien van toepassing, de verantwoordelijkheid van de toezichthouder.

	Beheer van privacyincidenten en inbreuken	Wps artikel 1.4 i64 Bps artikel 1.4 i61 en 2 Bps artikel 1.2 i61 i104	De procedure voor beheer van privacyincidenten en -inbreuken waarborgt dat op basis van de lering die uit de inbreuk wordt getrokken correcties en verbeteringen worden doorgevoerd, en dat de 'lessons learned' worden gebruikt in bewustwordingsprogramma's voor medewerkers.	Deze norm ziet op het structureel verbeteren van processen naar aanleiding van privacy-incidenten. De overheidsdeelnemers borgen dat uit incidenten lessen worden getrokken en dat corrigerende maatregelen worden doorgevoerd en gebruikt voor bewustwording en verbetering van de organisatie.	• Borg dat op basis van privacy-incidenten en inbreuken corrigerende maatregelen worden bepaald, en maak aantoonbaar dat deze maatregelen worden vastgelegd en doorgevoerd. • Zorg dat structureel lering wordt getrokken uit incidenten, en toon aan dat deze inzichten worden verwerkt in aanpassingen van processen en werkwijzen. • Waarborg dat lessen uit incidenten worden gebruikt voor bewustwording en training van medewerkers, en maak aantoonbaar dat dit plaatsvindt via awareness-programma's of interne communicatie. • Zorg dat verbetermaatregelen in herpuntoen worden gemonteerd en opgevolgd, en toon aan dat de voortgang en effectiviteit hiervan inzichtelijk zijn.	Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het leren van privacy-incidenten en het doorvoeren van verbetermaatregelen, door het beoordelen van beleidsdocumenten en werkinstructies, waarbij is vastgelegd dat incidenten worden geëvalueerd en dat verbeteringen worden doorgevoerd. Bestaan • 'Stel vast dat verbetermaatregelen worden bepaald op basis van incidenten, door het beoordelen van rapportages, evaluaties en actieslijten. • 'Stel vast dat analyse van incidenten wordt uitgevoerd en vastgelegd, door het beoordelen van rapportages (bijv. trends, oorzaken en risicoanalyse). • 'Stel vast dat lessen uit incidenten worden vertaald naar aanpassingen in processen en bewustwording, door het beoordelen van werkinstructies, beleid en trainingsmateriaal. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het beoordelen en analyseren van privacy-incidenten, door het beoordelen van beleidsdocumenten en werkinstructies, waarbij is vastgelegd dat incidenten worden geëvalueerd en dat verbetermaatregelen worden bepaald. Bestaan • 'Stel vast dat privacy-incidenten formeel worden beoordeeld, door het beoordelen van incidentdossiers, waarbij wordt vastgelegd dat evaluaties zijn vastgelegd. • 'Stel vast dat oorzaken en patronen van incidenten worden geanalyseerd, door het beoordelen van rapportages en analyses. • 'Stel vast dat verbetermaatregelen worden bepaald en vastgelegd, door het beoordelen van actieslijten en rapportages. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het periodiek evalueren en actualiseren van het incidentmanagementproces, door het beoordelen van beleidsdocumenten en werkinstructies, waarbij is vastgelegd dat evaluaties minimaal jaarlijks en bij significante wijzigingen of incidenten plaatsvinden. Bestaan • 'Stel vast dat de procedure minimaal jaarlijks wordt geëvalueerd, door het beoordelen van evaluaties, auditrapportages of reviews. • 'Stel vast dat aanpassingen worden gedaan bij wijzigingen in processen of systemen, door het beoordelen van gewijzigde werkinstructies en documentatie. • 'Stel vast dat evaluaties naar aanleiding van incidenten plaatsvinden, door het beoordelen van incidentanalyses en rapportages. Opzet • 'Stel vast dat de procedure is vastgesteld voor opleiding, bewustwording en kennisontwikkeling van procesgebruikers en ondersteunende staf. • 'Stel vast dat instructies of factbooks zijn opgesteld voor de toepasselijke wet- en regelgeving (WGS en BG) en de eisen ten aanzien van gegevensbescherming, doelbinding en proportionaliteit. Bestaan • 'Stel vast dat documentatie beschikbaar is waaruit blijkt welke trainingen procesgebruikers en ondersteunende staf hebben gevolgd. • 'Stel vast dat documentatie beschikbaar is waaruit blijkt dat de opleggers voorafgaand aan het casuïstisch zijn doorgelopen en dat een bevestiging is verkregen van de medewerkers van deelnemende partijen. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het bepalen en borgen van privacycompetenties van medewerkers, door het beoordelen van beleidsdocumenten, richtlijnen en competentieprofielen, waarbij is vastgelegd welke kennis en vaardigheden vereist zijn. Bestaan • 'Stel vast dat vereiste privacycompetenties zijn vastgelegd, door het beoordelen van beleid, richtlijnen en competentieprofielen. • 'Stel vast dat opleiding- en trainingsactiviteiten zijn ingericht, door het beoordelen van opleidingsplannen, e-learningmodules en documentatie. • 'Stel vast dat deelname en uitvoering van trainingen worden vastgelegd, door het beoordelen van opleidingsregistraties en evaluaties. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het vaststellen en beoordelen van privacycompetenties per medewerker (conform SCDO1), door het beoordelen van beleidsdocumenten, richtlijnen en werkinstructies. Bestaan • 'Stel vast dat per medewerker is vastgelegd in hoeverre deze beschikt over de vereiste privacycompetenties, door het beoordelen van HR-registraties, competentieprofielen of beoordelingen. • 'Stel vast dat een proces aanwezig is voor het identificeren en opspelen van lacunes in kennis en vaardigheden, door het beoordelen van beleid, werkinstructies en opleidingsplannen. • 'Stel vast dat privacycompetenties periodiek worden geëvalueerd, door het beoordelen van registraties, beoordelingen of audits. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het meten van privacycompetenties in werving, onboardng en beoordeling, door het beoordelen van beleidsdocumenten, werkinstructies en HR-richtlijnen, waarbij is vastgelegd dat privacy een onderdeel is van selectie en beoordeling. Bestaan • 'Stel vast dat de privacycompetenties zijn opgenomen in functiebeschrijvingen en selectiecriteria, door het beoordelen van HR-documentatie. • 'Stel vast dat onboardingsprogramma's aandacht besteden aan privacy, door het beoordelen van onboardingsdocumentatie en trainingsmateriaal. • 'Stel vast dat privacy onderdeel is van gesprekken en beoordelingen, door het beoordelen van gespreksverlagen, beoordelingsystemen en HR-registraties. Opzet • 'Stel vast dat beleid, procedures of werkinstructies zijn vastgesteld voor het waarborgen van de juistheid en volledigheid van persoonsgegevens. Bestaan • 'Stel vast dat registraties beschikbaar zijn van uitgevoerde correcties. • 'Stel vast dat documentatie aanwezig is waaruit blijkt hoe terugkoppeling naar gegevensleveranciers plaatsvindt. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het verzamelen, valideren en bijhouden van persoonsgegevens, door het beoordelen van beleidsdocumenten en werkinstructies, waarbij is vastgelegd hoe persoonsgegevens worden vastgesteld, gecontroleerd en geactualiseerd. Bestaan • 'Stel vast dat een proces aanwezig is voor het registreren en bijwerken van persoonsgegevens, door het beoordelen van werkinstructies en proceduredocumentatie. • 'Stel vast dat correcties en updates worden vastgelegd, door het beoordelen van registraties en casuïdissen. • 'Stel vast dat periodieke controles op juistheid en volledigheid plaatsvinden, door het beoordelen van controlelijsten en rapportages. Opzet • 'Stel vast dat correcties en updates worden vastgelegd, door het beoordelen van registraties en casuïdissen. • 'Stel vast dat periodieke controles op juistheid en volledigheid plaatsvinden, door het beoordelen van controlelijsten en rapportages.	Werking • 'Trek een steekproef uit incidenten en controleer: a. of incidenten worden geëvalueerd en leiden tot verbetermaatregelen; b. of maatregelen daadwerkelijk worden doorgevoerd; c. of lessen zichtbaar zijn in aanpassende processen en werkwijzen; d. of oplegging en voortgang van maatregelen aantoonbaar worden gemonteerd. Werking • 'Trek een steekproef uit incidenten en controleer: a. of incidenten systematisch worden geëvalueerd; b. of oorzaken en patronen worden meegenomen in de analyse; c. of maatregelen worden vastgesteld naar aanleiding van incidenten; c. of resultaten worden gerapporteerd en gebruikt voor besluitvorming. Voor deze norm is geen afzonderlijke werkingstoets van vastlegging, aanpak en de beoordeling zich richt op de aanwezigheid, volledigheid en actualiteit van de toelichtingen (opzet en bestaan). Werking • 'Selecteer een willekeurige sample uit de lijst van procesgebruikers en/of ondersteunende staf en stel vast dat zij de vereiste training tijdig voorafgaand aan deelname aan het casuïstisch hebben gevolgd. • 'Selecteer een willekeurige casuïstiekgeregule en stel vast dat de geldende veiligheids voorafgaand aan het casuïstisch zijn doorgelopen en bevestigd. Werking • 'Trek een steekproef uit opleidingsregistraties en controleer: a. of medewerkers trainingen volgen conform de vastgestelde eisen; b. of competenties aantoonbaar worden onderhouden; c. of evaluaties van trainingen plaatsvinden; d. of resultaten worden gebruikt voor bijsturing en verbetering. Werking • 'Trek een steekproef uit opleidingsregistraties en controleer: a. of medewerkers trainingen volgen conform de vastgestelde eisen; b. of competenties aantoonbaar worden onderhouden; c. of evaluaties van trainingen plaatsvinden; d. of resultaten worden gebruikt voor bijsturing en verbetering. Werking • 'Trek een steekproef uit medewerkers en controleer of: a. privacycompetenties onderdeel zijn geweest van werving of onboardng; b. privacycompetenties zijn bevestigd tijdens beoordelingsmomenten; c. bevestiging zijn vastgelegd; d. eventuele verbeterpunten zijn opgevolgd; e. privacybewust handelen aantoonbaar wordt gestimuleerd. Werking • 'Trek een steekproef uit lijst met correctie registraties en controleer: a. of correcties aantoonbaar worden vastgelegd; b. of periodieke controles daadwerkelijk worden uitgevoerd; c. of gegevens actueel en bruikbaar zijn voor besluitvorming; d. of de uitkomsten worden vastgelegd in een controle- of auditrapportage.	
P107	Beheer van privacyincidenten en inbreuken	Wps artikel 1.4 i64 Bps artikel 1.4 i61 en 2 Bps artikel 1.2 i61 i104	De procedure voor beheer van privacyincidenten en -inbreuken waarborgt dat: a. na elk beveiligingsincident en inbreuk met betrekking tot persoonsgegevens (datalekken) en elke grootschalige inbreuk in verband met persoonsgegevens een formele incidentbeoordeling wordt uitgevoerd, waarbij indien nodig externe expertise wordt ingeschakeld; b. incidenten worden geëvalueerd en de noodzakelijke verbeteringen worden geïdentificeerd op basis van: d. onderliggende oorzaken van het incident; e. incidentpatronen; o wijzigingen in de interne controle en wetgeving; c. de resultaten van de evaluatie en voortgang van de verbeteringen worden gerapporteerd aan de bevoegdheid voor het management.	Deze norm ziet op het zorgvuldig beoordelen en analyseren van privacy-incidenten binnen het Zorg- en Veiligheidshuis. De overheidsdeelnemers borgen dat incidenten systematisch worden geëvalueerd, inclusief de oorzaken en patronen, en dat op basis daarvan passende verbetermaatregelen worden vastgesteld.	• Borg dat elk privacy-incident in detail formeel wordt beoordeeld, en maak aantoonbaar dat deze beoordeling plaatsvindt op basis van vastgestelde criteria, eventueel met inzet van externe expertise. • Zorg dat incidenten systematisch worden geëvalueerd op onderliggende oorzaken, incidentpatronen en relevante wijzigingen in wet- en regelgeving, en toon aan dat deze analyses worden vastgelegd. • Waarborg dat op basis van deze evaluaties passende verbetermaatregelen worden bepaald, en maak aantoonbaar dat deze maatregelen worden vastgelegd en opgevolgd. • Borg dat de uitkomsten van incidentanalyses en de voortgang van verbeteringen worden gerapporteerd aan het management, en toon aan dat deze rapportages worden gemonteerd en betrokken bij verdere besluitvorming.	Opzet • 'Stel vast dat de procedure voor het beheer van privacy-incidenten en inbreuken minimaal eenmaal per jaar wordt geëvalueerd, en maak aantoonbaar dat deze periodieke beoordeling plaatsvindt (bijv. via evaluaties, reviews of auditrapportages). • 'Zorg dat de procedure wordt aangepast bij significante wijzigingen in systemen of processen, en toon aan dat deze aanpassingen worden vastgelegd en doorgevoerd. • 'Zorg dat de procedure wordt herzien naar aanleiding van ernstige incidenten, en maak aantoonbaar dat evaluaties en verbeteringen zijn uitgevoerd op basis van incidentanalyses. • 'Borg dat de actualiteit van de procedure structureel plaatsvindt en aansluit op de risico's en ontwikkelingen binnen het ZVH, en toon aan dat dit wordt geborgd via documentbeheer, versiening of besluitvorming.	Bestaan • 'Stel vast dat de procedure minimaal jaarlijks wordt geëvalueerd, door het beoordelen van evaluaties, auditrapportages of reviews. • 'Stel vast dat aanpassingen worden gedaan bij wijzigingen in processen of systemen, door het beoordelen van gewijzigde werkinstructies en documentatie. • 'Stel vast dat evaluaties naar aanleiding van incidenten plaatsvinden, door het beoordelen van incidentanalyses en rapportages. Opzet • 'Stel vast dat de procedure is vastgesteld voor opleiding, bewustwording en kennisontwikkeling van procesgebruikers en ondersteunende staf. • 'Stel vast dat instructies of factbooks zijn opgesteld voor de toepasselijke wet- en regelgeving (WGS en BG) en de eisen ten aanzien van gegevensbescherming, doelbinding en proportionaliteit. Bestaan • 'Stel vast dat documentatie beschikbaar is waaruit blijkt welke trainingen procesgebruikers en ondersteunende staf hebben gevolgd. • 'Stel vast dat documentatie beschikbaar is waaruit blijkt dat de opleggers voorafgaand aan het casuïstisch zijn doorgelopen en dat een bevestiging is verkregen van de medewerkers van deelnemende partijen.	Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het bepalen en borgen van privacycompetenties van medewerkers, door het beoordelen van beleidsdocumenten, richtlijnen en competentieprofielen, waarbij is vastgelegd welke kennis en vaardigheden vereist zijn. Bestaan • 'Stel vast dat vereiste privacycompetenties zijn vastgelegd, door het beoordelen van beleid, richtlijnen en competentieprofielen. • 'Stel vast dat opleiding- en trainingsactiviteiten zijn ingericht, door het beoordelen van opleidingsplannen, e-learningmodules en documentatie. • 'Stel vast dat deelname en uitvoering van trainingen worden vastgelegd, door het beoordelen van opleidingsregistraties en evaluaties. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het vaststellen en beoordelen van privacycompetenties per medewerker (conform SCDO1), door het beoordelen van beleidsdocumenten, richtlijnen en werkinstructies. Bestaan • 'Stel vast dat per medewerker is vastgelegd in hoeverre deze beschikt over de vereiste privacycompetenties, door het beoordelen van HR-registraties, competentieprofielen of beoordelingen. • 'Stel vast dat een proces aanwezig is voor het identificeren en opspelen van lacunes in kennis en vaardigheden, door het beoordelen van beleid, werkinstructies en opleidingsplannen. • 'Stel vast dat privacycompetenties periodiek worden geëvalueerd, door het beoordelen van registraties, beoordelingen of audits. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het meten van privacycompetenties in werving, onboardng en beoordeling, door het beoordelen van beleidsdocumenten, werkinstructies en HR-richtlijnen, waarbij is vastgelegd dat privacy een onderdeel is van selectie en beoordeling. Bestaan • 'Stel vast dat de privacycompetenties zijn opgenomen in functiebeschrijvingen en selectiecriteria, door het beoordelen van HR-documentatie. • 'Stel vast dat onboardingsprogramma's aandacht besteden aan privacy, door het beoordelen van onboardingsdocumentatie en trainingsmateriaal. • 'Stel vast dat privacy onderdeel is van gesprekken en beoordelingen, door het beoordelen van gespreksverlagen, beoordelingsystemen en HR-registraties. Opzet • 'Stel vast dat beleid, procedures of werkinstructies zijn vastgesteld voor het waarborgen van de juistheid en volledigheid van persoonsgegevens. Bestaan • 'Stel vast dat registraties beschikbaar zijn van uitgevoerde correcties. • 'Stel vast dat documentatie aanwezig is waaruit blijkt hoe terugkoppeling naar gegevensleveranciers plaatsvindt. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het verzamelen, valideren en bijhouden van persoonsgegevens, door het beoordelen van beleidsdocumenten en werkinstructies, waarbij is vastgelegd hoe persoonsgegevens worden vastgesteld, gecontroleerd en geactualiseerd. Bestaan • 'Stel vast dat een proces aanwezig is voor het registreren en bijwerken van persoonsgegevens, door het beoordelen van werkinstructies en proceduredocumentatie. • 'Stel vast dat correcties en updates worden vastgelegd, door het beoordelen van registraties en casuïdissen. • 'Stel vast dat periodieke controles op juistheid en volledigheid plaatsvinden, door het beoordelen van controlelijsten en rapportages.
P108	Beheer van privacyincidenten en inbreuken	Wps artikel 1.4 i64 Bps artikel 1.4 i61 en 2 Bps artikel 1.2 i61 i104	De procedure voor beheer van inbreuken wordt ten minste eenmaal per jaar geëvalueerd en zonodig herzien, en toevens (1) kort na de implementatie van wijzigende wijzigingen in systemen of procedures, en (2) nadat zich een ernstig incident heeft voorgedaan.	Deze norm ziet op het periodiek evalueren en actualiseren van het incidentmanagementproces. De overheidsdeelnemers borgen dat het proces minimaal jaarlijks wordt beoordeeld en waar nodig wordt aangepast, bijvoorbeeld na wijzigingen in wet- of naar aanleiding van incidenten.	• Borg dat de procedure voor het beheer van privacy-incidenten en inbreuken minimaal eenmaal per jaar wordt geëvalueerd, en maak aantoonbaar dat deze periodieke beoordeling plaatsvindt (bijv. via evaluaties, reviews of auditrapportages). • 'Zorg dat de procedure wordt aangepast bij significante wijzigingen in systemen of processen, en toon aan dat deze aanpassingen worden vastgelegd en doorgevoerd. • 'Zorg dat de procedure wordt herzien naar aanleiding van ernstige incidenten, en maak aantoonbaar dat evaluaties en verbeteringen zijn uitgevoerd op basis van incidentanalyses. • 'Borg dat de actualiteit van de procedure structureel plaatsvindt en aansluit op de risico's en ontwikkelingen binnen het ZVH, en toon aan dat dit wordt geborgd via documentbeheer, versiening of besluitvorming.	Opzet • 'Stel vast dat de procedure minimaal jaarlijks wordt geëvalueerd, door het beoordelen van evaluaties, auditrapportages of reviews. • 'Stel vast dat aanpassingen worden gedaan bij wijzigingen in processen of systemen, door het beoordelen van gewijzigde werkinstructies en documentatie. • 'Stel vast dat evaluaties naar aanleiding van incidenten plaatsvinden, door het beoordelen van incidentanalyses en rapportages. Opzet • 'Stel vast dat de procedure is vastgesteld voor opleiding, bewustwording en kennisontwikkeling van procesgebruikers en ondersteunende staf. • 'Stel vast dat instructies of factbooks zijn opgesteld voor de toepasselijke wet- en regelgeving (WGS en BG) en de eisen ten aanzien van gegevensbescherming, doelbinding en proportionaliteit. Bestaan • 'Stel vast dat documentatie beschikbaar is waaruit blijkt welke trainingen procesgebruikers en ondersteunende staf hebben gevolgd. • 'Stel vast dat documentatie beschikbaar is waaruit blijkt dat de opleggers voorafgaand aan het casuïstisch zijn doorgelopen en dat een bevestiging is verkregen van de medewerkers van deelnemende partijen.	Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het bepalen en borgen van privacycompetenties van medewerkers, door het beoordelen van beleidsdocumenten, richtlijnen en competentieprofielen, waarbij is vastgelegd welke kennis en vaardigheden vereist zijn. Bestaan • 'Stel vast dat vereiste privacycompetenties zijn vastgelegd, door het beoordelen van beleid, richtlijnen en competentieprofielen. • 'Stel vast dat opleiding- en trainingsactiviteiten zijn ingericht, door het beoordelen van opleidingsplannen, e-learningmodules en documentatie. • 'Stel vast dat deelname en uitvoering van trainingen worden vastgelegd, door het beoordelen van opleidingsregistraties en evaluaties. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het vaststellen en beoordelen van privacycompetenties per medewerker (conform SCDO1), door het beoordelen van beleidsdocumenten, richtlijnen en werkinstructies. Bestaan • 'Stel vast dat per medewerker is vastgelegd in hoeverre deze beschikt over de vereiste privacycompetenties, door het beoordelen van HR-registraties, competentieprofielen of beoordelingen. • 'Stel vast dat een proces aanwezig is voor het identificeren en opspelen van lacunes in kennis en vaardigheden, door het beoordelen van beleid, werkinstructies en opleidingsplannen. • 'Stel vast dat privacycompetenties periodiek worden geëvalueerd, door het beoordelen van registraties, beoordelingen of audits. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het meten van privacycompetenties in werving, onboardng en beoordeling, door het beoordelen van beleidsdocumenten, werkinstructies en HR-richtlijnen, waarbij is vastgelegd dat privacy een onderdeel is van selectie en beoordeling. Bestaan • 'Stel vast dat de privacycompetenties zijn opgenomen in functiebeschrijvingen en selectiecriteria, door het beoordelen van HR-documentatie. • 'Stel vast dat onboardingsprogramma's aandacht besteden aan privacy, door het beoordelen van onboardingsdocumentatie en trainingsmateriaal. • 'Stel vast dat privacy onderdeel is van gesprekken en beoordelingen, door het beoordelen van gespreksverlagen, beoordelingsystemen en HR-registraties. Opzet • 'Stel vast dat beleid, procedures of werkinstructies zijn vastgesteld voor het waarborgen van de juistheid en volledigheid van persoonsgegevens. Bestaan • 'Stel vast dat registraties beschikbaar zijn van uitgevoerde correcties. • 'Stel vast dat documentatie aanwezig is waaruit blijkt hoe terugkoppeling naar gegevensleveranciers plaatsvindt. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het verzamelen, valideren en bijhouden van persoonsgegevens, door het beoordelen van beleidsdocumenten en werkinstructies, waarbij is vastgelegd hoe persoonsgegevens worden vastgesteld, gecontroleerd en geactualiseerd. Bestaan • 'Stel vast dat een proces aanwezig is voor het registreren en bijwerken van persoonsgegevens, door het beoordelen van werkinstructies en proceduredocumentatie. • 'Stel vast dat correcties en updates worden vastgelegd, door het beoordelen van registraties en casuïdissen. • 'Stel vast dat periodieke controles op juistheid en volledigheid plaatsvinden, door het beoordelen van controlelijsten en rapportages.	
P109	Competenties medewerkers	Wps artikel 1.8 i69 Bps artikel 1.17	De medewerkers van het Zorg- en Veiligheidshuis hebben de noodzakelijke competenties om dat zorgvuldig te doen. Waaronder kennis van de toepasselijke wet- en regelgeving (WGS en BG) en de eisen ten aanzien van gegevensbescherming, doelbinding en proportionaliteit.	De medewerkers van het Zorg- en Veiligheidshuis beschikken over de noodzakelijke kennis en vaardigheden en zorgvuldig met persoonsgegevens om te gaan, waaronder kennis van de toepasselijke wet- en regelgeving (WGS en BG) en de eisen ten aanzien van gegevensbescherming, doelbinding en proportionaliteit.	• Borg dat medewerkers van het ondersteunendebureau beschikken over de benodigde privacykennis en competenties (WGS/BG, AVG, doelbinding, proportionaliteit) passend bij hun rol (i.e. procesregisseur en ondersteunende staf). • 'Zorg dat medewerkers van deelnemende partijen voorafgaand aan deelname aan casuïstieken worden geïnformeerd over geldende spelregels en geheimhoudingsverreken, en toon aan dat dit aantoonbaar plaatsvindt via instructies, onboardingsmateriaal of vastgelegde bevestiging.	Opzet • 'Stel vast dat de procedure is vastgesteld voor opleiding, bewustwording en kennisontwikkeling van procesgebruikers en ondersteunende staf. • 'Stel vast dat instructies of factbooks zijn opgesteld voor de toepasselijke wet- en regelgeving (WGS en BG) en de eisen ten aanzien van gegevensbescherming, doelbinding en proportionaliteit. Bestaan • 'Stel vast dat documentatie beschikbaar is waaruit blijkt welke trainingen procesgebruikers en ondersteunende staf hebben gevolgd. • 'Stel vast dat documentatie beschikbaar is waaruit blijkt dat de opleggers voorafgaand aan het casuïstisch zijn doorgelopen en dat een bevestiging is verkregen van de medewerkers van deelnemende partijen.	Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het bepalen en borgen van privacycompetenties van medewerkers, door het beoordelen van beleidsdocumenten, richtlijnen en competentieprofielen, waarbij is vastgelegd welke kennis en vaardigheden vereist zijn. Bestaan • 'Stel vast dat vereiste privacycompetenties zijn vastgelegd, door het beoordelen van beleid, richtlijnen en competentieprofielen. • 'Stel vast dat opleiding- en trainingsactiviteiten zijn ingericht, door het beoordelen van opleidingsplannen, e-learningmodules en documentatie. • 'Stel vast dat deelname en uitvoering van trainingen worden vastgelegd, door het beoordelen van opleidingsregistraties en evaluaties. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het vaststellen en beoordelen van privacycompetenties per medewerker (conform SCDO1), door het beoordelen van beleidsdocumenten, richtlijnen en werkinstructies. Bestaan • 'Stel vast dat per medewerker is vastgelegd in hoeverre deze beschikt over de vereiste privacycompetenties, door het beoordelen van HR-registraties, competentieprofielen of beoordelingen. • 'Stel vast dat een proces aanwezig is voor het identificeren en opspelen van lacunes in kennis en vaardigheden, door het beoordelen van beleid, werkinstructies en opleidingsplannen. • 'Stel vast dat privacycompetenties periodiek worden geëvalueerd, door het beoordelen van registraties, beoordelingen of audits. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het meten van privacycompetenties in werving, onboardng en beoordeling, door het beoordelen van beleidsdocumenten, werkinstructies en HR-richtlijnen, waarbij is vastgelegd dat privacy een onderdeel is van selectie en beoordeling. Bestaan • 'Stel vast dat de privacycompetenties zijn opgenomen in functiebeschrijvingen en selectiecriteria, door het beoordelen van HR-documentatie. • 'Stel vast dat onboardingsprogramma's aandacht besteden aan privacy, door het beoordelen van onboardingsdocumentatie en trainingsmateriaal. • 'Stel vast dat privacy onderdeel is van gesprekken en beoordelingen, door het beoordelen van gespreksverlagen, beoordelingsystemen en HR-registraties. Opzet • 'Stel vast dat beleid, procedures of werkinstructies zijn vastgesteld voor het waarborgen van de juistheid en volledigheid van persoonsgegevens. Bestaan • 'Stel vast dat registraties beschikbaar zijn van uitgevoerde correcties. • 'Stel vast dat documentatie aanwezig is waaruit blijkt hoe terugkoppeling naar gegevensleveranciers plaatsvindt. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het verzamelen, valideren en bijhouden van persoonsgegevens, door het beoordelen van beleidsdocumenten en werkinstructies, waarbij is vastgelegd hoe persoonsgegevens worden vastgesteld, gecontroleerd en geactualiseerd. Bestaan • 'Stel vast dat een proces aanwezig is voor het registreren en bijwerken van persoonsgegevens, door het beoordelen van werkinstructies en proceduredocumentatie. • 'Stel vast dat correcties en updates worden vastgelegd, door het beoordelen van registraties en casuïdissen. • 'Stel vast dat periodieke controles op juistheid en volledigheid plaatsvinden, door het beoordelen van controlelijsten en rapportages.	
SCDO1	Competenties medewerkers	Wps artikel 1.8 i69 Bps artikel 1.17	Het Zorg- en Veiligheidshuis heeft de competenties gedocumenteerd van alle medewerkers die met persoonsgegevens werken. Het Zorg- en Veiligheidshuis legt daarnaast vast hoe deze competenties kunnen worden verworven (i.e. door trainingen).	Er is een beleid of er zijn richtlijnen vastgesteld waarin de vereiste privacycompetenties voor alle betrokken medewerkers (en zowel het Zorg- en Veiligheidshuis als de deelnemende organisaties) eenduidig zijn gedefinieerd.	• Borg dat de benodigde privacycompetenties van medewerkers die met persoonsgegevens werken zijn vastgesteld en eenduidig zijn gedefinieerd voor zowel het Zorg- en Veiligheidshuis als de deelnemende organisaties, en maak aantoonbaar dat deze zijn vastgesteld in beleid, richtlijnen of competentieprofielen. • 'Zorg dat is vastgelegd hoe medewerkers deze competenties verkrijgen en onderhouden (bijv. via training of e-learning), en toon aan dat dit wordt toegepast en periodiek wordt geëvalueerd via opleidingsregistraties, evaluaties of audits.	Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het bepalen en borgen van privacycompetenties van medewerkers, door het beoordelen van beleidsdocumenten, richtlijnen en competentieprofielen, waarbij is vastgelegd welke kennis en vaardigheden vereist zijn. Bestaan • 'Stel vast dat vereiste privacycompetenties zijn vastgelegd, door het beoordelen van beleid, richtlijnen en competentieprofielen. • 'Stel vast dat opleiding- en trainingsactiviteiten zijn ingericht, door het beoordelen van opleidingsplannen, e-learningmodules en documentatie. • 'Stel vast dat deelname en uitvoering van trainingen worden vastgelegd, door het beoordelen van opleidingsregistraties en evaluaties. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het vaststellen en beoordelen van privacycompetenties per medewerker (conform SCDO1), door het beoordelen van beleidsdocumenten, richtlijnen en werkinstructies. Bestaan • 'Stel vast dat per medewerker is vastgelegd in hoeverre deze beschikt over de vereiste privacycompetenties, door het beoordelen van HR-registraties, competentieprofielen of beoordelingen. • 'Stel vast dat een proces aanwezig is voor het identificeren en opspelen van lacunes in kennis en vaardigheden, door het beoordelen van beleid, werkinstructies en opleidingsplannen. • 'Stel vast dat privacycompetenties periodiek worden geëvalueerd, door het beoordelen van registraties, beoordelingen of audits. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het meten van privacycompetenties in werving, onboardng en beoordeling, door het beoordelen van beleidsdocumenten, werkinstructies en HR-richtlijnen, waarbij is vastgelegd dat privacy een onderdeel is van selectie en beoordeling. Bestaan • 'Stel vast dat de privacycompetenties zijn opgenomen in functiebeschrijvingen en selectiecriteria, door het beoordelen van HR-documentatie. • 'Stel vast dat onboardingsprogramma's aandacht besteden aan privacy, door het beoordelen van onboardingsdocumentatie en trainingsmateriaal. • 'Stel vast dat privacy onderdeel is van gesprekken en beoordelingen, door het beoordelen van gespreksverlagen, beoordelingsystemen en HR-registraties. Opzet • 'Stel vast dat beleid, procedures of werkinstructies zijn vastgesteld voor het waarborgen van de juistheid en volledigheid van persoonsgegevens. Bestaan • 'Stel vast dat registraties beschikbaar zijn van uitgevoerde correcties. • 'Stel vast dat documentatie aanwezig is waaruit blijkt hoe terugkoppeling naar gegevensleveranciers plaatsvindt. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het verzamelen, valideren en bijhouden van persoonsgegevens, door het beoordelen van beleidsdocumenten en werkinstructies, waarbij is vastgelegd hoe persoonsgegevens worden vastgesteld, gecontroleerd en geactualiseerd. Bestaan • 'Stel vast dat een proces aanwezig is voor het registreren en bijwerken van persoonsgegevens, door het beoordelen van werkinstructies en proceduredocumentatie. • 'Stel vast dat correcties en updates worden vastgelegd, door het beoordelen van registraties en casuïdissen. • 'Stel vast dat periodieke controles op juistheid en volledigheid plaatsvinden, door het beoordelen van controlelijsten en rapportages.		
SCDO2	Competenties medewerkers	Wps artikel 1.8 i69 Bps artikel 1.17	Het Zorg- en Veiligheidshuis documenteert in hoeverre individuele medewerkers die met persoonsgegevens werken over deze competenties beschikken en heeft een procedure opgesteld om lacunes in competenties en vaardigheden op te vullen.	Er is beleid of zijn richtlijnen vastgesteld waarin is vastgelegd dat medewerkers die met persoonsgegevens werken beschikken over de voorgeschreven competenties, zoals opgenomen in SCDO1.	• Borg dat medewerkers die met persoonsgegevens werkt wordt vastgesteld in hoeverre deze beschikt over de vereiste privacycompetenties, en maak aantoonbaar dat deze beoordeling is gedocumenteerd en dat er een proces is ingericht om eventuele lacunes in kennis en vaardigheden te identificeren en op te vullen. • 'Zorg dat het beleid of richtlijnen zijn vastgesteld waarin de vereiste privacycompetenties (zoals opgenomen in SCDO1) zijn gedefinieerd, en toon aan dat deze competenties worden toegepast en periodiek worden geëvalueerd via registraties, beoordelingen of audits.	Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het vaststellen en beoordelen van privacycompetenties per medewerker (conform SCDO1), door het beoordelen van beleidsdocumenten, richtlijnen en werkinstructies. Bestaan • 'Stel vast dat per medewerker is vastgelegd in hoeverre deze beschikt over de vereiste privacycompetenties, door het beoordelen van HR-registraties, competentieprofielen of beoordelingen. • 'Stel vast dat een proces aanwezig is voor het identificeren en opspelen van lacunes in kennis en vaardigheden, door het beoordelen van beleid, werkinstructies en opleidingsplannen. • 'Stel vast dat privacycompetenties periodiek worden geëvalueerd, door het beoordelen van registraties, beoordelingen of audits. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het meten van privacycompetenties in werving, onboardng en beoordeling, door het beoordelen van beleidsdocumenten, werkinstructies en HR-richtlijnen, waarbij is vastgelegd dat privacy een onderdeel is van selectie en beoordeling. Bestaan • 'Stel vast dat de privacycompetenties zijn opgenomen in functiebeschrijvingen en selectiecriteria, door het beoordelen van HR-documentatie. • 'Stel vast dat onboardingsprogramma's aandacht besteden aan privacy, door het beoordelen van onboardingsdocumentatie en trainingsmateriaal. • 'Stel vast dat privacy onderdeel is van gesprekken en beoordelingen, door het beoordelen van gespreksverlagen, beoordelingsystemen en HR-registraties. Opzet • 'Stel vast dat beleid, procedures of werkinstructies zijn vastgesteld voor het waarborgen van de juistheid en volledigheid van persoonsgegevens. Bestaan • 'Stel vast dat registraties beschikbaar zijn van uitgevoerde correcties. • 'Stel vast dat documentatie aanwezig is waaruit blijkt hoe terugkoppeling naar gegevensleveranciers plaatsvindt. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het verzamelen, valideren en bijhouden van persoonsgegevens, door het beoordelen van beleidsdocumenten en werkinstructies, waarbij is vastgelegd hoe persoonsgegevens worden vastgesteld, gecontroleerd en geactualiseerd. Bestaan • 'Stel vast dat een proces aanwezig is voor het registreren en bijwerken van persoonsgegevens, door het beoordelen van werkinstructies en proceduredocumentatie. • 'Stel vast dat correcties en updates worden vastgelegd, door het beoordelen van registraties en casuïdissen. • 'Stel vast dat periodieke controles op juistheid en volledigheid plaatsvinden, door het beoordelen van controlelijsten en rapportages.		
SCDO3	Competenties medewerkers	Wps artikel 1.8 i69 Bps artikel 1.17	Het Zorg- en Veiligheidshuis besteedt bij de werving en onboardng van nieuwe medewerkers die zullen werken met persoonsgegevens aandacht aan competenties met betrekking tot privacy. De omgang met persoonsgegevens is een van de punten in individuele beoordelingsgesprekken.	Deze norm vereist dat het Zorg- en Veiligheidshuis privacycompetenties structureel meeneemt in werving, onboardng en beoordeling, zodat medewerkers aantoonbaar zorgvuldig omgaan met persoonsgegevens.	• Borg dat privacycompetenties structureel worden meegenomen in werving en onboardng van medewerkers die met persoonsgegevens werken, en maak aantoonbaar dat dit is vastgelegd in functiebeschrijvingen, onboardingsprogramma's of selectiecriteria. • 'Zorg dat de omgang met persoonsgegevens onderdeel is van individuele gesprekken en beoordelingen, en toon aan dat dit wordt toegepast en vastgelegd via gespreksverlagen, beoordelingsystemen of HR-registraties.	Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het meten van privacycompetenties in werving, onboardng en beoordeling, door het beoordelen van beleidsdocumenten, werkinstructies en HR-richtlijnen, waarbij is vastgelegd dat privacy een onderdeel is van selectie en beoordeling. Bestaan • 'Stel vast dat de privacycompetenties zijn opgenomen in functiebeschrijvingen en selectiecriteria, door het beoordelen van HR-documentatie. • 'Stel vast dat onboardingsprogramma's aandacht besteden aan privacy, door het beoordelen van onboardingsdocumentatie en trainingsmateriaal. • 'Stel vast dat privacy onderdeel is van gesprekken en beoordelingen, door het beoordelen van gespreksverlagen, beoordelingsystemen en HR-registraties. Opzet • 'Stel vast dat beleid, procedures of werkinstructies zijn vastgesteld voor het waarborgen van de juistheid en volledigheid van persoonsgegevens. Bestaan • 'Stel vast dat registraties beschikbaar zijn van uitgevoerde correcties. • 'Stel vast dat documentatie aanwezig is waaruit blijkt hoe terugkoppeling naar gegevensleveranciers plaatsvindt. Opzet • 'Stel vast dat beleid, processen en procedures zijn ingericht voor het verzamelen, valideren en bijhouden van persoonsgegevens, door het beoordelen van beleidsdocumenten en werkinstructies, waarbij is vastgelegd hoe persoonsgegevens worden vastgesteld, gecontroleerd en geactualiseerd. Bestaan		

[illegible]

	Geautomatiseerde gegevensanalyse	Wps artikel 1.9 lid 2 t/m 6	Bij de DPA wordt vastgesteld: a. de aard van de geplande verwerkingen; b. hun doelstelling, noodzaak, en proportionaliteit; c. de risico's die beoogde verwerkingen met zich meebrengen voor rechten en vrijheden van betrokkenen; d. welke maatregelen moeten worden genomen om deze risico's te beperken.	Deze norm ziet op de inhoudelijke uitwerking van de DPA. Het samenwerkingverband zorgt dat de aard en doelstelling van de verwerking, de noodzaak en proportionaliteit, de risico's voor betrokkenen en de reële maatregelen worden vastgesteld en gedocumenteerd.	• Leg vast dat de in de WGS-control/beheersingsmaatregel opgenomen punten zijn uitgewerkt en onderbouwd in een DPA-document of DPA-registrier, indien sprake is van een verwerking met een hoog risico voor de rechten en vrijheden van betrokkenen. • Leg vast dat de uitgewerkte DPA minimaal de geïdentificeerde risico's, de impact op betrokkenen en de opgenomen mitigerende maatregelen bevat, en leg vast dat deze informatie is opgenomen in het DPA-document of DPA-registrier. • Leg vast dat passende maatregelen die volgen uit de DPA zijn vastgelegd in beleidsdocumentatie, projectdocumentatie of een maatregelregister, en leg vast dat deze maatregelen worden toegepast in de inrichting en uitvoering van de gegevensverwerking binnen het Zorg- en Veiligheidshuis.	Opzet • Het vast dat beleid, processen en procedures zijn ingericht voor het uitvoeren en documenteren van DPA's bij verwerkingen met een hoog privacyrisico, door het beoordelen van beleidsdocumenten en werkstructuur, waarbij is vastgelegd welke elementen in een DPA moeten worden opgenomen. Bestaan • Stel vast dat DPA-documenten of registraties aanwezig zijn, door het beoordelen van DPA-dossiers of een DPA-registrier. • Stel vast dat DPA's minimaal risico's, impact en mitigerende maatregelen bevatten, door het beoordelen van DPA-documentatie. • Stel vast dat maatregelen voortvloeien uit DPA's zijn vastgelegd, door het beoordelen van beleidsdocumentatie, projectdocumentatie of maatregelregitries. Opzet • Stel vast dat beleid, processen en procedures zijn ingericht voor het betrekken van relevante partijen bij DPA's, door het beoordelen van beleidsdocumenten en werkstructuur, waarbij is vastgelegd welke stakeholders worden geraadpleegd en welke beoordelingscriteria worden toegepast. Bestaan • Stel vast dat betrokken stakeholders zijn vastgelegd, door het beoordelen van DPA-documenten of een DPA-registrier. • Stel vast dat inbreng en adviezen van stakeholders zijn gedocumenteerd, door het beoordelen van DPA-documentatie en verslagen. • Stel vast dat beoordelingscriteria zijn toegepast en vastgelegd, door het beoordelen van DPA-documenten.	Werking Trek een steekproef uit uitvoerende DPA's en controleer of: a. risico's en impact volledig zijn beschreven; b. passende maatregelen zijn bepaald; c. maatregelen worden toegepast in de praktijk; d. opvolging en uitvoering aantoonbaar worden vastgelegd
PIA02	Geautomatiseerde gegevensanalyse	Wps artikel 1.9 lid 2 t/m 6	Alle relevante belanghebbenden zijn bij de DPA betrokken en de specifieke rechten van de toezichthoudende autoriteit ten aanzien van beoordelingscriteria worden nageliefd.	Deze norm ziet op het betrekken van relevante partijen bij de DPA. Het samenwerkingverband zorgt dat betrokken stakeholders worden geraadpleegd en dat wordt voldaan aan geldende beoordelingscriteria bij de uitvoering van de DPA.	• Leg vast dat bij de uitvoering van een DPA alle relevante belanghebbenden worden betrokken, en leg vast dat deze betrokkenheid is opgenomen in het DPA-document of DPA-registrier, via deelnemerslijsten, consultaties of vertegenwoordigers. • Leg vast dat relevante stakeholders (zoals deelnemers, deskundigen of betrokken partijen) worden geraadpleegd en leg vast dat hun inbreng en adviezen zijn gedocumenteerd en terug te vinden zijn in de DPA-documentatie. • Leg vast dat de geldende beoordelingscriteria (incl. verzetten van de toezichthoudende autoriteit) worden toegepast bij de DPA, en leg vast dat deze expliciet zijn opgenomen en onderbouwd in het DPA-document of DPA-registrier. • Leg vast dat de uitvoering van de DPA controleerbaar en herleidbaar is, en leg vast dat de besluitvorming en afwegingen zijn vastgelegd in DPA-documentatie en aanvullende dossierstukken (bijv. beleidsdocumentatie of projectdossiers).	Bestaan • Leg vast dat een overzicht bestaat van alle systemen en toepassingen waarin persoonsgegevens worden verwerkt, en leg vast dat dit overzicht is opgenomen in het verwerkingsregister of een applicatie- en gegevensverwerkingsdocument. • Leg vast dat wijzigingen in systemen en verwerkingen worden geregistreerd, en leg vast dat deze wijzigingen zijn opgenomen in wijzigingsdocumentatie, change-log of updates van het verwerkingsregister. • Leg vast dat dit overzicht minimaal jaarlijks wordt beoordeeld op juistheid en volledigheid, en leg vast dat deze beoordeling is vastgelegd in een reviewdocument, auditrapport of wijzigingshistorie. • Leg vast dat het overzicht van systemen en verwerkingen wordt gebruikt voor sturing en controle op gegevensverwerking, en leg vast dat dit aantoonbaar is verwerkt in beheerprocessen, rapportages of beleidsdocumentatie. Opzet • Stel vast dat beleid, processen en procedures zijn ingericht voor het inzichtelijk maken van systemen en applicaties waarin persoonsgegevens worden verwerkt, door het beoordelen van beleidsdocumenten en werkstructuur, waarbij is vastgelegd dat systemen en wijzigingen daarin worden geregistreerd. Bestaan • Stel vast dat een overzicht aanwezig is van systemen en applicaties waarin persoonsgegevens worden verwerkt, door het beoordelen van registraties of documentatie. • Stel vast dat wijzigingen in systemen worden vastgelegd, door het beoordelen van wijzigingsdocumentatie en registraties. • Stel vast dat het overzicht periodiek wordt bijgewerkt, door het beoordelen van versies en actualisatiedata. Opzet • Stel vast dat beleid, processen en procedures zijn ingericht voor het inzichtelijk maken van systemen en applicaties waarin persoonsgegevens worden verwerkt, door het beoordelen van beleidsdocumenten en werkstructuur, waarbij is vastgelegd dat systemen en wijzigingen daarin worden geregistreerd. Bestaan • Stel vast dat een overzicht aanwezig is van systemen en applicaties waarin persoonsgegevens worden verwerkt, door het beoordelen van registraties of documentatie. • Stel vast dat wijzigingen in systemen worden vastgelegd, door het beoordelen van wijzigingsdocumentatie en registraties. • Stel vast dat het overzicht periodiek wordt bijgewerkt, door het beoordelen van versies en actualisatiedata.	Werking • Trek een steekproef uit registraties en controleer: a. of systemen waarin persoonsgegevens worden verwerkt volledig zijn opgenomen; b. of wijzigingen tijdig en correct worden vastgelegd; c. of het overzicht aansluit op de feitelijke situatie (bijv. vergelijking met systeem of processen); d. of actualisaties aantoonbaar worden uitgevoerd en vastgelegd.
PIA04	Geautomatiseerde gegevensanalyse	Wps artikel 1.9 lid 2 t/m 6	Het Zorg- en Veiligheidshuis documenteert welke systemen en software persoonsgegevens verwerken en houdt bij welke wijzigingen hierin zijn gepland en worden doorgevoerd.	Deze norm ziet op het inzichtelijk maken van gegevensverwerkingen. Het samenwerkingverband zorgt dat wordt vastgelegd welke systemen en toepassingen persoonsgegevens verwerken en dat wijzigingen hierin worden bijgehouden.	• Leg vast dat een overzicht bestaat van alle systemen en toepassingen waarin persoonsgegevens worden verwerkt, en leg vast dat dit overzicht is opgenomen in het verwerkingsregister of een applicatie- en gegevensverwerkingsdocument. • Leg vast dat wijzigingen in systemen en verwerkingen worden geregistreerd, en leg vast dat deze wijzigingen zijn opgenomen in wijzigingsdocumentatie, change-log of updates van het verwerkingsregister. • Leg vast dat dit overzicht minimaal jaarlijks wordt beoordeeld op juistheid en volledigheid, en leg vast dat deze beoordeling is vastgelegd in een reviewdocument, auditrapport of wijzigingshistorie. • Leg vast dat het overzicht van systemen en verwerkingen wordt gebruikt voor sturing en controle op gegevensverwerking, en leg vast dat dit aantoonbaar is verwerkt in beheerprocessen, rapportages of beleidsdocumentatie.	Opzet • Stel vast dat beleid, processen en procedures zijn ingericht voor het inzichtelijk maken van systemen en applicaties waarin persoonsgegevens worden verwerkt, door het beoordelen van beleidsdocumenten en werkstructuur, waarbij is vastgelegd dat systemen en wijzigingen daarin worden geregistreerd. Bestaan • Stel vast dat een overzicht aanwezig is van systemen en applicaties waarin persoonsgegevens worden verwerkt, door het beoordelen van registraties of documentatie. • Stel vast dat wijzigingen in systemen worden vastgelegd, door het beoordelen van wijzigingsdocumentatie en registraties. • Stel vast dat het overzicht periodiek wordt bijgewerkt, door het beoordelen van versies en actualisatiedata. Opzet • Stel vast dat beleid, processen en procedures zijn ingericht voor het inzichtelijk maken van systemen en applicaties waarin persoonsgegevens worden verwerkt, door het beoordelen van beleidsdocumenten en werkstructuur, waarbij is vastgelegd dat systemen en wijzigingen daarin worden geregistreerd. Bestaan • Stel vast dat een overzicht aanwezig is van systemen en applicaties waarin persoonsgegevens worden verwerkt, door het beoordelen van registraties of documentatie. • Stel vast dat wijzigingen in systemen worden vastgelegd, door het beoordelen van wijzigingsdocumentatie en registraties. • Stel vast dat het overzicht periodiek wordt bijgewerkt, door het beoordelen van versies en actualisatiedata.	Werking • Trek een steekproef uit uitvoerende DPA's en controleer of: a. de systemen waarin persoonsgegevens worden verwerkt volledig zijn opgenomen; b. of wijzigingen tijdig en correct worden vastgelegd; c. of het overzicht aansluit op de feitelijke situatie (bijv. vergelijking met systeem of processen); d. of actualisaties aantoonbaar worden uitgevoerd en vastgelegd.
PIA05	Geautomatiseerde gegevensanalyse	Wps artikel 1.9 lid 2 t/m 6	Een verandermanagementproces is vastgesteld om ervoor zorg te dragen dat de in de DPA vastgestelde privacymaatregelen in de beoogde nieuwe of gewijzigde processen (producten/diensten worden geïmplementeerd. DPA's worden periodiek herhaald.	Deze norm ziet op het borgen van opvolging van DPA-maatregelen. Het samenwerkingverband zorgt dat vastgestelde maatregelen worden geïmplementeerd via een wijzigingsproces en dat DPA's periodiek worden herzien bij relevante wijzigingen	• Leg vast dat DPA-maatregelen worden geïmplementeerd via een ingericht verandermanagementproces(change management proces), en maak aantoonbaar dat wijzigingen in processen, producten of systemen worden vastgelegd en doorgevoerd. • Leg vast dat DPA's periodiek worden herzien bij relevante wijzigingen, en leg vast dat deze herzieningen en de aanleiding daarvoor zijn opgenomen in het DPA-document of DPA-registrier. • Leg vast dat de opvolging van DPA-maatregelen wordt gemonteerd en vastgelegd, en leg vast dat de voortgang en implementatie van deze maatregelen inzichtelijk zijn via een activiteits-, maatregelregister of voortgangsrapportage.	Opzet • Stel vast dat DPA-maatregelen worden geïmplementeerd via een ingericht verandermanagementproces(change management proces), en maak aantoonbaar dat wijzigingen in processen, producten of systemen worden vastgelegd en doorgevoerd. • Leg vast dat DPA's periodiek worden herzien bij relevante wijzigingen, en leg vast dat deze herzieningen en de aanleiding daarvoor zijn opgenomen in het DPA-document of DPA-registrier. • Leg vast dat de opvolging van DPA-maatregelen wordt gemonteerd en vastgelegd, en leg vast dat de voortgang en implementatie van deze maatregelen inzichtelijk zijn via een activiteits-, maatregelregister of voortgangsrapportage. Bestaan • Stel vast dat DPA-maatregelen worden geïmplementeerd via een ingericht wijzigingsproces, door het beoordelen van projectdocumentatie, wijzigingsregistraties en maatregelregitries. • Stel vast dat DPA's periodiek worden herzien, door het beoordelen van DPA-documenten en registraties, waarbij wordt vastgesteld dat aanleiding en herzieningen zijn vastgelegd. • Stel vast dat voortgang en implementatie van maatregelen inzichtelijk zijn, door het beoordelen van activiteiten-, maatregelregitries of voortgangsrapportages. Opzet • Stel vast dat beleid en/of richtlijnen expliciet beschrijven dat geen gebruik wordt gemaakt van geautomatiseerde gegevensanalyses binnen het ZVH. Bestaan • Indien hiervan geen sprake is, wordt dit vastgesteld en gedocumenteerd. • Stel vast dat dit uitgangspunt is opgenomen in relevante documentatie (bijv. verwerkingsregister, DPA's of beleid). Opzet • Stel vast dat beleid, processen en procedures zijn ingericht voor het functioneren van de rechtmatigheidscommissie (RAC) en de toetsing van (nieuwe of gewijzigde) gegevensverwerkingen, door het beoordelen van beleidsdocumenten, werkstructuur en procedurebeschrijvingen, waarbij is opgenomen dat toetsing voorafgaand aan uitvoering plaatsvindt en wordt vastgelegd. Bestaan • Stel vast dat (nieuwe of gewijzigde) gegevensverwerkingen aantoonbaar voorafgaand zijn beoordeeld door de RAC, door het beoordelen van adviesaanvragen, registraties en/of dossierstukken, waarbij wordt vastgesteld dat deze toetsing per verwerking is vastgelegd. • Stel vast dat adviezen van de RAC worden betrokken in de besluitvorming, door het beoordelen van besluitvormingsdocumentatie (bijv. notulen of adviezen), waarbij wordt vastgesteld dat afwijkingen van adviezen expliciet en gemonteerd zijn vastgelegd. • Stel vast dat de toetsing per afzonderlijke verwerking plaatsvindt en herleidbaar is in de dossiervorming, door het beoordelen van registraties.	Werking • Trek een steekproef uit uitvoerende DPA's en controleer of: a. maatregelen daadwerkelijk worden geïmplementeerd; b. wijzigingen worden doorgevoerd en vastgelegd; c. DPA's periodiek worden herzien; d. voortgang en opvolging aantoonbaar worden gemonteerd. Werking • Voer een steekproef uit op het verwerkingsregister, DPA's en procedurebeschrijvingen en stel vast: a. of geautomatiseerde gegevensanalyse plaatsvindt; b. indien geen sprake is van geautomatiseerde gegevensanalyse, leg deze non-occurrence vast; c. indien wel sprake is van geautomatiseerde gegevensanalyse, stel vast dat wordt voldaan aan de wettelijke vereisen en dat de benodigde beheersmaatregelen zijn ingericht
PIA06	Geautomatiseerde gegevensanalyse	Wps artikel 1.9 lid 2 t/m 6	Geautomatiseerde analyses worden uitdrukkelijk toegestaan voor vooraf vastgestelde doelen en met gebruik van toegestane gegevenscategorieën. De substanten van deze analyses worden niet zonder menselijke beoordeling gebruikt en zijn niet direct leidend voor besluitvorming. Het gebruik en de werking van geautomatiseerde analyses worden periodiek gemonteerd en geëvalueerd.	Voor het Zorg- en Veiligheidshuis is geen expliciete wettelijke grondslag opgenomen in de WGS of het RGVS voor het gebruik van geautomatiseerde gegevensanalyse. Aangezien dergelijke verwerking alleen is toegestaan voor zover deze expliciet is gereguleerd, wordt ervan uitgegaan dat dit geen onderdeel vormt van de reguliere gegevensverwerking binnen het ZVH.	• Stel vast dat wordt beoordeeld of binnen het ZVH sprake is van geautomatiseerde gegevensanalyse (zoals bedoeld in de WGS), en leg vast dat indien dit niet van toepassing is. • Stel per inspectie van het verwerkingsregister of de DPA vast dat geen sprake is van geautomatiseerde gegevensanalyse.	Opzet • Stel vast dat beleid en/of richtlijnen expliciet beschrijven dat geen gebruik wordt gemaakt van geautomatiseerde gegevensanalyses binnen het ZVH. Bestaan • Indien hiervan geen sprake is, wordt dit vastgesteld en gedocumenteerd. • Stel vast dat dit uitgangspunt is opgenomen in relevante documentatie (bijv. verwerkingsregister, DPA's of beleid). Opzet • Stel vast dat beleid, processen en procedures zijn ingericht voor het functioneren van de rechtmatigheidscommissie (RAC) en de toetsing van (nieuwe of gewijzigde) gegevensverwerkingen, door het beoordelen van beleidsdocumenten, werkstructuur en procedurebeschrijvingen, waarbij is opgenomen dat toetsing voorafgaand aan uitvoering plaatsvindt en wordt vastgelegd. Bestaan • Stel vast dat (nieuwe of gewijzigde) gegevensverwerkingen aantoonbaar voorafgaand zijn beoordeeld door de RAC, door het beoordelen van adviesaanvragen, registraties en/of dossierstukken, waarbij wordt vastgesteld dat deze toetsing per verwerking is vastgelegd. • Stel vast dat adviezen van de RAC worden betrokken in de besluitvorming, door het beoordelen van besluitvormingsdocumentatie (bijv. notulen of adviezen), waarbij wordt vastgesteld dat afwijkingen van adviezen expliciet en gemonteerd zijn vastgelegd. • Stel vast dat de toetsing per afzonderlijke verwerking plaatsvindt en herleidbaar is in de dossiervorming, door het beoordelen van registraties.	Werking • Voer een steekproef uit op verwerkingen en stel vast dat: a. toetsing door de RAC daadwerkelijk voorafgaand aan de verwerking heeft plaatsgevonden; b. RAC-adviezen aantoonbaar zijn meegenomen in de besluitvorming; c. afwijkingen van RAC-adviezen expliciet en gemonteerd zijn vastgelegd in het dossier; d. de toetsing en besluitvorming per verwerking volledig en herleidbaar zijn gedocumenteerd.
Wps-16	Management en monitoring	Wps artikel 1.8 lid 6 Wps artikel 2.26 Wps artikel 2.3 lid 9 en 10 Bp. artikel 1.13 lid 1 t/m 6 Bp. artikel 1.14 lid 1 t/m 5 Bp. artikel 1.15 lid 1 en 2 Bp. artikel 2.17 lid 1 t/m 3	Een onafhankelijke rechtmatigheidscommissie beoordeelt structureel ne een en gewijzigde verwerkingen voortgaand aan de uitvoering daarvan en adviseert over corrigerende maatregelen. De uitkomsten van de beoordeling leiden tot een advies over de toelaatbaarheid van de verwerking, waarbij de afwegingen en adviezen worden vastgelegd en herleidbaar zijn. Deze toetsing vindt plaats per afzonderlijke verwerking of causus.	Het Zorg- en Veiligheidshuis borgt dat een rechtmatigheidscommissie is ingericht en functioneert conform de wettelijke vereisten, inclusief een aantoonbaar vastgelegde samenstelling, werkwijze en bevoegdheden. De rechtmatigheidscommissie brengt onafhankelijk, aantoonbaar en zorgvuldig tot stand gekomen adviezen uit over de rechtmatigheid en noodzakelijkheid van nieuwe en gewijzigde gegevensverwerkingen binnen het Zorg- en Veiligheidshuis. Deelnemers borgen dat deze adviezen worden betrokken bij de besluitvorming en dat afwijkingen van een rechtmatigheidscommissie-advies uitdrukkelijk gemonteerd, transparant en aantoonbaar worden vastgelegd, gedocumenteerd in het besluitvormingsdossier en gerapporteerd aan de rechtmatigheidscommissie en de coördinerend functionaris voor gegevensbescherming.	• Zorg dat in beleid en procedures is vastgelegd in welke gevallen een voorafgaande rechtmatigheidstoets door de RAC vereist is (bijv. bij verstrekking aan derden), en maak aantoonbaar dat deze toetsing in de grotere plaatsvindt (bijv. via adviesaanvragen). • Borg dat adviezen van de RAC worden betrokken in de besluitvorming, en dat eventuele afwijkingen gemonteerd en aantoonbaar worden vastgelegd. • Zorg dat deze toetsing plaatsvindt per relevante verwerking, en toon aan dat dit zichtbaar is in de registratie of dossiervorming.	Opzet • Stel vast dat beleid, processen en procedures zijn ingericht voor het functioneren van de rechtmatigheidscommissie (RAC) en de toetsing van (nieuwe of gewijzigde) gegevensverwerkingen, door het beoordelen van beleidsdocumenten, werkstructuur en procedurebeschrijvingen, waarbij is opgenomen dat toetsing voorafgaand aan uitvoering plaatsvindt en wordt vastgelegd. Bestaan • Stel vast dat (nieuwe of gewijzigde) gegevensverwerkingen aantoonbaar voorafgaand zijn beoordeeld door de RAC, door het beoordelen van adviesaanvragen, registraties en/of dossierstukken, waarbij wordt vastgesteld dat deze toetsing per verwerking is vastgelegd. • Stel vast dat adviezen van de RAC worden betrokken in de besluitvorming, door het beoordelen van besluitvormingsdocumentatie (bijv. notulen of adviezen), waarbij wordt vastgesteld dat afwijkingen van adviezen expliciet en gemonteerd zijn vastgelegd. • Stel vast dat de toetsing per afzonderlijke verwerking plaatsvindt en herleidbaar is in de dossiervorming, door het beoordelen van registraties.	Werking • Voer een steekproef uit op verwerkingen en stel vast dat: a. toetsing door de RAC daadwerkelijk voorafgaand aan de verwerking heeft plaatsgevonden; b. RAC-adviezen aantoonbaar zijn meegenomen in de besluitvorming; c. afwijkingen van RAC-adviezen expliciet en gemonteerd zijn vastgelegd in het dossier; d. de toetsing en besluitvorming per verwerking volledig en herleidbaar zijn gedocumenteerd.
Wps-17	Rechtmatigheidstoets & governance	Wps artikel 2.31 lid 1 en lid 2 Wps artikel 2.31 lid 6, 12 en 13 Wps artikel 2.32 lid 2, lid 3 en lid 5 Bp. artikel 2.20 Bp. artikel 2.22	Er is een proces ingericht om: a. gebeurtenissen en factoren te identificeren die het behalen van de privacydoelstellingen in gevaar brengen; b. de gevolgen van deze gebeurtenissen en factoren en de kans dat zij plaatsvinden te beoordelen, en vervolgens een passende risicoscoren en beheersingsmaatregelen te formuleren. Wanneer nieuwe of gewijzigde privacyrisico's worden geïdentificeerd, worden de privacyrisicobeoordeling en de risicobeheersstrategieën herzien en zo nodig bijgewerkt. Het management heeft acceptatiecriteria voor privacyrisico's vastgesteld, pedgekeurd, gedocumenteerd en past deze toe.	Deze norm ziet op het agenderen en periodiek bespreken van privacyrisico's binnen het Zorg- en Veiligheidshuis. Het Zorg- en Veiligheidshuis borgt dat de stuurgroep minimaal jaarlijks privacy als vast onderwerp bespreekt, waarbij actuele en toekomstige risico's worden geïdentificeerd en beoordeeld. Significante privacyrisico's, auditbevindingen, datalekken en overige relevante ontwikkelingen op het gebied van privacy worden gemonteerd door de FG en, indien de aard of impact daartoe aanleiding geeft, bespreken binnen de stuurgroep of een andere daarvoor aangewezen governance-structuur. Besluiten over risicoacceptatie, prioritering en opvolging worden bestuurlijk vastgelegd.	• Borg dat de stuurgroep minimaal eenmaal per jaar het onderwerp privacy op de agenda zet en maak aantoonbaar dat actuele en toekomstige privacyrisico's (bijv. inzet van AI, data-oververeinstelt en capaciteitsuitdagingen) worden besproken, bijvoorbeeld via agenda's en notulen van de stuurgroep. • Zorg dat geïdentificeerde privacyrisico's worden samengevat en opgenomen in bestuurlijke rapportages, en toon aan dat deze zijn vastgelegd en gedeeld, bijvoorbeeld via een jaarverslag of managementrapportage. • Waarborg dat deze risico's en aandachtspunten worden betrokken bij de verdere sturing en prioritering binnen het Zorg- en Veiligheidshuis, en maak aantoonbaar dat opvolging plaatsvindt via acceptatiepunten, besluitvorming of voortgangsrapportages.	Opzet • Stel vast dat beleid, processen en procedures zijn ingericht voor het periodiek bespreken van privacyrisico's binnen het Zorg- en Veiligheidshuis, door het beoordelen van beleidsdocumenten, werkstructuur en governance-afspraken, waarbij is vastgelegd dat privacyrisico's minimaal jaarlijks door de stuurgroep worden geagenderd en beoordeeld. Bestaan • Stel vast dat privacyrisico's periodiek worden besproken in de stuurgroep, door het beoordelen van agenda's en notulen, waarbij wordt vastgesteld dat actuele en toekomstige risico's (bijv. AI, datadeling, capaciteitsuitdagingen) zijn opgenomen. • Stel vast dat geïdentificeerde privacyrisico's worden samengevat en opgenomen in bestuurlijke rapportages, door het beoordelen van managementrapportages en/of het jaarverslag, waarbij wordt vastgesteld dat deze risico's zijn vastgelegd en gedeeld. • Stel vast dat privacyrisico's worden betrokken bij sturing en prioritering binnen het Zorg- en Veiligheidshuis, door het beoordelen van besluitvorming, acceptatiepunten en voortgangsrapportages, waarbij wordt vastgesteld dat opvolging aantoonbaar is vastgelegd.	Werking • Voer een steekproef uit op agenda's, notulen en bestuurlijke rapportages en stel vast dat: a. privacyrisico's periodiek (minimaal) jaarlijks worden geagenderd en besproken in de stuurgroep; b. actuele en toekomstige risico's inhoudelijk worden benoemd en beoordeeld; c. geïdentificeerde risico's aantoonbaar zijn vastgelegd en terugkomen in rapportages (bijv. jaarverslag of managementrapportage); d. op basis van deze risico's besluiten, prioritering en opvolging aantoonbaar zijn vastgelegd (bijv. in acceptatiepunten of voortgangsrapportages).
RIA04	Rechtmatigheidstoets & governance						