Verklaring van accountability 2018

Verantwoording van Riwis Zorg & Welzijn

aan betrokkenen over het voldoen aan wet- en regelgeving

op het gebied van privacy & informatiebeveiliging

Auteur: Joris van den Heuvel
Datum: 24 januari 2019
Status: Definitief

Voorwoord

Informatie komt in verschillende vormen voor. Bijvoorbeeld gedrukt of geschreven op papier, elektronisch opgeslagen, per post of via elektronische middelen verzonden, via film tonen of mondeling uitwissellen. Informatie behoort altijd op geschikte wijze te worden beschermd, rekening houdend met de vorm of de wijze waarop het is gedeeld of opgeslagen. Het omgaan met informatie is in veel wetgeving geregeld.

In snel tempo wordt wetgeving op het gebied van privacy en informatiebeveiliging aangenomen. Per 1 juli 2017 is de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (gedeeltelijk) in werking getreden. Deze wet verplicht zorginstellingen om hun informatiebeveiliging conform de NEN-normen in te richten. De NEN-normen zijn opgesteld door de stichting Nederlands Normalisatie-instituut en specifiek gericht op de zorg:

- NEN 7510: norm voor het organisatorisch en technisch inrichten van de informatiebeveiliging in de zorg;
- NEN 7512: nadere invulling van NEN 7510 betreffende de veiligheid van gegevensuitwisseling tussen partijen in de zorg
- NEN 7513: nadere invulling van NEN 7510 betreffende het vastleggen van acties op elektronische cliëntendossiers

Naast deze wet zijn er meer wetten waar bepalingen opgenomen zijn over privacy en informatiebeveiliging. Denk hierbij aan de Wet Maatschappelijke ondersteuning, de Wet op de Geneeskundige Behandelovereenkomst, de archiefwet, de Jeugdwet, de Wet langdurige zorg en de Wet kwaliteit klachten en geschillen in de zorg. Naast deze wetten is er ook wetgeving om de privacy te beschermen: de Europese Algemene Verordening Gegevensbescherming (AVG).

In wetten zijn 'Accountability' en 'Auditability' de kernbegrippen. Bescherming van persoonsgegevens is een grondrecht en met deze gegevens moet de verwerkingsverantwoordelijke[1] zorgvuldig omgaan. Dit geldt ook voor de verwerker en/of zijn subverwerker. Er is sprake van ketenaansprakelijkheid, dat wil zeggen dat de verwerkingsverantwoordelijke in de organisatie verantwoordelijk èn aansprakelijk is voor het feit dat zijn verwerkers[2] (en mogelijke subverwerkers) de AVG naleven.

Accountable zijn betekent het volgende. De AVG vereist van de verwerkingsverantwoordelijke dat alles gedocumenteerd wordt waar hij of zij voor verantwoordelijk èn aansprakelijk is. Dit betekent het bijhouden van een privacy & informatiebeveiligingsadministratie. In deze administratie wordt overzicht en inzicht gegeven in de verantwoordelijkheid en aansprakelijkheid in de eigen organisatie en de verbonden partijen (verwerkers) waarmee contractuele verplichtingen zijn aangegaan. Daarnaast wordt overzicht en inzicht gegeven in de verwerkingen van persoonsgegevens, de bijbehorende processen, de informatiesystemen die de verwerkingen uitvoeren. De AVG verlangt van de verwerkingsverantwoordelijke dat hij of zij kan waarborgen en aantonen dat technische en organisatorische maatregelen zijn genomen dat het verwerken van persoonsgegevens in overeenstemming met de AVG wordt uitgevoerd. Door het bijhouden van de administratie is de verantwoordelijke tevens **Auditable** want we documenteren aantoonbaar wat we deden, doen en gaan doen.

Riwis Zorg & Welzijn (hierna te noemen Riwis) vindt het vanzelfsprekend en van groot belang dat we goed omgaan met privacygevoelige persoonsgegevens. Daarbij vindt Riwis het belangrijk dat we met persoonsgegevens van een ander omgaan zoals iedereen wenst dat er met zijn/haar eigen persoonsgegevens wordt omgegaan. Dit betekent privacybewustzijn bij iedere medewerker. Hierbij nemen we de volgende punten mee bij het maken van keuzes:

[1] De verwerkingsverantwoordelijke uit de AVG is diegene die de eindverantwoordelijkheid op het gebied van privacy heeft. Meestal een bestuurder of directeur.

[2] De verwerker uit de AVG is diegene die persoonsgegevens in opdracht van de verwerkingsverantwoordelijke op basis van een verwerkingsovereenkomst verwerkt (verzamelt, corrigeert, aanvult, wijzigt, verwijderd).

- Privacy en gegevensbescherming mag de zorg niet in de weg staan;
- Evenwicht tussen gebruikersgemak en gegevensbescherming;
- Uitgangspunt is vertrouwen in de professionaliteit van de medewerker en controle van de professionaliteit;
- Zorgvuldigheid staat voorop, het helemaal uitsluiten van datalekken is niet mogelijk.

In 2018 is Riwis intensief bezig geweest met het versterken van privacy en informatiebeveiliging. Aan de hand van de nieuwe wetgeving zijn de doelen aangescherpt en zijn bestaande documenten en werkwijzen aangepast. Het privacy framework waarin de verschilllende onderdelen van privacy en informatiebeveiliging omschreven zijn (zie hoofdstuk 5), biedt een kapstok om te beschrijven wat de stand van zaken is, waar eventuele verbeterpunten liggen en welke ambitie Riwis heeft voor de komende periode.

Op de website van Riwis is beperkte informatie opgenomen over privacy en informatiebeveiliging. In 2019 wil Riwis meer informatie verstrekken. Zo zullen delen van deze verklaring van accountability, de privacyverklaring en de gegevens van de functionaris gegevensbescherming op de site geplaatst gaan worden.

1. Inleiding 5
1.1. Doel verklaring van accountability 5
1.2. Gebruik verklaring van accountability 5
2. Mededeling raad van bestuur 7
3. Mededeling functionaris gegevensbescherming 8
4. Vastleggen persoonsgegevens 9
5. Privacy framework 10
5.1 In- en externe wet- en regelgeving 10
5.2 Handelen en gedrag 12
5.3 Technische en fysieke beveiliging 12
6. Analyse van datalekken 13
7. Ambitie voor 2019 14

1. Inleiding

1.1. Doel verklaring van accountability

In de Governancecode Zorg staat dat de raad van bestuur verantwoording aflegt over de realisatie van de 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.

In deze verklaring van accountability legt Riwis verantwoording af aan alle belanghebbenden over de naleving van verplichtingen vanuit wetgeving op het gebied van privacy 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 controles. Hiermee wordt een totaalbeeld van 'accountability' gegeven.

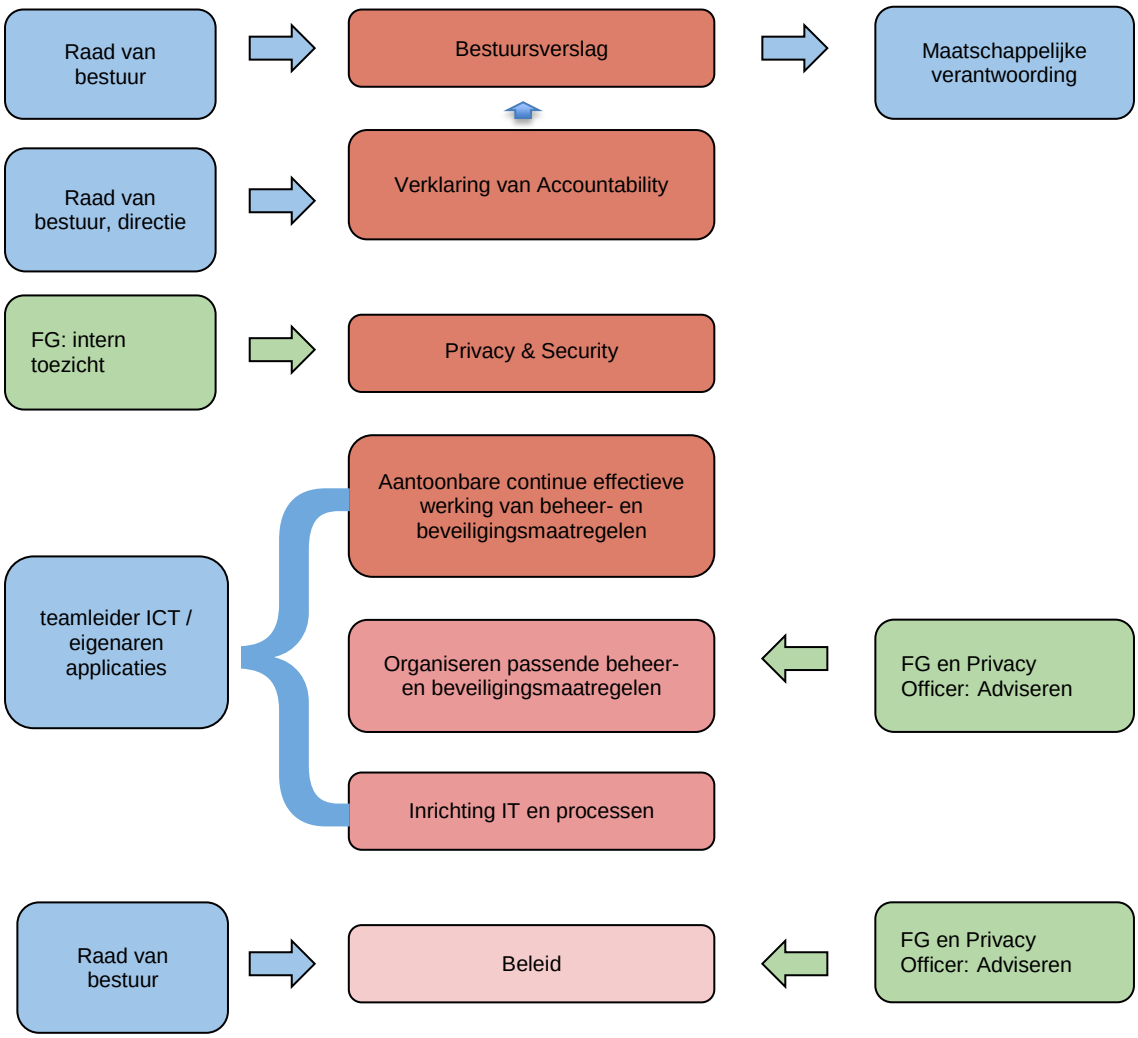
1.2. Gebruik verklaring van accountability

Deze verklaring van accountability is een aanvulling op de governance paragraaf in het jaarlijkse bestuursverslag. Deze verklaring is bestemd voor stakeholders (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.

In de 'mededeling van de raad van bestuur' nemen de leden van de raad van bestuur de volledige verantwoordelijkheid op zich voor het afleggen van de verantwoording.

Privacy en informatiebeveiliging is een onderdeel van de governance & compliance van Riwis. In het onderstaand overzicht staan de stappen rondom privacy en verantwoording beschreven en wie welke rol heeft. In de middelste kolom is schematisch weergegeven hoe het proces van het opstellen van beleid, tot invulling, toezicht en verantwoording loopt. Aan de zijkanten staan de betrokken partijen.

Governance & compliance privacy



2. Mededeling raad van bestuur

Een belangrijke opdracht is dat we de persoonsgegevens van onze cliënten, medewerkers en vrijwilligers beschermen en er zeer zorgvuldig mee omgaan. Wij verwerken dagelijks (geautomatiseerd) persoonsgegevens.

Zorgvuldigheid betrachten doen we niet alleen vanuit een wettelijke verplichting. We vinden het zelf belangrijk. Hier staat het bestuur voor. Onze cliënten, medewerkers en vrijwilligers mogen ervan uitgaan dat wij hun rechten niet schenden en dat wij zorgvuldig met zijn of haar persoonsgegevens omgaan. Voor ons begint dat bij bewustwording van medewerkers bij het gebruiken van persoonsgegevens.

Ieder individu heeft het recht op inzage in zijn persoonsgegevens die over hem worden verwerkt, mag deze laten aanpassen, aanvullen of verwijderen indien dit noodzakelijk is voor het juiste inzicht over hem en in lijn is met het doel waarvoor zijn gegevens worden verwerkt. Ook mag iedereen, als hij dat wenst, het gebruik gedeeltelijk of volledig beperken van zijn persoonsgegevens. Iedereen mag een klacht indienen bij de Autoriteit Persoonsgegevens als hij denkt dat zijn persoonsgegevens niet met respect en/of juist worden verwerkt en/of onvoldoende zijn beschermd.

Met het ingaan van de Europese Algemene Verordening Gegevensbescherming hebben we het bestaande beleid ten aanzien van privacy & gegevensbescherming verder aangescherpt. Eind 2017 heeft Riwis een functionaris gegevensbescherming (FG) aangenomen. Deze functionaris heeft het beleid aangescherpt en een roadmap gemaakt voor de verdere implementatie van de AVG. In de zomer van 2018 heeft deze FG Riwis verlaten. Riwis koos ervoor om met een privacy officer en een externe FG te werken. De privacy officer begon in september en de FG in november.

De maatregelen die Riwis in 2018 nam op het gebied van privacy & informatiebeveiliging worden in deze verklaring van accountability beschreven. We zijn trots dat wij belangrijke stappen vooruit hebben gezet. Onze ambitie voor het komende jaar is te lezen in hoofdstuk zeven.

Bram Noorlander
Bestuurder a.i.

3. Mededeling functionaris gegevensbescherming

In november 2018 startte ik als functionaris gegevensbescherming bij Riwis. Riwis koos voor een model waarin een privacy officer en een functionaris gegevensbescherming werken. Hierdoor kan ik me concentreren op mijn taken als interne toezichthouder en het adviseren van de Raad van Bestuur en de privacy officer.

In 2018 investeerde Riwis in verdere verbeteringen van het privacyvraagstuk en informatiebeveiliging. Naast de stuurgroep privacy waren er een werkgroep NEN 7510 en een werkgroep Datalek. In deze groepen waren de privacy officer, de manager bedrijfsvoering, het hoofd ICT, adviseur HRM en de coördinator bedrijfsvoering vertegenwoordigd. De kracht van de multidisciplinaire aanpak bewijst zich in de praktijk. Het bewustworden en het draagvlak voor het verder ontwikkelen van het privacy en informatiebeveiligingsbeleid nam toe.

Zo is onder andere het privacybeleid herschreven, is een eerste aanzet gemaakt met het opstellen van een verwerkingsregister en is de procedure voor het melden van datalekken herzien. Datalekken zijn afgehandeld conform deze procedure. Daarnaast is er veel aandacht besteed aan awareness en het communiceren over de rechten van betrokkenen.

Riwis volgt hiermee wet- en regelgeving.

In deze verklaring worden alle in 2018 ondernomen acties verantwoord. Ook worden eventuele verbeterpunten en de ambitie voor de komende periode benoemd.

Joris van den Heuvel
Functionaris Gegevensbescherming

4. Vastleggen persoonsgegevens

Riwis legt persoonsgegevens vast van haar cliënten, medewerkers, stagiaires en vrijwilligers en zakelijke relaties. Inherent aan het werk van Riwis legt zij veel privacygevoelige gegevens vast. Een groot deel van de verwerkingen betreffen zogenaamde bijzondere gegevens, namelijk 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 namen 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 (andere) 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 naasten van cliënten, passanten, contractpartners, uitzendkrachten, ZZP'ers, detachanten en ketenpartners. Van al deze verwerkingen van (persoons)gegevens worden de doelen en de specifieke gegevens die verwerkt worden verder vastgelegd in 2019.

5. Privacy framework

Het privacy framework biedt een kapstok om te beschrijven wat de stand van zaken is, 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**
Privacy en informatie-beveiligingsonderdelen	Wet- en regelgeving Beroeps- en gedragscodes NEN- normen Beleidsdocumenten Protocollen Werkinstructies	Bewustworden Presentaties Opleiden Trainen Acties	Nieuwe technieken Innovatieve oplossingen Systeembeschrijvingen Applicaties /Software Meldsysteem incidenten
Controls	Monitoren ontwikkelingen wet- en regelgeving Evalueren en herzien proces Audits (in- en extern) GAP analyse Datalekken analyse	Monitoren gedrag en naleven regels Evalueren en herzien proces Audits (in- en extern) GAP analyse Datalekken analyse	Monitoren toegang en netwerk Evalueren en herzien proces Audits (in- en extern) GAP analyse Datalekken analyse Controle autorisaties Pentesten
Middelen	Privacyverklaring Privacybeleid Privacy administratie Handboek	VOG Geheimhoudingsverklaringen Naleven in- en externe wet- en regelging	Autorisatiebeleid / matrix authenticatiebeleid / matrix Wachtwoordbeleid Applicatie logboek / archief Sleutel- en sluitplan

5.1 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 gedragcodes naar Riwis.

Privacy & informatiebeveiligingsbeleid

In 2018 is het privacy & informatiebeveiligingsbeleid herzien. Dit beleid geeft richting aan de invulling van de visie en uitgangspunten van Riwis. Het doel van dit beleid is om de kaders te stellen voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens die voldoet aan de wettelijke eisen. Begin 2019 worden de laatste wijzigingen in het beleid doorgevoerd waarna het vastgesteld kan worden.

Privacyverklaringen

In de privacyverklaring wil Riwis betrokkenen informatie geven 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.

Daarnaast willen wij betrokkenen via dit privacyreglement informeren over hun rechten en bij wie ze terecht kunnen met vragen, verzoeken of klachten.
In mei 2018 is een privacy statement op de website geplaatst. Er wordt momenteel gewerkt aan een uitgebreide privacyverklaring. Begin 2019 wordt de privacyverklaring definitief vastgesteld en op de website geplaatst.

Privacy en informatiebeveiligingsadministratie

Het hart van alle activiteiten rondom privacy en informatiebeveiliging is administratie. In deze administratie is het verwerkingsregister opgenomen. Het verwerkingsregister is geen eenmalige registratie, maar een organisch proces. Het registreren moet daarom op structurele wijze opgenomen worden in de organisatie zodat bij elke wijziging de integriteit van het verwerkingsregister behouden blijft.
In onze privacyadministratie zijn de volgende zaken 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 door Riwis gedane activiteiten op het gebied van privacy en informatiebeveiliging;
- onderzoeken die door Riwis gedaan zijn;
- onderzoek van datalekken.

We willen de administratie in 2019 verder aanvullen, de volgende acties staan gepland:

- 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 tijden de afhandeling. Begin 2019 wordt de procedure definitief vastgesteld.

Het melden van incidenten is in de eerste plaats bedoeld om te leren. De inhoudelijke lessen, maar zeker ook het proces van het melden, leiden tot een verbetering van de veiligheid en kwaliteit van een organisatie. Een melding is het startsein voor feedback en dus het proces van verbetering en bewustworden. Riwis beschikt over een goed werkend systeem voor het melden van incidenten.

Gap analyse

Om inzicht te krijgen in de eisen vanuit wet en regelegeving gebruikt Riwis het privacy control

framework van Norea (beroepsorganisatie van IT-auditors) en de beheersmaatregelen van de de NEN normen voor informatiebeveiliging. Aan de hand van deze kapstokken kijkt Riwis wat de huidge stand van zaken is en welke acties er nog ondernomen moeten worden. In 2019 wordt het NEN kader aangepast aan de inmiddels vernieuwde norm.

5.2 Handelen en gedrag

Bewustworden

Riwis heeft in 2018 veel aandacht besteed aan de bewustwording van medewerkers op het onderwerp privacy & informatiebeveiliging. De privacy officer heeft 25 teams bezocht, uitleg gegeven en vragen beantwoord. Deze bezoeken lopen door in 2019. Daarnaast is in 2018 gestart met het houden van privacy lunchsessies.

Op intranet zijn er door het jaar heen 11 berichten geplaatst over privacy. Deze berichten gingen onder andere over het schonen van mappen, datalekken, de introductie van follow me printing, veilig mailen en het nieuwe protocol cliëntdossier.

Met Sinterklaas is een actie geweest met een nepphishing e-mail voor medewerkers.

In 2019 blijft Riwis doorlopend aandacht besteden aan bewustwording.

Gedragsregels en geheimhoudingsverklaringen

Er zijn gedragsregels met betrekking tot privacy en informatiebeveiliging opgesteld. Het doel is het professionele handelen van onze medewerkers te vergroten. Jaarlijks krijgt de medewerker via het medewerkersportaal de gedragsregels aangeboden en moet zij/hij actief aangeven hiervan kennis te hebben genomen. Ook zijn de arbeidsovereenkomsten aangepast met een verwijzing naar deze regels en het privacy en informatiebeveiligingsbeleid.

Voor het geval iemand van buiten Riwis ingehuurd wordt is er een gedragscode voor toegang tot informatiesystemen en een verklaring toegang tot informatiesystemen die door de externe medewerker getekend wordt.

Verklaring omtrend gedrag (VOG)

Voor elke nieuwe medewerker, vrijwilliger en stagiaire wordt een verklaring omtrend gedrag aangevraagd.

5.3 Technische en fysieke beveiliging

Autorisatie en authenticatie beleid

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 begin 2018 herzien is. In de komende periode wordt dit voor de overige applicaties ook specifiek vastgelegd.

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. Er wordt op dit moment beperkt gewerkt met two-way-authenticatie. Gezien het feit dat we met medische gegevens werken is dit wel een vereiste vanuit de NEN, over nadere invulling gaan we in 2019 nadenken.

Onderzoeken

In 2018 vonden er verschillende preventieve onderzoeken plaats. Er deden zich geen specifieke dreigingen voor. De onderzoeken waren:

- Data Privacy Impact Assessment voor de applicaties Boomerweb en ONS;
- Onderzoek naar Follow me pro printing;
- Onderzoek naar veilig mailen;
- Monitoring technische IT infrastructuur;
- Onderzoek naar afsluiten van cyberverzekering, offertes opgevraagd, de definitieve keuze vindt in 2019 plaats;
- Onderzoek naar de omgang met beeldmateriaal wat heeft geresulteerd in het opstellen van een protocol;
- Opstellen van een privacy control framework.

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 2018 geen specifieke beveiligings- en penetratietesten gedaan. De ambitie voor 2019 is om in ieder geval één test te doen. De keuze voor het systeem waarop deze test gedaan wordt, wordt bepaald aan de hand van een risico-analyse.

Controle autorisaties

Er worden periodieke controles uitgevoerd. In 2018 is een matrix ontwikkeld waarbij per medewerker inzichtelijk is welke autorisatie hij heeft in de verschillende systemen. De functioneel beheerders controleren aan de hand van deze lijst periodiek 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. In 2019 wordt deze controle verder geautomatiseerd.

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. Hiernaast heeft Riwis een tool zelf 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 2019 willen we kijken of deze informatie volledig en juist is vastgelegd.

6. 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 2018 zijn er in totaal 45 datalekken gemeld binnen de onderstaande categorieën:

Oorzaak datalek	Aantal
Registratie persoonsgegevens bij verkeerde cliënt / medewerker in digitaal systeem Riwis	31
Persoonsgegevens verstuurd naar verkeerd adres buiten Riwis	3
Onrechtmatige ontvangst van persoonsgegevens	2
Verlies of diefstal van dossier / laptop / telefoon / USB-stick of andere gegevensdrager	1
Niet afgesloten gebouw / ruimte / kast / computer / laptop en onrechtmatige toegang tot / plaatsing van persoonsgegevens	4
Overig	4

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

7. Ambitie voor 2019

Riwis heeft voor 2019 de volgende doelstellingen benoemd:
- Vaststellen van het privacy en informatiebeveiligingsbeleid;
- Vaststellen van het datalek protocol;
- Afronden verwerkingsregister 1.0 versie zodat het in het organisch proces kan worden opgenomen;
- Monitoren afsluiten van verwerkingsovereenkomsten;
- Openen eisen vanuit de NEN normen en andere eisen ten aanzien van privacy en informatie-beveiliging in het totale compliance privacy framework;
- Risico analyse op basis van nieuwe NEN normen en het privacy control framework;
- Onderzoeken welke audits op het gebied van privacy en informatiebeveiliging wenselijk zijn aan de hand van de risico-inventarisatie;
- Verhogen bewustzijn gegevensbescherming op werkvloer;
- Afsluiten van een cyberverzekering;
- Uitvoeren DPIA voor alle kernapplicaties die Riwis gebruikt;
- Uitvoeren van een PEN test;
- Automatiseren van de controle op de autorisaties vergroten;
- Controleren of de informatie over applicaties gestructureerd en volledig is vastgelegd.

Bijlage 1: Samenvatting voor bestuursverslag 2018

Riwis Zorg en Welzijn vindt het vanzelfsprekend en van groot belang dat goed wordt omgegaan met privacygevoelige gegevens. Daarbij vindt Riwis het belangrijk dat met de gegevens van een ander wordt omgegaan zoals iedereen zou willen dat er met de eigen persoonsgegevens wordt omgegaan. Dit betekent privacy bewustzijn bij iedere medewerker. Hierbij nemen we de volgende punten mee bij het maken van keuzes:

- Privacy en gegevensbescherming mag de zorg niet in de weg staan
- Evenwicht tussen gebruikersgemak en gegevensbescherming
- Uitgangspunt is vertrouwen in de professionaliteit van de medewerker, er vindt wel controle plaats
- Zorgvuldigheid staat voorop maar het helemaal uitsluiten van datalekken is niet mogelijk.

In snel tempo wordt wetgeving op het gebied van privacy en informatiebeveiliging aangenomen. Aan de hand van de nieuwe wetgeving zijn de doelen aangescherpt. De verantwoording van alle acties van Riwis is te vinden in de verklaring van accountability die op de internetsite van Riwis terug te vinden is. Deze paragraaf is een samenvatting van deze verklaring. De verantwoording wordt gedaan aan de hand van de categorieën: in- en externe wet- en regelgeving, handelen en gedrag en technische en fysieke beveiliging.

<u>In- en externe wet- en regelgeving</u>

Het beleid van Riwis is verwoord in verschillende documenten waar een sterke samenhang tussen bestaat. De volgende documenten maken onderdeel uit van het beleid:

- privacy en informatiebeveiligingsbeleid
- protocol afhandeling datalekken
- privacyreglementen
- autorisatie en authenticatie beleid
- gedragsregels en geheimhoudingsverklaringen

In deze documenten is de vertaling gemaakt vanuit wet- en regelgeving naar de praktijk binnen Riwis. De privacyreglementen worden in 2019 opgesteld. Het privacy en informatiebeveiligingsbeleid en het protocol datalekken worden begin 2019 formeel vastgesteld.

Het hart van alle activiteiten rondom privacy & informatiebeveiliging is de privacy en informatiebeveiligingsadministratie. In deze administratie zijn de verwerkingen van persoonsgegevens, de bijbehorende processen en systemen en de technische beveiligingsmaatregelen opgenomen. Ook zijn hierin de organisaties opgenomen waarmee Riwis persoonsgegevens uitwisselt

<u>Handelen en gedrag</u>

Riwis besteedt doorlopend aandacht aan de bewustwording van medewerkers op het onderwerp privacy & informatiebeveiliging. In 2018 is dit onder ander gedaan door privacy bijeenkomsten in teams, een phishing actie en artikelen op intranet.

<u>Technische en fysieke informatiebeveiliging</u>

Er zijn diverse maatregelen genomen om de technische en fysieke informtiebeveiliging te garanderen. Denk hierbij aan controle op autorisaties en monitoring van de technische infrastructuur. Eventuele risico's worden continu gemonitord, hiervoor worden verschillende instrumenten ingezet:

- analyse van datalekken
- onderzoeken naar specifieke vragen en knelpunten
- monitoring van het IT netwerk
- uitvoeren van gegevensbeschermingseffectbeoordelingen (DPIA)

Uit deze onderzoeken en analyses zijn aandachtspunten naar voren gekomen die tot verbetering hebben geleid.

Ambitie 2019

Voor 2019 heeft Riwis de ambitie om de volgende zaken op te pakken:

- Vaststellen van het privacy en informatiebeveiligingsbeleid;
- Vaststellen van het datalek protocol;
- Afronden verwerkingsregister 1.0 versie zodat het in het organisch proces kan worden opgenomen;
- Monitoren afsluiten van verwerkingsovereenkomsten;
- Openen eisen vanuit de NEN normen en andere eisen ten aanzien van privacy en informatie-beveiliging in het totale compliance privacy framework;
- Risico analyse op basis van nieuwe NEN normen en het privacy control framework;
- Onderzoeken welke audits op het gebied van privacy en informatiebeveiliging wenselijk zijn aan de hand van de risico-inventarisatie;
- Verhogen bewustzijn gegevensbescherming op werkvloer;
- Afsluiten van een cyberverzekering;
- Uitvoeren DPIA voor alle kernapplicaties die Riwis gebruikt;
- Uitvoeren van een PEN test;
- Automatiseren van de controle op de autorisaties vergroten;
- Controleren of de informatie over applicaties gestructureerd en volledig is vastgelegd.