Riwis ZORG & WELZIJN Geloof in eigen kunnen

Verklaring van Verantwoording 2020

Gegevensbescherming & informatiebeveiliging

Verantwoording van Riwis Zorg & Welzijn aan betrokkenen over het voldoen aan wet- en regelgeving op het gebied van privacy, gegevensbescherming & informatiebeveiliging

Auteur: Kristian Kramer
Datum: april 2021
Status: definitief
Versie: 1.0

Privacy heb je zelf in de hand

Inhoudsopgave

Inleiding

Stichting Riwis Zorg & Welzijn is als zorginstelling verantwoordelijk voor cliëntenzorg en goed werkgeverschap. Het leveren van kwaliteit staat bij het verlenen van zorg voorop. Om kwaliteit aan onze cliënten, medewerkers en andere betrokkenen te kunnen bieden is een betrouwbare informatievoorziening heel belangrijk. Deze informatievoorziening moet goed beheerd worden met uitgebreide aandacht voor de beveiliging van de opslag, het verwerken en het delen van informatie. Dit vereist continue alertheid, want de informatie en de systemen moeten tijdig beschikbaar, juist, volledig en veilig zijn.

Riwis vindt het vanzelfsprekend en van groot belang dat de organisatie (lees: de medewerkers) goed omgaat met persoonsgegevens. Daarbij gaan wij ervan uit dat we met persoonsgegevens van een ander omgaan zoals iedereen wenst dat er met zijn/haar eigen persoonsgegevens wordt omgegaan. Onze medewerkers hebben een hoog privacybewustzijn nodig. Bij het maken van keuzes heeft Riwis de volgende uitgangspunten:

- Privacy en gegevensbescherming mag de zorg niet in de weg staan.
- Er moet evenwicht zijn tussen gebruikersgemak en gegevensbescherming.
- Uitgangspunt is vertrouwen in de professionaliteit van de medewerker en controle hierop.
- Zorgvuldigheid staat voorop, al is het volledig uitsluiten van datalekken niet mogelijk.

Hoe organisaties moeten omgaan met (persoons)gegevens is in wet- en regelgeving geregeld. Wetswijzigingen en nieuwe wetten op het gebied van privacy en informatiebeveiliging volgen elkaar in hoog tempo op. Kernbegrippen in deze wetten, vooral de AVG, zijn *Accountability* en *Auditability*.

Accountability en Auditability

De Algemene Verordening Gegevensbescherming (AVG) vereist van Riwis dat zij goed nadenkt over hoe persoonsgegevens worden verwerkt en beschermd. De verantwoordingsplicht (***accountability***) houdt in dat Riwis moet kunnen *aantonen* dat de verwerking van persoonsgegevens aan de regels van de AVG voldoet. Dit aantonen doet Riwis door het bijhouden van een privacy- & informatiebeveiligingsadministratie. In deze administratie wordt overzicht en inzicht gegeven in de verantwoordelijkheid en aansprakelijkheid van Riwis en de verbonden partijen (verwerkers en mede-verwerkingsverantwoordelijken) waarmee gegevens worden uitgewisseld. Daarnaast wordt overzicht en inzicht gegeven in de verwerkingen van persoonsgegevens, de bijbehorende processen en de informatiesystemen die de verwerkingen uitvoeren. Riwis moet passende technische en organisatorische maatregelen nemen om de gegevens te beschermen[1]. Door het bijhouden van de privacyadministratie is Riwis ***auditable*** (controleerbaar). Met de administratie documenteren we aantoonbaar wat we deden, doen en gaan doen.
In de Governancecode Zorg staat dat de raad van bestuur verantwoording aflegt over het behalen van doelstellingen van de eigen zorgorganisatie en het gevoerde beleid ten aanzien van de belanghebbenden. De organisatie moet transparant zijn in haar handelen en de gemaakte keuzes om daar vervolgens verantwoording over af te leggen aan belanghebbenden.

Verklaring van Verantwoording

In deze Verklaring van Verantwoording wordt aan alle belanghebbenden verantwoording afgelegd over de naleving van verplichtingen vanuit wetgeving op het gebied van privacy, gegevensbescherming en informatiebeveiliging. Met deze verklaring geeft de organisatie aan hoe ze *in control* is en hoe ze de verplichtingen vanuit wetgeving naleeft. Dit gebeurt op basis van alles dat is gedocumenteerd in de privacy- & informatiebeveiligingsadministratie en bijbehorende controles. Hiermee wordt een totaalbeeld van *accountability* gegeven.
Deze Verklaring van Verantwoording is een aanvulling op de governance paragraaf in het jaarlijkse bestuursverslag. Deze verklaring is bestemd voor belanghebbenden zoals cliënten, medewerkers, leveranciers, financiers en andere geïnteresseerden. De controle (op aspecten) van privacy en informatiebeveiliging is onderdeel van de accountantscontrole op de jaarrekening. De accountant kan de uitkomsten van deze verklaring meenemen in het vaststellen van zijn controleverklaring.

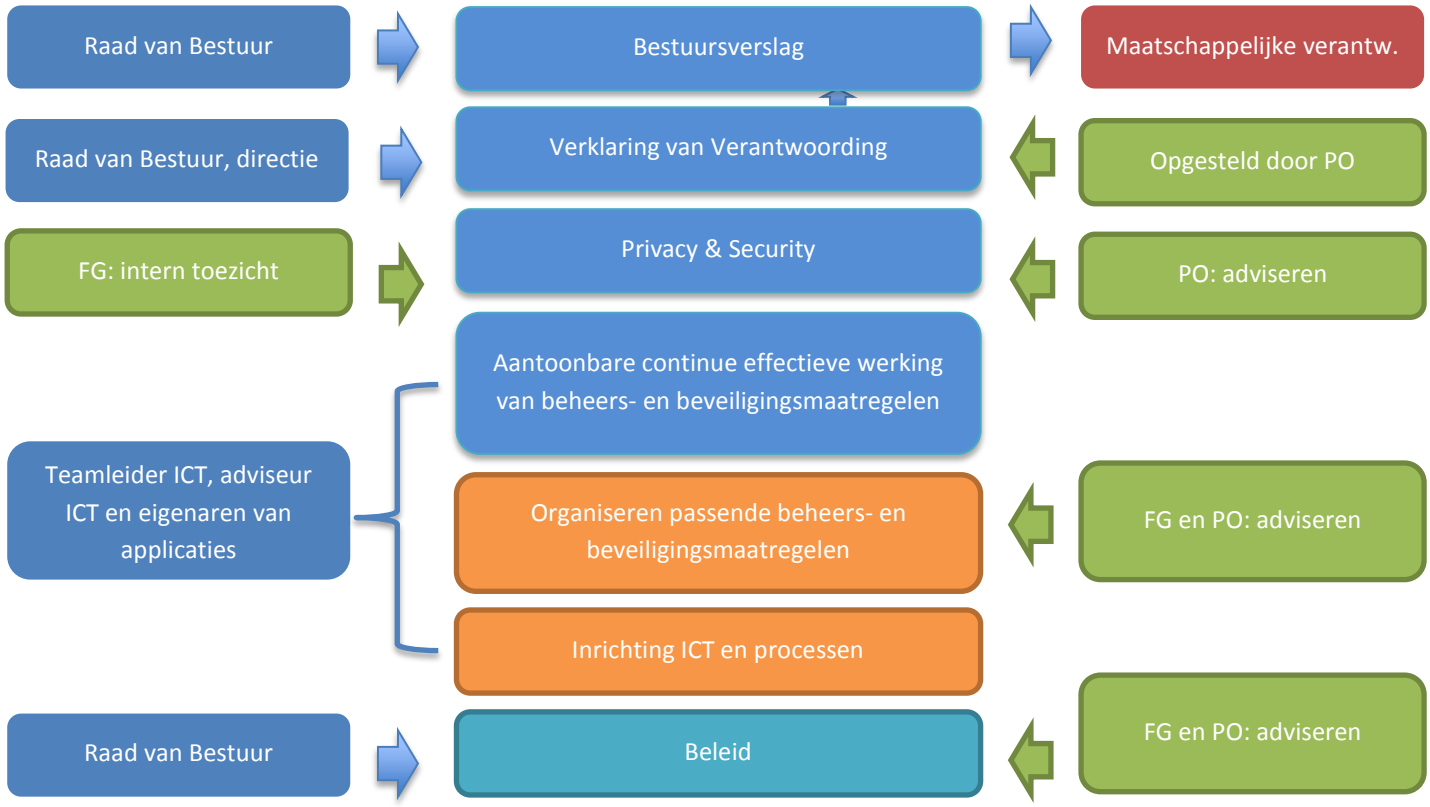
Op de website van Riwis is informatie opgenomen over privacy en informatiebeveiliging: een verkorte privacyverklaring, de Verklaring van Verantwoording en de contactgegevens van de privacyfunctionarissen.

[1] AVG artikel 24.

Governance & compliance

Privacy en informatiebeveiliging zijn onderdeel van de governance & compliance van Riwis. Binnen privacy en gegevensverwerking zijn er diverse rollen te onderscheiden. De Functionaris voor Gegevensbescherming (FG) ziet toe op de naleving van de AVG, aanpalende wetgeving en het privacybeleid van Riwis. De AVG schrijft diverse taken voor die de FG toebedeeld krijgt[2], deze zijn dan ook bij hem belegd. Hierbij moet gedacht worden aan adviseren en informeren van verwerkingsverantwoordelijke over de verplichtingen van de AVG, toezicht op naleving van de AVG en beleid, advies geven over DPIA's en voorkomende gevallen samenwerken met de Autoriteit Persoonsgegevens. Ook audits in verband met gegevensverwerking behoren tot de taken van de FG bij Riwis, dit in samenwerking met de Privacy officer (PO).

De eigenaren van de applicaties[3] en de manager bedrijfsondersteuning (die o.a. leiding geeft aan de afdeling ICT) zijn verantwoordelijk voor de coördinatie van de informatiebeveiliging. Hier ligt de verantwoordelijkheid voor het aantonen van de continue effectieve werking van de technische en organisatorische maatregelen[4] die Riwis neemt om te kunnen waarborgen en aantonen dat (persoons)gegevens in overeenstemming met de AVG worden verwerkt. Bijvoorbeeld door het vaststellen van beleid, het nemen van beveiligingsmaatregelen van applicaties, de inrichting van ICT en daar aan gerelateerde processen. De FG en PO hebben hier voornamelijk een adviserende rol.



[2] AVG artikel 39 – Taken (functionaris voor gegevensbescherming)
[3] Meestal de managers van het betreffende bedrijfsonderdeelfunctioneel.
[4] Zoals onder andere bedoeld in AVG artikel 24.

Mededeling Raad van Bestuur

Na goede stappen op het gebied van privacy en informatiebeveiliging in 2019, is ook 2020 een jaar geweest waarin Riwis goede vooruitgang heeft gemaakt op dit gebied. Het kan niet anders dan dat we ook hier de coronacrisis moeten noemen. Deze crisis bemoeilijkte bijvoorbeeld de bewustwording rondom privacy omdat locaties niet bezocht konden worden. Ook maakte de coronacrisis en het bijbehorende thuiswerken, dat er op het gebied van informatiebeveiliging de nodige uitdagingen waren. Het is goed om te zien hoe Riwis snel kon schakelen en thuiswerken eigenlijk vanaf dag 1 goed heeft gewerkt. Het beeldbellen en thuiswerken is ondertussen de gewoonste zaak van de wereld en dankzij inspanningen van ICT en privacyteam gebeurt dit ook veilig. Het kost wel tijd om te wennen aan nieuwe apps en de verdere implementatie is nog *ongoing*, zeker waar het gaat om contact met cliënten via een videoverbinding. Cliënten hebben, door corona, ook opeens nieuwe technologie moeten gebruiken. In veel gevallen ging dat goed, al was het soms wel even wennen. Eigenlijk net als bij onze medewerkers. Ondertussen horen beeldbellen en video-vergaderen bij de communicatiemiddelen die wij dagelijks gebruiken. In 2021 zijn sommige zaken natuurlijk wel gewoon verder gegaan. Zo zijn er beleidsstukken op het gebied van privacy & informatiebeveiliging opgesteld, is aan het bewustzijn gewerkt (op afstand) en is de privacyadministratie verder op orde gebracht.

De medewerkers van Riwis Zorg & Welzijn verwerken dagelijks (geautomatiseerd) veel persoonsgegevens. Het spreekt voor zich dat wij zorgvuldig met deze persoonsgegevens omgaan, niet alleen omdat dit verplicht is door wet- en regelgeving, maar ook omdat wij het zelf belangrijk vinden. Ook verwachten onze cliënten, medewerkers en vrijwilligers dit van ons, net als onze andere stakeholders. Onze cliënten, medewerkers en vrijwilligers mogen ervan uitgaan dat wij hun rechten niet schenden en dat wij zorgvuldig met hun persoonsgegevens omgaan.

Het blijft een continu onderdeel van het verwerken van persoonsgegevens: bewustwording bij onze medewerkers die dagelijks omgaan met persoonsgegevens. Goed zorgen voor cliënten betekent ook goed zorgen voor hun persoonsgegevens. Daarbij zijn wij ons bewust van bredere belangen en onze maatschappelijke verantwoordelijkheid. Naast het speelveld van de zorg heeft Riwis ook een verantwoordelijkheid richting deze maatschappij. Dat betekent dat wij soms afwegingen moeten maken tussen belangen van cliënten en maatschappij. Dus tussen persoonlijke rechten en de veiligheid van de omgeving.

Verleden en toekomst

De maatregelen die Riwis in 2020 nam op het gebied van privacy & informatiebeveiliging worden in deze Verklaring van Verantwoording beschreven. We zijn trots dat wij weer stappen vooruit hebben gezet. Een overzicht van onze ambities voor 2021 is te vinden op pagina 12.

Joost Harkink — 29 maart 2021
Bestuurder

Mededeling functionaris gegevensbescherming

Technische ontwikkelingen en wet- en regelgeving op het gebied van privacy en informatiebeveiliging volgen elkaar snel op. Bij het verder ontwikkelen van de organisatie houdt Riwis hier zoveel mogelijk rekening mee. Het blijft een uitdaging om een evenwicht te vinden tussen het voldoen aan de gestelde eisen en het door laten gaan van de reguliere bedrijfsvoering: met het verlenen van goede zorg als hoofdtaak. Elke keer moet een keuze gemaakt worden waar tijd en geld ingezet gaat worden.

In 2020 heeft de focus gelegen op het verder implementeren van privacy- en informatiebeveiliging-maatregelen. Zowel op technisch, beleidsmatig als organisatorisch gebied zijn weer belangrijke stappen gezet. Bij implementaties worden risico´s in kaart gebracht door het doen van Data Privacy Impact Assessments. Bevindingen hieruit worden opgepakt en opgelost. Met tussentijdse controles, zoals de controle op de autorisaties, worden risico´s gemonitord. Beleid is op punten verder aangescherpt en geïmplementeerd. Diverse technische maatregelen zijn genomen zoals het steeds meer werken met twee factor authenticatie (wee stappen succesvol moet doorlopen om ergens toegang tot te krijgen).

Privacyteam

Om het onderwerp privacy en informatiebeveiliging goed vorm te geven, heeft Riwis ervoor gekozen om te werken met een privacyteam dat bestaat uit een privacy officer en een functionaris voor gegevens-bescherming. De privacy officer is onder andere verantwoordelijk voor het vormgeven en bewaken van het privacybeleid binnen de organisatie. Hij ondersteunt bij het in kaart brengen van de risico's en verzamelt periodiek bewijsmateriaal ten behoeve van accountability. Daarnaast adviseert hij teamleiders en teams op vraagstukken vanuit de AVG en bij de beoordeling en de afwikkeling van beveiligingsincidenten. Privacy en informatiebeveiliging zijn onderdeel van de governance & compliance van Riwis. De Functionaris voor Gegevensbescherming (FG) ziet toe op de naleving van de AVG, aanpalende wetgeving en het privacybeleid van Riwis. De AVG schrijft diverse taken voor die de FG toebedeeld krijgt , deze zijn dan ook bij hem belegd.

Door de grote dynamiek op het onderwerp privacy en informatiebeveiliging is het werk nooit 'af' en hebben we weer voldoende plannen voor 2021.

Joris van den Heuvel 5 februari 2021
Functionaris Gegevensbescherming

Vastleggen en verwerken van persoonsgegevens

Riwis legt persoonsgegevens vast van haar cliënten, medewerkers, stagiaires en vrijwilligers en van zakelijke relaties. Dit is inherent aan het werk van Riwis en geldt dus ook voor gevoelige gegevens. Een groot deel van de verwerkingen betreft zogenaamde bijzondere gegevens, bijvoorbeeld gegevens betreffende de gezondheid en de begeleiding van cliënten. Bijkomende bijzonderheid is dat de cliënten zich veelal in een kwetsbare levensfase bevinden en in de begeleiding ook ketenpartners en naastbetrokkenen een belangrijke rol spelen.

Riwis legt persoonsgegevens van cliënten vast met de volgende doelen:

- Het begeleiden, verzorgen en/of huisvesten van cliënten met een (tijdelijke) beperkte zelfredzaamheid;
- Het bieden van ketenzorg aan cliënten, door samen te werken en persoonsgegevens te delen met ketenpartners en/of hulpverleners;
- Het beheren en verstrekken van medicatie aan cliënten;
- Het uitvoeren van een periodiek tevredenheidsonderzoek onder cliënten;
- Het bieden van opleiding in het kader van begeleiding van cliënten naar werk;
- Het begeleiden van cliënten naar (vrijwilligers)werk;
- Het informeren van cliënten over ontwikkelingen binnen en initiatieven van Riwis;
- Het bespreken casuïstiek van cliënten met complexe problematiek in Regionale Toegang;
- Het beschermen van de openbare orde en veiligheid in de regio;
- Het verbeteren van de kwaliteit van zorg door intern onderzoek;
- Het uitvoeren van wetenschappelijk onderzoek;
- Het verantwoorden van de financiën;
- Het verantwoorden van de geleverde prestaties in het kader van het begeleiden, verzorgen en/of huisvesten van cliënten;
- Het declareren van de kosten voor zorgverlening bij diverse instanties en cliënten;
- Het aanvragen van financiële bijstand of bijstand in natura (voedsel, huishoudelijke artikelen) namens de cliënt;
- Het bemiddelen tussen cliënt en de woningbouwvereniging;
- Het uitvoeren van interne en externe controle en de accountantscontrole;
- Het opleggen van de eigen bijdrage;
- Vastleggen van wensen van de cliënt ten aanzien van overlijden en het wel of niet reanimeren (op specifiek verzoek van een cliënt).

Daarnaast legt Riwis persoonsgegevens van met name medewerkers vast voor de volgende doelen:

- Het geven van leiding aan de werkzaamheden van medewerkers;
- Het behandelen en administreren van personeelszaken;
- Het opleiden en ontwikkelen van medewerkers;
- Het bieden van bedrijfsmedische zorg aan medewerkers;
- Het uitvoeren van voor de medewerkers geldende arbeidsvoorwaarden of afspraken;
- Het verlenen van ontslag en, indien van toepassing, het regelen van uitkeringen in verband met de beëindiging van een dienstverband;
- Het innen van vorderingen, waaronder inbegrepen het in handen van derden stellen van die vorderingen;
- Het behandelen van geschillen;
- Het uitvoeren of toepassen van een wet;
- Het berekenen, vastleggen en betalen van salarissen, vergoedingen, belastingen, premies, uitkeringen en andere geldsommen en beloningen in natura aan of ten behoeve van medewerkers;
- Het berekenen, vastleggen en innen van (pensioen)premies;
- Het kunnen aanbieden van collectieve ziektekostenverzekering;
- Het aanvragen van verklaring omtrent gedrag;
- Het verstrekken van attenties;
- Het afnemen van assessments bij medewerkers;
- Het aanvragen van subsidie en/of premiekortingen;
- Het verantwoorden aan gemeenten over aantal mensen in dienst met een afstand tot de arbeidsmarkt;
- Het faciliteren van een (vrijwillig) smoelenboek;
- Het faciliteren van toegangsbeveiliging;
- Het opstellen van een lijst van data van verjaardagen van werknemers en andere feestelijkheden en gebeurtenissen;
- Het verantwoorden van financiën;
- Het uitvoeren van interne en externe controle, de bedrijfsbeveiliging en accountantscontrole.

Naast gegevens van cliënten en medewerkers administreert Riwis ook gegevens van sollicitanten, de raad van toezicht, vrijwilligers, familie en andere naasten van cliënten, passanten, contractpartners, uitzendkrachten, ZZP'ers, gedetacheerde werknemers en ketenpartners. Van al deze verwerkingen van (persoons)gegevens zijn de doelen en de specifieke gegevens die verwerkt worden verder vastgelegd in 2020.

Soorten persoonsgegevens

Gegevens van cliënten en medewerkers staan in elektronische dossiers. Cliënten en medewerkers kunnen hun eigen dossier zelf inzien. Voorbeelden van persoonsgegevens die wij vastleggen staan in de privacyverklaring die op de website van Riwis staat en op het intranet te vinden is (voor medewerkers).
Persoonsgegevens van naastbetrokkenen, sollicitanten en anderen kunnen worden vastgelegd, een overzicht van de soorten persoonsgegevens die wij van hen vastleggen is te vinden in de privacyverklaring.

Verwerkers

Met verwerkers die gegevens verwerken in opdracht van Riwis sluiten wij verwerkersovereenkomsten af. In een dergelijke overeenkomst worden afspraken vastgelegd over onder andere welke persoonsgegevens een verwerker verwerkt, welke beveiligingsmaatregelen er getroffen zijn en de procedure voor het melden van incidenten[5].
Indien er sprake is van gezamenlijke gegevensverwerking met een andere *verwerkingsverantwoordelijke* dan worden vergelijkbare afspraken vastgelegd in een gegevensuitwisselingsovereenkomst.

[5] In de AVG staan eisen waaraan een dergelijke overeenkomst minimaal moet voldoen (AVG artikel 28 lid 3). Riwis zorgt ervoor dat de overeenkomsten minimaal aan die eisen voldoen.

Privacy framework

Het privacy framework biedt een kapstok om te beschrijven wat de stand van zaken is op het gebied van privacy en informatiebeveiliging, waar eventuele verbeterpunten liggen en welke ambitie Riwis heeft voor de komende periode.

	In- en externe wet- en regelgeving	Handelen en gedrag	Technische en fysieke beveiliging
Onderdelen Privacy en Informatiebeveiliging	Wet- en regelgeving Beroeps- en gedragscodes Nen-normen Beleid/reglementen Protocollen Werkinstructies/formulieren	Bewustwording Presentaties Opleiden Trainen Acties Bijeenkomsten	Nieuwe technieken Innovatieve oplossingen Systeembeschrijvingen Applicaties/Software Meldsysteem incidenten
Controls	Monitoren ontwikkelingen wet- en regelgeving Evalueren en herzien proces Audits (in- en extern) Datalekken analyse DPIA	Monitoren gedrag en naleven regels Evalueren en herzien proces Audits (in- en extern) Datalekken analyse Verwerkingsregister GAP-analyse	Monitoren toegang en netwerk Evalueren en herzien proces Audits (in- en extern) Datalekken analyse Controle autorisaties PEN-testen DPIA
Instrumenten	Privacyverklaring Privacybeleid Privacyadministratie Digitaal Handboek Verwerkingsregister	VOG Geheimhoudingsverklaring Naleven in- en externe wet- en regelgeving DPIA	Autorisatiebeleid/-matrix Authenticatiebeleid/-matrix Wachtwoordbeleid Applicatielogboek/archief Sleutel- en sluitplan

In- en externe wet- en regelgeving

Het beleid van Riwis is verwoord in verschillende documenten waar een sterke samenhang tussen bestaat. Hieronder is per document het doel en de voortgang omschreven. In deze documenten is de vertaling gemaakt vanuit wet- en regelgeving en beroeps- en gedragscodes naar de Riwis-organisatie. In 2020 zijn verdere stappen gemaakt om een deel van deze documenten meer in lijn met elkaar te brengen. In 2021 gaan wij hier mee verder.

Privacy & informatiebeveiligingsbeleid

In 2018 is het privacy- & informatiebeveiligingsbeleid herzien. Dit beleid geeft richting aan de invulling van de visie en uitgangspunten van Riwis op het gebied van privacy en informatiebeveiliging. Met dit beleid willen wij kaders stellen voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens die voldoet aan de wettelijke eisen. Begin 2019 zijn de laatste wijzigingen in het beleid doorgevoerd en is het beleid ook vastgesteld. Het beleid wordt geëvalueerd en, indien nodig, aangepast. Dit willen we in de loop van 2021 oppakken, ook omdat het beleid jaarlijks herzien moet worden.

Privacyverklaring

In de privacyverklaring geven wij betrokkenen informatie over:

- de persoonsgegevens die wij verwerken;
- de manier waarop wij dat doen;
- de verstrekking van gegevens aan anderen binnen of buiten Europa;
- hoe lang wij gegevens bewaren; en
- hoe wij deze gegevens beveiligen.

In de privacyverklaring leggen wij aan betrokkenen uit wat hun rechten zijn en bij wie ze terecht kunnen met vragen, verzoeken of klachten. In mei 2018 is een eerste bijgewerkte privacyverklaring op de website van Riwis gezet. In 2019 is gewerkt aan een vernieuwde versie, deze is begin 2020 op de website en het intranet van Riwis gepubliceerd.

Privacy en informatiebeveiligingsadministratie

Riwis Zorg & Welzijn streeft ernaar om alle activiteiten rondom privacy en informatiebeveiliging op te nemen in de privacyadministratie. In deze administratie is onder andere het verwerkingsregister opgenomen. Het verwerkingsregister is geen eenmalige registratie van alle verwerkingen, maar een organisch proces. Immers, verwerkingen ‘komen en gaan’. Het registreren van verwerkingen moet daarom op structurele wijze opgenomen worden in de organisatie zodat bij elke wijziging de integriteit van het verwerkingsregister behouden blijft. Dit betekent dat alle medewerkers zich bewust moeten zijn van het feit dat verwerkingen die zij doen in het register moeten staan. En ook dat er bij elke verwerking wordt stilgestaan bij de AVG: wat is het doel, wat is de grondslag, etc. Hier is ook een rol voor de privacy officer weggelegd, hij kan de medewerkers

begeleiden bij het beantwoorden van deze vragen. Het nadenken over de vragen en mogelijke antwoorden draagt ook bij aan de algemene privacybewustwording binnen Riwis. In onze privacyadministratie is (en wordt) het volgende vastgelegd:

- overzicht met de verbonden partijen waarmee Riwis persoonsgegevens uitwisselt;
- overzicht van afgesloten verwerkingsovereenkomsten;
- omschrijving van alle verwerkingen met doelen, stakeholders, gegevenssets, processen en informatiesystemen;
- verantwoording van alle activiteiten op het gebied van privacy en informatiebeveiliging binnen Riwis;
- onderzoeken (op het gebied van privacy) die door Riwis gedaan zijn;
- overzicht, onderzoek en analyse van datalekken.

In 2019 zijn de volgende acties in gang gezet om het verwerkingsregister verder te verrijken en in 2020 afgerond:

- controle op de volledigheid van de omschrijving van de verwerkingen en gegevens;
- controle op de volledigheid van alle in gebruik zijnde systemen;
- controle op de volledigheid van de verbonden partijen.

Protocol afhandeling datalekken

Eind 2018 is de procedure datalekken herzien. In dit protocol is beschreven welke stappen er zijn bij de afhandeling van een beveiligingsincident/datalek en aan welke zaken gedacht moet worden tijdens de afhandeling. In de loop van 2019 is deze procedure geoptimaliseerd op basis van nieuwe inzichten en definitief vastgesteld. In 2020 is deze procedure, samen met alle andere communicatie rondom privacy, worden 'uitgerold'.

Kern van het datalekkenprotocol is dat het maken van fouten (bijna) niet te voorkomen is. Dat betekent dat we alert moeten blijven, maar dat het melden van incidenten in de eerste plaats bedoeld is om van te leren. Door elke melding krijgen we een beter inzicht: waar en in welke processen gaat het gemakkelijk fout? Welke maatregelen kunnen we nemen om dezelfde fout te voorkomen?
Deze lessen en analyses van de meldingen, maakt dat wij de veiligheid en kwaliteit van onze organisatie nog verder kunnen verbeteren. En voor de betrokken medewerkers is het vaak weer even een *wake-up call*, en komt het de bewustwording ten goede.

In 2018 en 2019 is het systeem van het melden van datalekken en incidenten verbeterd: door goede afspraken en duidelijke stappen die bij elk datalek genomen moeten worden weten de diverse betrokken medewerkers precies wat hen te doen staat. In 2020 is veel gecommuniceerd rondom datalekken. Niet alleen met artikelen op intranet, maar ook door teamleiders en aandachtfunctionarissen na elk datalek te betrekken bij mogelijke oplossingen. En door bij teamoverleggen het betreffende datalek te bespreken.

Gap-analyse

Riwis gebruikt het zogenaamde *privacy control framework* van Norea (de beroepsorganisatie van IT-auditors) en de beheersmaatregelen van de Nen-normen voor informatiebeveiliging om inzicht te krijgen in de eisen die wet- en regelgeving ons opleggen.
Aan de hand van deze 'kapstokken' kijkt Riwis wat de huidige stand van zaken is en welke acties er nog ondernomen moeten worden. In 2019 is op basis van deze analyse bijvoorbeeld gekeken welke 114 maatregelen uit de NEN 7510 van toepassing zijn op Riwis. Vervolgens is per 'van toepassing zijnde maatregel' onderzocht in hoeverre Riwis hier aan voldoet en/of welke acties Riwis eventueel moet doen om te gaan voldoen. Uit deze inventarisatie zijn diverse verbeterpunten naar voren gekomen die geprioriteerd zijn. Deze verbeterpunten zijn in 2020 grotendeels opgepakt en afgerond. Daarmee heeft Riwis een robuustere privacyadministratie gekregen en meer grip op gegevensverwerking en informatiebeveiliging. In 2021 gaan we nogmaals kijken hoe we ervoor staan met betrekking tot deze normen en wordt ook gekeken naar andere – nieuwere – normen, zoals NEN 7513.

Risicomanagement

Riwis zet zich in voor risicobeheer als een integraal onderdeel van haar activiteiten, en richt zich er op om het risico te minimaliseren dat de doelstellingen van Riwis niet worden gehaald. Bij het inschatten van risico's gaan wij ervan uit dat we als organisatie transparant moeten en willen zijn. In 2020 zijn de risico's, juist ook op het gebied van privacy & informatiebeveiliging beter in kaart gebracht.

Handelen en gedrag

Bewustworden

Net als in voorgaande jaren heeft Riwis in 2020 veel aandacht besteed aan de interne bewustwording rondom privacy & informatiebeveiliging. Het bezoek aan teams was lastig door de coronamaatregelen. Zodra de maatregelen dit weer toestaan, zal de privacy officer weer teams bezoeken om uitleg te geven en vragen te beantwoorden. De bezoeken voorzien duidelijk in een behoefte en draagt bij aan de 'zichtbaarheid' van privacy. In plaats van het bezoeken van locaties, heeft de privacy officer de teamleideroverleggen bijgewoond om daar vragen te beantwoorden en privacy te bespreken.

Op intranet zijn er door het jaar heen 10 berichten geplaatst over privacy. Deze berichten gingen onder andere over het opschonen van mappen en e-mail, het melden van datalekken (VIM-meldingen), tips & tricks en blogs van een cliënt die onder pseudoniem zijn kijk geeft op privacyonderwerpen aangevuld met commentaar van de privacy officer. In 2021 wordt dit format voortgezet.

Bewustwording is een relatief traag proces. Kennis, houding en gedrag zijn de opeenvolgende stadia in deze. Met de kennis dat men zorgvuldig moet omgaan met persoonsgegevens zit het goed binnen de organisatie. De houding is ook al gekanteld (of begint te kantelen): medewerkers begrijpen dat het belangrijk is om zorgvuldig te werk te gaan. In 2021 blijft Riwis doorlopend aandacht besteden aan bewustwording rondom privacy.

Gedragsregels en geheimhoudingsverklaringen

In 2018 zijn er zijn gedragsregels met betrekking tot privacy en informatiebeveiliging opgesteld, in 2019 is hier aandacht aan besteed. Het doel van de gedragsregels is om de Riwis-medewerkers handvatten te geven om nog beter om te gaan met (gevoelige) persoonsgegevens. Jaarlijks krijgen de medewerkers de gedragsregels digitaal aangeboden en moet men actief aangeven hiervan kennis te hebben genomen. Ook zijn de arbeidsovereenkomsten aangepast met een verwijzing naar deze regels en het privacy en informatiebeveiligingsbeleid. In 2020 zijn de gedragsregels aangescherpt voor het gebruik van social media op het werk.

Voor ZZP'ers en andere 'externen' is er een gedragscode voor toegang tot onze informatiesystemen en een verklaring toegang tot informatiesystemen die door de externe medewerker getekend wordt.

Verklaring Omtrent het Gedrag (VOG)

Voor elke nieuwe medewerker, vrijwilliger en stagiaire wordt een verklaring omtrent het gedrag aangevraagd en vastgelegd in het personeelsdossier. In 2019 is besloten om deze VOG elke vier jaar te 'vernieuwen' en in 2020 in dit beleid in gang gezet en zijn de eerste nieuwe VOG's aangevraagd..

Technische en fysieke beveiliging

Autorisatie en authenticatie beleid

De doelstelling van het Riwis-autorisatiebeleid is het waarborgen van een, door beleidsbepaling overeengekomen, gecontroleerde toegang tot en gebruik van systemen door medewerkers en/of derde partijen van Riwis. Het autorisatiebeleid geeft aan wie waarvoor toegang heeft in een bepaald applicatie en welke periodieke controle daarop plaatsvindt. Voor het elektronisch cliëntdossier is dit beleid vastgelegd in het protocol cliëntdossier dat in 2018 herzien is. In 2019 is dit voor overige applicaties ook specifiek vastgelegd en in 2020 wordt hier op gecontroleerd waarbij naar maandelijkse controles wordt toegewerkt.

Authenticatie is het proces waarbij nagegaan wordt of iemand echt is wie hij beweert te zijn. Voor het inloggen wordt gebruik gemaakt van gebruikersnaam en een sterk wachtwoord dat periodiek gewijzigd moet worden. Er is een technisch wachtwoordbeleid gemaakt. In 2020 is voor een groot deel van onze applicaties twee factor authenticatie (2FA) ingevoerd. O.a. voor AFAS (financiële administratie), Ons (roosteren, Elektronisch Cliënten Dossier) en het digitale handboek waarin ook VIM-meldingen worden gedaan. Dit laatste is eind 2020 in gang gezet en in januari 2021 afgerond.

Periodieke beveiligings- en penetratietesten

Een penetratietest of pentest (binnendringingstest) is een toets van een of meer computersystemen op kwetsbaarheden, waarbij deze kwetsbaarheden ook werkelijk gebruikt worden om in deze systemen in te breken. Riwis heeft in 2020 geen specifieke beveiligings- en penetratietesten gedaan. De ambitie voor 2021 is om te oriënteren op de mogelijkheden van een pen-test (kosten, leveranciers) om een test mogelijk in 2022 uit te voeren.

Controle autorisaties

In 2018 en 2019 is een matrix ontwikkeld waarbij per medewerker inzichtelijk is welke autorisatie hij heeft in de verschillende systemen. In 2020 is begonnen met het daadwerkelijk toepassen van deze controles. De functioneel beheerders controleren aan de hand van deze lijst of de gebruikers in het systeem enerzijds nog een relatie hebben met Riwis en anderzijds of hun rol nog past bij de rechten waarover zij binnen de applicaties beschikken. Niet alleen vanuit functioneel perspectief, maar ook vooral met het oog op privacy- en informatiebeveiliging is het van groot belang dat de autorisaties correct zijn. Eind 2020 is een deel van de controles maandelijks en een deel tweemaandelijks. De functioneel beheerders zijn ondertussen gewend aan het werken met de autorisatiematrix en vinden het prettig dat dit 'vangnet' er is.

Monitoring (technische infrastructuur)

Het netwerk wordt zeven dagen per week gemonitord door een externe leverancier. Signalering van incidenten vindt direct plaats. Periodiek worden hier rapportages van gemaakt. Daarnaast heeft Riwis een *tool* ontwikkeld waarin de beschikbaarheid van de datalijnen naar de locaties wordt gemonitord.

Systeem beschrijvingen/applicatie logboek

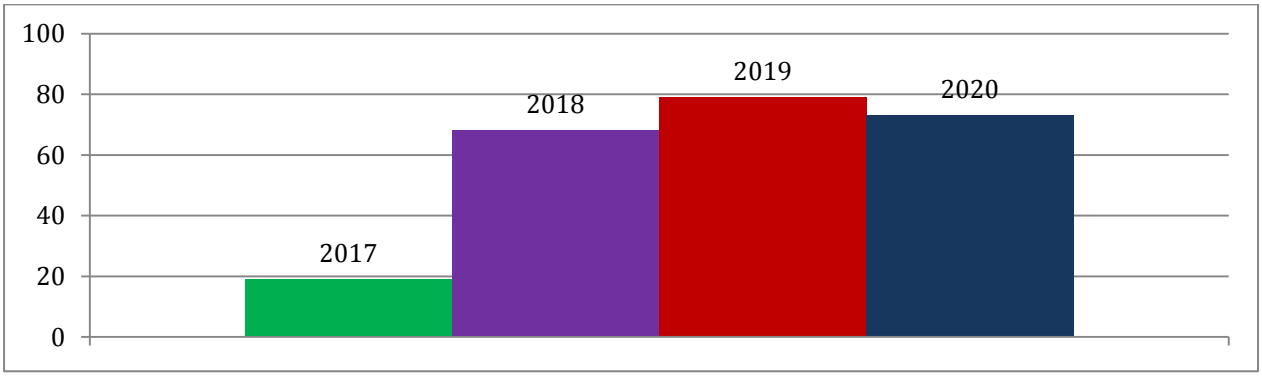
Binnen Riwis is de informatie over alle applicaties beschikbaar bij de functioneel beheerders. In 2020 is van een aantal applicaties bekeken of de informatie volledig en juist is vastgelegd. In 2021 wordt deze actie verder uitgevoerd.

Analyse van datalekken

De analyse van datalekken leidt tot het vergroten van de bewustwording. Medewerkers kunnen datalekken melden via het incidentmanagementsysteem. Datalekken worden afgehandeld conform het protocol datalekken.

In de afgelopen jaren (2017 tot en met 2019) is er een toename te zien van het aantal gemelde datalekken. In 2020 nam het aantal weer licht af. Gezien het grote aantal handelingen waarbij persoonsgegevens betrokken zijn in combinatie met een altijd aanwezige kans op vergissingen, is het niet realistisch om te verwachten dat het aantal incidenten tot nul zal dalen. Streven is wel om het aantal incidenten te verminderen, maar daarvoor moeten we wel eerst in kaart hebben waar de grootste kans op fouten en vergissingen is. Kijken we naar 2019 en 2020, dan is het werken in ONS en het gebruik van Outlook het meest 'gevaarlijk'. Daar worden de meeste vergissingen begaan. In de communicatie wordt ook benadrukt om 10 seconden extra de tijd te nemen bij het werken in ONS en gebruik van Outlook. En dat veilig mailen belangrijk (verplicht) is, zeker bij het versturen van bijzondere persoonsgegevens. In 2021 stapt Riwis over van KPN Zorgmail naar Zivver voor het veilig versturen van e-mails. Zivver is gebruikersvriendelijker, geeft hints bij bepaalde trefwoorden en past het beveiligings-niveau automatisch van verzenden aan op basis van bijlagen en inhoud van de e-mail.

Met het creëren van een veilig, stimulerend en ondersteunend klimaat, wil Riwis zorgen voor een toenemende meldingsbereidheid.



Eind 2020 hebben we de meldingen nog eens gecontroleerd op de juiste categorisering. Uit de controle bleek dat niet alle meldingen goed waren geregistreerd. Dit hebben we verbeterd. De afname in de categorie 'Overig' komt bijvoorbeeld door deze correctie.

Oorzaak datalek[6]	**Aantal in 2020**	**Aantal in 2019**
Registratie persoonsgegevens bij verkeerde cliënt/medewerker in digitaal systeem Riwis	35	29
Persoonsgegevens verstuurd naar verkeerd adres/onrechtmatige ontvangst	20	19
Document met persoonsgegevens in openbare ruimte	4	5
Verlies of diefstal van apparatuur/dossier of andere gegevensdrager	4	2
Niet afgesloten ruimte/kast/ e.d.	2	1
Overig	8	23
Totaal	**73**	**79**

Van de datalekken zijn er vier gemeld aan de Autoriteit Persoonsgegevens en betrokkenen.

[6] In 2019 zijn de categorieën datalekken gewijzigd, waardoor er wat verschillen ontstaan zijn met vorige rapportages.

Ambities 2020 en 2021

De afgelopen jaren is Riwis op veel deelonderwerpen van privacy en informatiebeveiliging hard aan de slag gegaan. De volgende onderwerpen stonden voor 2020 op de agenda:

Ambitie	**Stand van zaken/toelichting**
Beleid maken op omgang met logbestanden	De voorbereiding voor dit beleid zijn getroffen, in 2021 wordt dit beleid uitgewerkt.
Opnieuw aanvragen VOG voor medewerkers die al langer in dienst zijn.	Beleid gemaakt, gecommuniceerd en begonnen met uitvoering beleid door HRM.
Vervangen van het verouderde serverpark	Analyse en wensenlijst gemaakt. Door corona is e.e.a. vertraagd. In 2020 is begonnen met het ontwikkelen van een nieuwe digitale strategie voor Riwis. Daarin wordt dit onderwerp ook meegenomen. Daarnaast werken veel diensten (AFAS, Ons) in de *cloud.* Het aantal applicaties dat op onze eigen servers draait, neemt af. Dit betekent dat Riwis gemakkelijker passende alternatieven kan vinden voor het verouderde serverpark.
Transitie naar de *cloud* van diverse applicaties	Dit is in 2020 afgerond voor bijvoorbeeld Afas en Ons.
2FA bij algemene login	Dit is voor grote applicaties als Afas, Ons en het digitale handboek gerealiseerd.
Mobile Device Management	In 2020 nog niet helemaal afgerond, maar wordt onderdeel van nieuwe digitale werkplekken die in 2021 worden uitgerold.
Uitvoeren van DPIA's	In 2020 zijn enkele DPIA's gedaan (AFAS, Ons) en is begonnen met een inventarisatie van bestaande verwerkingen waar een (hernieuwde) DPIA nodig is.
Verder verhogen van privacybewustzijn medewerkers	Dit is een continu proces. Bijeenkomsten, vergaderingen, teamoverleg en andere communicatiekanalen worden gebruikt om de privacyboodschap over te brengen.
Verwerkingsregister verder uitbouwen/upgraden	In 2020 zijn hier grote stappen in gezet. In 2021 wordt dit verder verfijnd.
Camerabeleid	Herzien in 2020 en geïmplementeerd. In 2021 worden alle locaties waar nu camera's zijn langs de lat van dit beleid gehouden.
Audits op verschillende onderwerpen m.b.t. privacy en informatiebeveiliging	Er zijn audits geweest op de opslag van documenten, gebruik van camera's, HR-processen, Afas, tijdelijke accounts van externe medewerkers, en een audit op de general IT en application controls. Op basis van deze audits zijn verbeterpunten bepaald en opgenomen in het verbeterregister van Riwis.
Uitvoeren van een testtoets op kwetsbaarheden van computersystemen	Dit is onderdeel van de nieuwe digitale strategie voor Riwis.
Een volgende stap nemen en een Information Security Management System conform NEN 7510 ontwikkelen	Hier zijn de eerste stappen voor gezet in 2020, wordt in 2021 uitgewerkt.

Ambities voor 2021

- Interne beleidsdocumenten meer met elkaar in lijn brengen. Herzien en, indien relevant, aanpassen aan veranderende wetgeving.
- Privacyverklaring: in de loop van 2021 wordt geëvalueerd of het privacybeleid anders en gebruiksvriendelijker gepresenteerd kan worden.
- Bewustwording: dit is een continu 'proces'. Communicatie is een belangrijk onderdeel van privacy beheer.
- Verwerkingsregister: verder uitbouwen, m.n. leveranciers, systemen e.d. Daardoor wordt het nog duidelijker welke gegevens in welk systeem worden verwerkt. Omdat het een levend document is, zullen wijzigingen in verwerkingen worden opgenomen.
- In 2021 gaan we nogmaals kijken hoe we ervoor staan met betrekking tot deze normen en wordt ook gekeken naar andere – nieuwere – normen, zoals NEN 7513.
- Managementsysteem conform NEN 7510 opstellen en implementeren.
- Audits op het gebied van privacy en informatiebeveiliging.
- Locaties met camera's langs de lat van onze nieuwe DPIA-standaard leggen.
- DPIA's voor bestaande verwerkingen evalueren en/of opnieuw doen.
- Mobile Device Management: verbeteren, vernieuwen (onderdeel nieuwe digitale werkplekken).
- Omgang met logbestanden: afronden beleid, uitrollen beleid.

Bijlage 1: Samenvatting voor bestuursverslag 2020

Stappen

In 2020 zijn goede stappen gezet om de privacy en informatiebeveiliging te verbeteren. De bewustwording is vergroot, er zijn diverse beleidsstukken opgesteld, het verwerkingsregister is bijgewerkt en het aantal incidenten is stabiel.

Risico's

Wat zijn de risico's voor Riwis in het kader van privacy en informatiebeveiliging? Deze zijn vooral te vinden op het vlak van het niet voldoen aan wet- en regelgeving en beveiligingsniveaus en -normen, zoals de AVG, NTA 7516/NEN7510 en (andere) Nen-normen. Ook loopt Riwis een risico wanneer werkzaamheden en ambities op het gebied van privacy en informatiebeveiliging voor de komende jaren niet afgerond worden. De afweging die wij soms (moeten) maken tussen belangen van betrokkenen en maatschappelijke belangen houdt ook een risico in. Denk hierbij aan persoonlijke rechten en de veiligheid van de omgeving. Verder vormen datalekken en andere incidenten een risico, niet alleen voor de betrokkenen wiens gegevens wellicht in gevaar zijn bij een incident, maar ook reputatieschade voor Riwis ligt op de loer.

Registratiesystemen

De registratiesystemen die bijdragen aan het doel van een goed beheer van privacy en goede informatiebeveiliging zijn eigenlijk alle systemen waar persoonsgegevens in verwerkt worden. Daarbij zijn de belangrijkste:

- ONS voor cliëntendossiers, roosters e.d.
- AFAS voor personeelsdossiers en financiële administratie.
- Het digitale handboek voor protocollen en VIM-meldingen (datalekken/incidenten).
- Contractregister, zodat we overzicht hebben van alle verwerkersovereenkomsten.