Cliënt centraal,
medewerkers weerbaar,
processen op orde.

Veilig digitaal werken binnen de zorg.

FACTOR 50
informatieveiligheid

Philadelphia

In deze brochure beschrijven we de werkzaamheden, die Factor50 informatieveiligheid heeft uitgevoerd bij Philadelphia Zorg

Samen met de mensen van Philadelphia zorg hebben we gewerkt om de organisatie en de processen veilig en Avg-compliant te maken. Tijdens dit traject hebben we de organisatie weerbaar gemaakt voor (digitale) dreigingen. Aan het woord komen verschillende functionarissen van Philadelphia en de projectverantwoordelijken van Factor50. Zij vertellen over hun ervaringen tijdens het traject, vanuit hun eigen verantwoordelijkheden.

De medewerkers van Philadelphia en Factor50 delen hun ervaringen, tips en geleerde lessen

Vanuit Factor50 hebben we ervaren welke spanningsvelden er bestaan tussen zorgverlening, informatieveiligheid en de bescherming van persoonsgegevens van cliënten, medewerkers, naasten en ketenpartners. Samen met Philadelphia hebben we gewerkt aan oplossingen en werkwijzen die passen binnen het zorgproces en bij de organisatiecultuur. Zo hebben we een proces opgezet voor het behandelen van meldingen, incidenten en datalekken.

Philadelphia stelt ons in de gelegenheid deze kennis ook in uw organisatie toe te passen. We nodigen u van harte uit voor een gesprek over informatiebeveiliging en het weerbaar maken van uw organisatie.

Jeroen Wittink - Ton Oosterwijk

Jeroen Wittink
Jeroen@Factor50.eu
06 52 64 39 08

Ton Oosterwijk
Ton@Factor50.eu
06 50 40 48 44

Philadelphia aan het woord

"Het heeft ons rust gebracht, omdat we het gevoel hebben AVG-proof te zijn nu. Dat is inmiddels ook feitelijk uit de audits naar voren gekomen: er is grip op het proces."

Siem van den Broek
Secretaris Raad van Bestuur en directeur bestuurlijke en juridische zaken

"Ze zijn heel goed bekend met de materie, begrijpen de AVG tot in detail en kunnen zowel op management- als praktijkniveau met je meedenken van eenvoudige tot complexe of hoog risicovolle privacygevoelige kwesties en kwetsbaarheden in de organisatie."

Mette Dekhuijzen
Security Officer

"En dat alles bij elkaar maakte dit proces tot een ware ontdekkingsreis die mede door Factor50 in gang is gezet en dankzij hen echt betekenis heeft voor de manier waarop wij werken aan onze missie."

Jeroen Zomerplaag
Manager, adviseur en expert in de langdurende zorg

FACTOR 50
informatieveiligheid

Factor50 is een metafoor. Een metafoor voor de manier waarop we naar informatie kijken. Organisaties hebben informatie nodig, net zoals mensen de zon. Het gebruik van deze informatie brengt ook risico's met zich mee. Maar dit is geen reden voor paniek, zolang de organisatie zich maar passend beschermd.

Méér is hierbij niet beter. De noodzakelijke maatregelen verschillen per organisatie en branche, vergelijkbaar met huidtypes en blootstelling aan de zon. Soms is insmeren afdoende. In andere situaties is het noodzakelijk om beschermende kleding te dragen of helemaal uit de zon te blijven.

Samen met u stellen we een afgewogen pakket van maatregelen vast. Deze zijn altijd toegespitst op uw specifieke situatie en organisatie. Hiermee helpt Factor50 u, de bescherming van uw waardevolle informatie op het juist niveau te brengen en te houden.

Van een onzekere organisatie naar een weerbare organisatie.

" Filadelfia komt van het Griekse Philadelpheia, het woord staat van oudsher voor

Over Philadelphia

Philadelphia ondersteunt door heel Nederland heen zo'n 8.200 mensen met een beperking. Dit doen ze vanuit één centraal servicekantoor en 530 kleinschalige zorglocaties, van waaruit professionals voor ondersteuning op maat zorgen. Het gaat dan om ondersteuning van mensen die bij een locatie van Philadelphia inwonen, intensieve zorg krijgen en/of gebruikmaken van ambulante begeleiding. Philadelphia helpt mensen om het beste uit zichzelf te halen, talenten te ontdekken en hun dag zinvol in willen in te vullen.

De professionals van Philadelphia werken op hun beurt weer samen met zorgaanbieders, vrijwilligersorganisaties, gemeenten, overheidsinstellingen, diverse belanghebbenden, en ondernemers uit de omgeving. Men bevindt zich in een dynamisch en met regelmaat uitdagend speelveld. Eén visie hebben de betrokken medewerkers in elk geval gemeen: men kijkt vooral naar mogelijkheden en kansen. Die positieve blik is de basis voor de zorgvisie die met liefde en aandacht voor élke cliënt wordt opgesteld.

Philadelphia over het project

In 5 vragen informeerden we bij functionarissen uit verschillende lagen binnen Philadelphia naar de mate van tevredenheid over de begeleiding. Deze aanpak waarin we de opdrachtgever zelf het verhaal laten vertellen, vinden we waardevol omdat ieder vanuit zijn eigen praktijk kijkt naar hoe Factor50 informatieveiligheid geholpen heeft. De één kijkt op strategisch niveau vanuit een bestuursfunctie, de volgende beoordeelt de samenwerking meer vanuit een security-visie en de ander, tot slot, praat vanuit een managersrol waarbij geacteerd wordt op het snijvlak van praktijk en beleid.

broederlijke liefde. „

In 5 vragen...

Siem van den Broek,

secretaris Raad van Bestuur en directeur bestuurlijke en juridische zaken vertelt:

1. Wat is het grootste verschil in jullie werkwijze sinds Factor50 geholpen heeft?

'Het eerste contact met Ton was via een telefoontje waarin hij een directe collega van mij, vanuit zijn persoonlijke ervaring, wees op een bepaalde aanpak die we beter konden doen. Daar was ik van onder de indruk, dat iemand de moeite nam om dit te melden door gewoon pragmatisch de telefoon te pakken en in alle openheid positief-kritische feedback te geven.

Dit contactmoment viel toevallig net samen met de ontwikkelingen rondom de AVG en wij konden wel wat hulp gebruiken bij het juist implementeren van deze nieuwe Europese regelgeving.

Ten tweede wilden we binnen onze organisatie meer awareness creëren, ook met het oog op de almaar voortschrijdende technologieën. We realiseren ons terdege dat het afsluiten van een kast met daarin papieren dossiers allang niet meer van deze tijd is, en dat we juist ook in het digitale veld slagen moesten maken.

Tot slot, je zou het de derde pijler kunnen noemen, wilden we de manier waarop we onze informatie beveiligden weer eens tegen het licht houden. We hadden zelf al een traject opgezet, waarbij we intern Security Functionarissen hadden benoemd. Factor50 is erin geslaagd om informatieveiligheid en privacy naadloos samen te brengen.'

2. Hoe heeft Factor50 dit aangepakt?

'Uiteindelijk is het een groot en langlopend project van een jaar geworden, waar we op inhoudelijk vlak vanzelfsprekend nog altijd mee bezig zijn. Feitelijk rollen we de strategie van destijds steeds verder uit. Zo hebben we bijvoorbeeld een Privacy Officer aangesteld die als eerste aanspreekpunt fungeert en twaalf functionarissen door het hele land die voor een gedeelte van een werktijd vrijgespeeld zijn voor de AVG, privacy en alles wat daarmee samenhangt.

Eigenlijk kan ik het samenvatten door te zeggen dat Factor50 een groot project in overzichtelijke stukken aan ons heeft aangeboden en ons daar op alle lagen binnen de organisatie zowel praktisch als vanuit een theoretisch kader in hebben begeleid.
Ze kwamen niet met een kant-en-klare oplossing, maar hebben zich eerst verdiept in onze organisatie. En ze gaven ook direct van die praktische tips, bijvoorbeeld over de vervanging van oude printers. Of we er wel aan dachten dat er veel privacygevoelige informatie achter blijft in het geheugen van deze kolossen... Bij het gros van de bedrijven gaat dat nog altijd zó de deur uit, zonder dat de (soms gevoelige) achterblijvende informatie gewist wordt.'

3. Welke van je taken zijn concreet veranderd/ aangescherpt sinds Ton en Jeroen jullie geholpen hebben?

'Door het inrichten van goede, werkbare processen over incidentmanagement, maar ook door actief met medewerkers over hun gedrag te spreken, zijn we organisatiebreed weerbaar geworden. En dat was zonder de hulp van Ton en Jeroen niet gelukt. We zien deze weerbaarheid en de manier waarop we alle belangrijke thema's vorm hebben gegeven, uitgerold en geborgd, inmiddels als een belangrijk asset, een USP eigenlijk, van onze organisatie. Wat overigens ook opviel was de warme manier waarop er met mensen gesproken werd. Ik geloof niet dat er iemand is die zich niet serieus genomen of behandeld voelde met het welbekende opgeheven vingertje. Het was meer zo'n houding vanuit Factor50 van 'oké, als dat jouw probleem is, dan kijken we daar samen naar en dan gaan we het zó oplossen dat er recht wordt gedaan aan de privacyregels, terwijl het nog wel werkbaar blijft.'

Ton en Jeroen zijn letterlijk met ons op pad gegaan, ze stonden open voor ons, bewogen mee in onze wensen, verdiepten zich in het DNA van de organisatie en maakten de verstaalslag naar wet- en regelgeving. Het heeft ons rust gebracht, omdat we het gevoel hebben AVG-proof te zijn nu. Dat is inmiddels ook feitelijk uit de audits naar voren gekomen: er is grip op het proces. Natuurlijk kunnen er altijd nog zaken beter, maar dat blijft, het is een lerend proces.'

"Ze kwamen niet met een kant-en-klare oplossing, maar hebben zich eerst verdiept in onze organisatie."

4. Wat kun je anderen aanraden rondom het compliant worden aan de AVG en privacy?

'Het is en blijft een actueel onderwerp dat niet meer weg te denken is uit onze steeds digitaler wordende maatschappij. Om me heen hoor en zie ik dat grote bedrijven volop maatregelen nemen om de privacy van gegevens te waarborgen. Wat mij betreft blijft de menselijke kant van het hele verhaal toch de grootste impact hebben. Je zult echt moeten investeren in houding en gedrag, want het menselijk bewustzijn over 'hoe het zou moeten' blijkt niet altijd overeen te komen met de concrete handeling die daarbij uitgevoerd wordt. We kennen allemaal wel het voorbeeld van die link waarvan je, als je logisch nadenkt, weet dat je er niet op moet klikken. Maar de mens is nieuwsgierig en dan wordt er tóch geklikt. Het gevolg laat zich raden: met een beetje pech liggen vervolgens gevoelige gegevens op straat, bijvoorbeeld door een virus of geslaagde hackaanval. Dat soort handelingen is niet in een proces te vatten, de mens blijkt, ondanks alle regels en afspraken, in praktijk toch de zwakste schakel te zijn. Daarom raad ik anderen aan om vooral het awareness-gedeelte voor de medewerkers veel tijd en aandacht te geven.'

5. Zou je Factor50 aanraden en zo ja, waarom?

'Zeker. Ik weet nog goed dat ik me na het eerste gesprek met Ton ten volle bewust werd, van hetgeen er op onze organisatie af ging komen. De impact van de regelgeving rondom privacy, AVG, informatieveiligheid, datalekken, incidentmanagement en meer van die thema's is echt veel groter dan je in eerste instantie wellicht denkt. Factor50 heeft ons, en vergeef me het containerbegrip, ontzorgd. Ton en Jeroen, zagen het totaalplaatje, hadden een planmatige aanpak en hadden beiden, elk vanuit hun eigen karakter en persoonlijkheid, de kracht om met elke collega, op elk niveau zo te schakelen dat iedereen zich serieus genomen voelde. Daardoor werden weerstanden overwonnen, gingen neuzen dezelfde kant op en werd er meer en meer verantwoordelijkheid genomen en gevoeld binnen de organisatie.

En nog altijd zijn ze meer dan bereid tot meedenken en hebben ze me, gedurende het project verbaasd, omdat ze zo snel hun weg wisten te vinden in onze grote organisatie. Vragen die we hadden, of onderwerpen waar we over wilden sparren konden we op allerlei manier voorleggen, via e-mail, door te bellen en zelfs gewoon door een appje te sturen, waar dan weer snel op gereageerd werd. Factor50 heeft de theoretische kennis op orde, is sterk in conceptueel denken, maar ook in staat om praktisch aan de slag te gaan. Ton en Jeroen zijn fysiek door het land gereisd en hebben met veel medewerkers gesprekken gevoerd. Dat kom je niet zoveel tegen, dat adviseurs zowel op managementniveau als operationeel zó goed kunnen schakelen en afstemmen op het doel.

Tot slot raad ik bedrijven, die een soortgelijk traject uit willen rollen, aan om vooraf goed hun huiswerk te doen, door een afgewogen plan van aanpak te maken. Dat helpt echt om doelen sneller te bereiken.'

> *"Ton en Jeroen, zagen het totaalplaatje, hadden een planmatige aanpak."*

In 5 vragen...

Mette Dekhuijzen,

Security Officer vertelt:

1. Wat is het grootste verschil in jullie werkwijze sinds Factor50 geholpen heeft?

'Het onderwerp AVG en de uitvoering hiervan is in een organisatie als Philadelphia erg omvangrijk. Er is niet één groot verschil te noemen. Factor50 heeft heel veel werk verricht in het opzetten van de verwerkersovereenkomsten, van processen en van andere AVG-gerelateerde vraagstukken. Het gaat vooral ook om de hoeveelheid werk die ze hebben opgeleverd,

> *Ze denken mee met iedereen op alle niveaus in de organisatie: een manager heeft immers andere uitdagingen dan een medewerker die met problematiek op de werkvloer te maken krijgt.*

waardoor er nu over de gehele linie AVG-onderwerpen zijn opgepakt en geborgd, en processen zijn ingericht in de organisatie.

Zelf ben ik verantwoordelijk voor de informatiebeveiliging binnen Philadelphia. Denk aan informatie die zowel digitaal als fysiek veilig wordt bewaard, behandeld en verwerkt. Ik kijk naar informatiebeveiliging binnen en buiten de ICT-infrastructuur van Philadelphia, waarbij ik speciaal oog heb voor de risico's die gelopen worden en hoe we deze kunnen voorkomen door continu te verbeteren. Dat betekent enerzijds sturen op processen en technologie en anderzijds vooral op de werkwijze ofwel het menselijk handelen. Kennis bijbrengen is één ding, maar het menselijk gedrag veranderen is minstens net zo belangrijk.

In eerste instantie viel het werkgebied van de AVG ook onder mijn hoede, maar daar hebben we inmiddels iemand voor aangetrokken, een Privacy Officer. De AVG doe je er immers niet zomaar even bij, dat is een baan op zich binnen een organisatie met deze omvang. Als je dat goed wilt doen, tenminste. Er zit wel overlap met mijn functie, dus we werken nauw met elkaar samen.'

2. Hoe heeft Factor50 dit aangepakt?

'Ze zijn vooral de organisatie ingegaan en hebben vanuit verschillende kanten alle werkzaamheden bekeken, uitgeplozen en besproken. Ton en Jeroen zijn het gesprek aangegaan met zowel directie, managers als met medewerkers op de werkvloer die direct bij het zorgproces van de cliënt zijn betrokken. Ze denken mee met iedereen op alle niveaus in de organisatie: een manager heeft immers andere uitdagingen dan een medewerker die met problematiek op de werkvloer te maken krijgt. Factor50 wist hen goed te faciliteren in de AVG-onderwerpen wat ze nodig hadden.'

3. Welke van je taken zijn concreet veranderd/ aangescherpt sinds Ton en Jeroen jullie geholpen hebben?

'We kiezen nog steeds voor finetunen en maken af waar Factor50 al mee bezig was. Gezien de omvang van onze organisatie en de impact van het onderwerp, was het werk niet klaar toen het project ophield. En dat hoeft ook niet, het is een onderwerp dat continu aandacht blijft vergen. Al is het alleen al omdat we ruim 530 locaties verdeeld over heel Nederland hebben. Kortom, we zijn nog altijd volop met informatiebeveiliging en privacy bezig, ook in combinatie met de ISO 27001-certificering voor informatiebeveiliging, waar privacy een belangrijk aandeel in heeft.

Het is en blijft nog een uitdaging om AVG goed uit te zetten. AVG is niet iets 'van het hoofdkantoor', AVG raakt juist ook de werkvloer, omdat er met veel gevoelige gegevens gewerkt wordt. Het is een kunst

om aansluiting te vinden tussen de theorie en de praktijk. Ton en Jeroen hebben zich daartoe goed in staat getoond, door levendige voorbeelden uit de praktijk te geven tijdens de bewustwordingssessies, maar ook door vragen uit de organisatie te beantwoorden.
Het ging dan vaak om vragen die complex of lastig waren.
AVG staat vaak dichterbij jezelf dan dat je denkt; zou jij een brief met medische gegevens in de huiskamer van Philadelphia laten liggen waar iedereen naar binnen loopt? Of een lijstje met jouw medische gegevens op de muur hangen bij Philadelphia? Dat zou je zelf ook niet prettig vinden, dus cliënten ook niet. Door op die manier met elkaar over de materie te spreken verhoogde het bewustzijn enorm.'

4. Wat kun je anderen aanraden rondom het compliant worden aan de AVG en privacy?

'Je kunt dit vanuit verschillende kanten aanvliegen; enerzijds vergen de onderwerp AVG, informatiebeveiliging en privacy in grote organisaties een planmatige aanpak, zodat je bewust begint met het aanpakken van de grootste privacy-risico's. Op die manier weet je immers ook binnen afzienbare tijd voldoende medewerkers te bereiken dankzij de planmatige aanpak. Anderzijds, in de uitvoering, zou je juist klein moeten beginnen door het bij jezelf te houden, bij de medewerker die dagelijks direct in het zorgproces met de cliënt werkt. Als het gaat om bewustwording; begin klein en praktisch. Wanneer je te hoog over begint, dan raak je de mensen binnen je bedrijf kwijt en krijg je de neuzen niet gemakkelijk dezelfde kant op. Laat je collega's ook echt ervaren wat het voor hun dagelijkse praktijk betekent. Het onderwerp AVG is breed; aandacht voor privacy, verwerkersovereenkomsten, data, informatiebeveiliging en aanverwante zaken. Houd het verder ook dichtbij je zelf en vraag

> *"Laat je collega's ook echt ervaren wat het voor hun dagelijkse praktijk betekent."*

je af hoe je je team kunt raken zodat ze echt vanuit een awareness-gerichte houding gaan beseffen waar de risico's en kwetsbaarheden liggen.

Wanneer je dat goed voor elkaar hebt, en je je dus hebt ingeleefd in je doelgroep, dan ontstaan er zomaar levendige discussie en raken mensen intrinsiek geïnteresseerd en gemotiveerd om het anders, veiliger of beter te gaan doen. Leg ook praktisch uit wat bijvoorbeeld een datalek is en houd het interactief, zodat mensen als vanzelf actief meedoen en -denken. Het ergste wat je kan gebeuren is dat je zo'n training geeft, waarbij iedereen murw van het luisteren met een schuin oog op de klok kijkt of na afloop zegt dat het iets voor de service organisatie of het management is. Dat is natuurlijk niet zo; de AVG wetgeving raakt iedereen, of je het nu wilt of niet.

5. Zou je Factor50 aanraden en zo ja, waarom?

'Ja, absoluut. Ze zijn heel goed bekend met de materie, begrijpen de AVG tot in detail en kunnen zowel op management- als praktijkniveau met je meedenken van eenvoudige tot complexe of hoog risicovolle privacygevoelige kwesties en kwetsbaarheden in de organisatie.

Ton en Jeroen zijn zowel als team als in een individuele setting, heel toegankelijk. Hun aanpak is praktisch en pragmatisch. Ze zijn goed benaderbaar en open en transparant waar mogelijk. Hierdoor ervaar ik de samenwerking met hen als bijzonder prettig en plezierig. Er was een zakelijke klik. Dat maakte het samenwerken gemakkelijk en ik heb er energie van gekregen. Dat heb ik als erg prettig ervaren, ook omdat ik heb ervaren dat het in de praktijk weleens anders kan zijn met adviseurs of consultants. Ik kan anderen Factor50 dan ook aanbevelen.

In 5 vragen...

Jeroen Zomerplaag,

manager, adviseur en expert in de langdurende zorg vertelt:

1. Wat is het grootste verschil in jullie werkwijze sinds Factor50 geholpen heeft?

'Dat is een lastige vraag, want je weet natuurlijk niet wat er gebeurd was als Factor50 er niet was geweest. Wat ik wel heb gezien is dat Philadelphia, net als alle andere organisaties, geconfronteerd werd met de AVG. Onze eerste impuls was om tal van administratieve en beleidsmatige uitdagingen te gaan regelen. Wat Factor50 heeft gedaan is verbinding zoeken met de praktijk. En dan niet zozeer kijkend naar de invalshoek van hoe regelen we de administratie, hoe stellen we het beleid op en hoe richten we de systemen in, maar veel meer vanuit onze medewerkers. Het idee was dat we onze mensen zó in hun kracht konden zetten, dat ze vanuit zorgvuldigheid naar onze cliënten toe op een adequate manier met de aangescherpte privacyregels om wisten te gaan.'

'Aanvankelijk begonnen zij zoals elke AVG-adviseur dat zou doen,

> *Daar konden we dan weer over praten samen, en mede daardoor werden theorie en praktijk zo optimaal mogelijk aan elkaar gekoppeld.*

door te infomeren over welke ingrijpende veranderingen er op ons af zouden komen. Daarbij onderstreepten ze ook dat er tal van partijen zijn die belang hebben bij het hacken van (gevoelige) informatie en dat we onze cliënten en onszelf daar actief tegen dienden te beschermen. Ook werd benadrukt dat er relatief eenvoudig gegevens op straat konden komen te liggen door onachtzaamheid van medewerkers.'

'Wat ik bijzonder vond was dat ze ook oog hadden voor wat deze aangescherpte werkwijze voor medewerkers betekent. Ton en Jeroen waren uitstekend in staat om zowel verbale als non-verbale signalen feilloos op te pikken, serieus te nemen en te bespreken met de betrokken persoon of personen. Ze lieten in hun hele doen en laten merken dat ze het als een gezamenlijke opgave zagen om dit project tot een succes te maken. Ze hebben onze medewerkers geholpen om op een adequate manier om te leren gaan met informatiebeveiliging enerzijds, maar anderzijds ook met de drang het allemaal goed te willen regelen en zaken vast te leggen in procedures, om te voorkomen dat je in de fout gaat.'

'Ik heb veel met hen gesproken over het veld waarin ik opereer, dat zich bevindt op het snijvlak tussen praktijk en beleid. Dit waren open gesprekken en Ton en Jeroen toonden zich dikwijls oprecht verwonderd over waar medewerkers mee te maken kunnen krijgen in hun dagelijkse praktijk. Daar konden we dan weer over praten samen, en mede daardoor werden theorie en praktijk zo optimaal mogelijk aan elkaar gekoppeld. Vragen als: "Hoe ga je om met bepaalde informatie en hoe beïnvloedt dat dan de vertrouwensrelatie met je cliënten?", liggen in principe buiten de context van de AVG, maar hebben wel degelijk impact.

We zochten, in verschillende samenstellingen, continu naar een werkbare oplossing die toch aan de regels zou voldoen.'

2. Hoe heeft Factor50 dit aangepakt?

'Ze zijn begonnen met het geven van presentaties, waarbij ze ook onze grote organisatie zorgvuldig onder de loep hebben genomen, bijvoorbeeld door te onderzoeken wie welke rol en belangen heeft. Het hele traject is uiteindelijk echt wel een maatwerkverhaal geworden.'
'Toen die basis er eenmaal lag zijn er allerlei overleggen en bijeenkomsten georganiseerd om met elkaar oplossingen voor de uitdagingen te vinden. Voor een deel waren Ton en Jeroen ook faciliterend, fungeerden ze als gespreksleiders, nodigden ze mensen uit, gaven ze het doel van de bijeenkomst aan, inventariseerden ze wie bij welk onderwerp aan moest sluiten, maakten ze verslagen, regelden ze afspraken, en bewaakten steeds wat de volgende stap moest zijn. Lang verhaal kort: ze hebben de organisatie écht en intrinsiek in beweging gekregen om verdere invulling te geven aan ons te voeren beleid.'

3. Welke van je taken zijn concreet veranderd/ aangescherpt sinds Ton en Jeroen jullie geholpen hebben?

'In mijn dagelijkse praktijk bestaat mijn rol vooral uit sparringpartner zijn voor de directieleden, de managers en de medewerkers voor zorginhoudelijke taken. En ook informatiebeveiliging zou daarbij moeten horen, en dat was, op dit nieuwe niveau in elk geval, iets nieuws. Factor50 heeft mij geholpen om informatieveiligheid een integraal onderdeel van de organisatie te laten zijn.'

'Door de manier waarop ik met hen heb kunnen samenwerken en door het vinden van een oplossing voor vraagstukken, kan ik diezelfde informatieveiligheid nu integraal betrekken op mijn andere verantwoordelijkheden. Informatieveiligheid is nu beter verbonden met zorginhoudelijke vragen en het kwaliteitsbeleid. Ik kan daardoor nu bijvoorbeeld veel beter uitleggen waarom het belangrijk is om aandacht te besteden aan informatiebeveiliging en waarom dit binnen Philadelphia op de gekozen manier ingevuld is. Het maakt mijn werk plezieriger en ik merk ook dat er door de gehele organisatie heen een sfeer van intrinsieke motivatie en scherp bewustzijn rondom dit thema hangt.'

4. Wat kun je anderen aanraden rondom het compliant worden aan de AVG en privacy?

'In elk geval dat je de AVG en privacy écht verbindt aan de missie en de doelen van je organisatie. Informatieveiligheid is uiteraard geen doel op zich, maar een belangrijk ondersteunend middel. In onze situatie gaat dat over onze vaak kwetsbare mensen die we graag willen helpen om zo zelfredzaam mogelijk invulling te geven aan hun eigen leven.'

5. Zou je Factor50 aanraden en zo ja, waarom?

'Ik zou ze zeker aanraden, vooral omdat ze, in tegenstelling tot veel andere adviseurs, niet meteen in de weer gingen met processen en procedures waarmee we konden voldoen aan de regels. Ze zijn juist eerst gestart met luisteren naar wat er in de organisatie speelt, om zich vervolgens op verschillende niveaus te verdiepen door met de medewerkers te praten. Ton en Jeroen stelden zich echt open, waren heel transparant in alles wat ze deden en waren ook in staat tot zelfreflectie. En dat alles bij elkaar maakte dit proces tot een ware ontdekkingsreis die mede door Factor50 in gang is gezet en dankzij hen echt betekenis heeft voor de manier waarop wij werken aan onze missie.'

"En dat alles bij elkaar maakte dit proces tot een ware ontdekkingsreis die mede door Factor50 in gang is gezet en dankzij hen echt betekenis heeft voor de manier waarop wij werken aan onze missie."

Onze aanpak & werkwijze

‘Philadelphia verwerkt in grote mate bijzondere persoonsgegevens, vanzelfsprekend medische gegevens van kwetsbare groepen mensen, maar ook persoonsgegevens van medewerkers, stagiaires en belanghebbenden.’ Aan het woord zijn Ton Oosterwijk en Jeroen Wittink, oprichters van Factor50. ‘Philadelphia heeft ons, na een eerste telefonisch contact vanuit Ton’s zijde ingeschakeld om te werken conform de AVG. Men verzocht ons concreet om begeleiding te bieden bij het opstellen van registers van verwerkingen, de inrichting van processen en de resultaten daarvan te borgen. Dit allemaal rondom de thema’s zoals verwerkersovereenkomsten, gegevensbescherming, incidenten en datalekken. Voorlichting geven aan de hele organisatie over veilig digitaal werken en de verplichtingen onder de AVG en het opzetten van Vraag & Antwoord hoorden bij onze taak. In praktijk ging dat om de centrale serviceorganisatie, maar ook om het betrekken van bestuurders en servicedeskmedewerkers en van beleidsmedewerkers tot mensen die op de locaties zelf werken, zoals locatiemanagers en -begeleiders. Ook wilden we met elkaar de weerbaarheid van de organisatie verhogen, risico’s in kaart brengen, tegenmaatregelen voorstellen, de verschillende functionarissen opleiden en actief ondersteunen bij het inrichten van de governance. Tot slot zijn de resultaten, komend uit dit project, geïntegreerd en geborgd in het ISO 27001-traject.’

Actieve training van mensen in hun rol

‘Wat we, meer vanuit bredere zin bezien hebben gedaan, is een constructieve sfeer creëren rondom taken die niet tot de primaire taak van de meeste (zorg)medewerkers behoren. Ik doel dan op compliant zijn aan de AVG en op een bewuste- en veilige manier digitaal werken. Men wéét wel dat het belangrijk is, maar vindt het tegelijkertijd ook hinderlijk, vervelend en soms zelfs overbodig om hiermee te moeten dealen. Kijk, je kunt volop processen inrichten en procedures schrijven, maar als de neuzen niet dezelfde kant op staan, dan bereik je uiteindelijk weinig’, vervolgt Ton. ‘En daarom hebben we eerst volop aandacht gegeven aan de beleving intern en reageerden we actief op (soms kritische of bezorgde) uitingen van mensen door het gesprek met ze aan te gaan.’

Positieve feedback door concrete voorbeelden

‘We zijn gestart met het geven van voorlichting aan grote delen van de organisatie. Dat deden we op een actieve manier, in de vorm van interactieve sessies en werkvergaderingen. Het leverde ons veel positieve feedback op over onze aanpak, de concrete voorbeelden die we gaven en de stijl van werken’, vult Jeroen Wittink aan.
‘Ook werd er waardering uitgesproken voor de concrete voorbeelden die we benoemden en vervolgens direct koppelden aan de dagelijkse werkpraktijk. We hebben een structuur opgezet waarbij we per afdeling aandachtsfunctionarissen hebben benoemd. Deze zijn ingepast in de bestaande structuur van Philadelphia. Binnen deze structuur zijn de mensen actief getraind binnen hun rol, zodat ze deze ook daadwerkelijk actief op konden pakken. Verder zijn de security functionarissen uit de regio opgeleid, intrinsiek in hun kracht gezet en gepositioneerd.’

Processen in begrijpelijke taal

Ton vervolgt: ‘Ook tijdens het inrichten van het proces hebben we nauw met de mensen zelf samengewerkt. Bijvoorbeeld door veel

gestelde vragen een plaats te geven, met elkaar na te denken over de vindbaarheid van relevante informatie op het intranet en samen stil te staan bij de leesbaarheid van het proces zelf. Ton: 'Wanneer een proces in begrijpelijke taal, met herkenbare voorbeelden wordt geschreven dan staan mensen immers als vanzelf meer open voor het toepassen ervan. Dat is ook de reden waarom we privacy en informatie tot onderdeel van en verankerd hebben in de verschillende processen. Denk dan aan het inkoop-, change- en het HR-proces en aan het intakeproces van applicaties. Uiteraard hebben we ook afdelingen en clusters actief bij elkaar gebracht om gezamenlijk afdelings- en clusteroverschrijdende processen op te pakken.'

Risicogebaseerde aanpak van privacy en informatieveiligheid

'Verder hebben we ook grondig stilgestaan bij (en soms zelfs een beetje gestreden voor) een risicogebaseerde kijk op privacy en informatieveiligheid, uitgaand van reële risico's. We voeren verschillende risicoanalyses uit op het gebied van privacy en informatieveiligheid in de vorm van DPIA's, voluit Data Protection Impact Assessments genoemd. Ook hiervoor hebben we een helder proces ingeregeld', aldus Jeroen. 'Aanvullend hebben we geholpen bij het verbeteren van de verbinding, en dus de samenwerking, tussen de centrale serviceorganisatie in Amersfoort en de vestigingen in het land. Dit deden we door de vestigingen fysiek te bezoeken, voorlichting te geven aan de zorgclusters en door het actief trainen van de security functionarissen, de security officers en de functionaris gegevensbescherming. Daarnaast hebben we een stevige basis gelegd voor een administratie die voldoet aan de AVG. Dit gaven we vorm door de registers van verwerkingen op te stellen, processen gericht op de AVG te beschrijven en templates voor onder meer DPIA's in te richten. We hebben in kaart gebracht hoe men communiceert over risico's en deze vervolgens behandeld. Ook hebben we met elkaar gekeken naar de processen die borgen dat de administratie op orde

blijft. Hierbij hoort het actief ondersteunen van verschillende rollen binnen de organisatie, zoals de Information Security Officer, de Security Functionarissen en de Functionaris Gegevensbescherming.'

Omgaan met meldingen, Incidenten en datalekken

'We hebben een proces opgezet voor het behandelen van datalekken en andere incidenten. Uiteraard is dit proces tot in detail geïntegreerd in de bestaande processen rondom crisis- en incidentmanagement. Onderdeel hiervan was het ontwerpen van een plan van aanpak met daarin de te nemen processtappen en de wijzigingen die in applicaties aangebracht moesten worden. De risico's en de KPI's per processtap zijn concreet beschreven en vormgegeven. Door verschillende afdelingen bij elkaar te brengen en actief het gesprek aan te gaan, hebben we iedereen op één lijn gekregen. We hebben ook aansluiting gevonden bij het primaire zorgproces.'

Tot slot...

Complimenten voor de betrokken medewerkers zijn hierin zeker op zijn plaats, want dit soort trajecten kun je alleen sámen tot een succes maken. Reeds lopende risico's zijn opgepakt en correct en voortvarend behandeld. We hebben ondersteuning geboden bij het omgaan met toezichthouders, betrokkenen en andere partijen. Ook hebben we proactief geadviseerd over het omgaan met (de data) van andere belanghebbenden, zoals familieleden, naasten en officiële organen, zoals de betrokken familieraad en de OR', besluit Ton.

Specifieke kennis vereist

Een project zoals dit vereist specifieke kennis, inlevingsvermogen, communicatieve vaardigheden en bovendien praktijkervaring binnen de zorg.

Samen met u stellen we een afgewogen pakket van maatregelen vast. Deze zijn altijd toegespitst op uw specifieke situatie en organisatie. Hiermee helpt Factor50 u, de bescherming van uw waardevolle informatie op het juist niveau te brengen en te houden.

Neem contact op

We nodigen u van harte uit voor een gesprek over informatiebeveiliging en het weerbaar maken van uw organisatie.

Jeroen Wittink CISM, CRISC, CIPP/E, CIPM
Jeroen@Factor50.eu
06 52 64 39 08

Ton Oosterwijk
Ton@Factor50.eu
06 50 40 48 44

Adres
Zijlweg 148b, 2015 BJ Haarlem

Telefoon
085 800 02 45

E-mail
contact@factor50.eu

Internet
www.factor50.eu

FACTOR 50
informatieveiligheid