Complan Valens bv
Informatiebeveiliging en Privacy beleid

Datum: 7 april 2018

Versie: 18.04.001

Document	Informatiebeveiliging en privacy beleid 18.04.001.docx
Eigenaar	PSM de Jong
Classificatie	(3) vertrouwelijk
Status	definitief

Datum	versie	changes	Auteur
12-06-2017	2.0	Definitief	PSM
07-04-2018	18.04.001	Aanpassingen & afstemingen nav interne audit	

MANAGEMENT SECURITY STATEMENT

Informatie is overal. Het is overal om ons heen te vinden: op ons bureau, op ons computerscherm. We zijn als dienstverlener continu bezig met het verzamelen, bewerken, creëren en het verspreiden van informatie. Het betreft informatie over Complan Valens bv, maar voornamelijk informatie over onze klanten en zijn/haar patiënten.

Informatieverwerking beschrijft in één woord al onze activiteiten. Complan Valens bv is hierdoor sterk afhankelijk van informatie en de informatieverwerkende systemen. Deze componenten staan voortdurend bloot aan dreigingen zoals storingen, fouten, beschadigingen, en verlies. De gevolgen kunnen desastreus zijn voor Complan Valens bv en haar klanten. Om de continuïteit van onze onderneming te kunnen blijven waarborgen moet Complan Valens bv zich als collectief inspannen voor de beveiliging van informatie en informatieverwerkende systemen.

Complan Valens bv stelt zich ten doel optimale dienstverlening te bieden aan onze klanten, waarbij inspanningen ter behoud van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie als vanzelfsprekend worden geacht. De infrastructurele voorzieningen (hardware en software), de organisatie, processen en procedures moeten hierin faciliteren.

Dit betekent dat:

- Complan Valens bv zich inspant om een “veilige” werkomgeving voor de medewerkers te creëren.
- Het management van Complan Valens bv aan de medewerkers handvatten uitreikt voor het beveiligingsbewust handelen.
- Het management van Complan Valens bv periodiek het managementsysteem voor informatiebeveiliging en privacy beoordelen.
- Het management van Complan Valens bv instemmen met de uitvoering van de beleidsuitgangspunten die in dit beleid zijn vastgelegd.
- Medewerkers zich bewust moeten zijn van hun eigen verantwoordelijkheden.

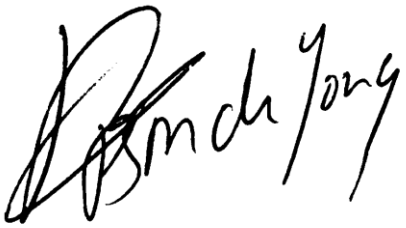
Het informatiebeveiliging en privacy beleid kan worden beschouwd als onderdeel van het Complan Valens bv organisatiebeleid. Het biedt de medewerkers houvast bij de uitvoering van de dagelijkse

werkzaamheden, maar verschaft bovenal duidelijkheid met betrekking tot de algemene en individuele verantwoordelijkheden op het gebied van informatiebeveiliging Risk Management.

Hoogachtend,

PSM de Jong

Directie



INHOUDSOPGAVE

1 DOCUMENTGEGEVENS

1.1 DOCUMENTEIGENSCHAPPEN

Documenteigenschap	
Titel	Complan Valens bv Informatiebeveiliging en Privacy beleid
Onderwerp	Informatiebeveiliging & Privacy
Auteur	PSM de Jong
Document Type	Beleidsrichtlijn
Subtitel	n.v.t.
Versie nummer	18.04.001
Classificatie	vertrouwelijk
Datum	7 april 2018
Eigenaar	PSM de Jong
Autorisatie	
Autorisatie datum	
Status	definitief

1.2 DISTRIBUTIELIJST

Aan	Versie	Datum
Complan Valens bv medewerkers		

2 INLEIDING

Informatiebeveiliging is van toepassing op alle bedrijfsprocessen. Het heeft betrekking op informatie, informatiesystemen, netwerken, de fysieke omgeving en de mensen die de bedrijfsprocessen van Complan Valens bv ondersteunen. Vertrouwen is voor Complan Valens bv de basis om met onze medewerkers, relaties en partners samen te werken. Dit vraagt om openheid van Complan Valens bv en van onze medewerkers over de gegevens die wij van onze medewerkers en klanten vragen.

In dit document wordt het beleid van Complan Valens bv ten aanzien van de bescherming van vertrouwelijkheid, integriteit en beschikbaarheid van haar componenten uiteengezet. Componenten zoals hardware, software en de informatie die door de organisatie wordt verwerkt.

Het beleid dient als richtlijn en/of norm bij het selecteren en implementeren van maatregelen en bij de evaluatie van informatiebeveiliging en privacy. De verantwoordelijkheden en bevoegdheden met betrekking tot informatiebeveiliging zijn vastgelegd in het informatiebeveiliging en privacy handboek.

Het doel van het informatiebeveiliging en privacy beleid is het bieden van sturing en ondersteuning van het management ten behoeve van informatiebeveiliging en privacy aspecten. In dit beleid wordt vastgesteld:

1. in welke richting en binnen welke kaders informatiebeveiliging en privacy dient plaatst te vinden;
2. welke rollen belangrijk zijn in het kader van informatiebeveiliging en privacy;
3. hoe de verantwoordelijkheden voor informatiebeveiliging en privacy zijn belegd.

Het informatiebeveiliging en privacy beleid beschrijft de algemene aanpak van Complan Valens bv op het gebied van informatiebeveiliging en privacy op strategisch niveau. Op lagere niveaus worden meer gedetailleerde beschrijvingen van de aanpak en specifieke beveiligingsmaatregelen gegeven.

De opbouw van dit document is als volgt. In het volgende hoofdstuk wordt ingegaan op informatiebeveiliging en privacy in het algemeen, de doelstelling, reikwijdte en uitgangspunten, etc. Tevens wordt een aantal belangrijke definities gegeven. In hoofdstuk 4 wordt het managementproces beschreven. In hoofdstuk 5 staat de aanpak centraal, gevolgd door het beleid in hoofdstuk 6. Dit beleid wordt afgesloten met het onderdeel kwaliteitsbewaking, dit wordt beschreven in hoofdstuk 7.

3 INFORMATIEBEVEILIGING EN PRIVACY

3.1 DOELSTELLING

De doelstelling van informatiebeveiliging is het waarborgen van de betrouwbaarheid van de informatievoorziening en het verbeteren van de continuïteit van bedrijfsprocessen. Informatiebeveiliging dient de beveiliging van informatieverwerkende componenten van Complan Valens bv te waarborgen. Dit bestaat uit:

- Behoud van beschikbaarheid

  Er voor zorgen dat componenten zoals vereist en wanneer nodig voor de bedrijfsdoelstellingen van Complan Valens bv beschikbaar zijn.

- Behoud van integriteit

  Het beschermen van componenten tegen niet geautoriseerde en/of (on)opzettelijke wijzigingen ten behoeve van de juistheid, volledigheid en inhoudelijke betrouwbaarheid van informatie.

- Behoud van vertrouwelijkheid

  Het beschermen van informatie tegen niet geautoriseerde openbaarmaking.

De doelstelling van privacy is het waarborgen van de beveiliging en de rechtmatige verwerking van de persoonsgegevens van de Complan Valens bv-medewerkers en de Complan Valens bv relaties. Iedereen moet erop kunnen vertrouwen dat zijn persoonsgegevens voldoende worden beveiligd en worden verwerkt voor het doel waarvoor het is verzameld. Slechte beveiliging kan leiden tot een datalek en vervolgens tot misbruik van deze gegevens.

Complan Valens bv stelt zich ten doel optimale dienstverlening te bieden, waarbij inspanningen ter behoud van beschikbaarheid, integriteit en vertrouwelijkheid van informatie als vanzelfsprekend worden geacht. Het behoud van beschikbaarheid, integriteit en vertrouwelijkheid van informatie is onderdeel van de doelstelling om drie redenen:

1. Het voldoen aan wet- en regelgeving. Denk aan de Wet bescherming persoonsgegevens (Wbp), gedragscodes voor medewerkers, auteursrechten, service level agreements (SLA's) en geheimhoudingsverklaringen.

2. Het voldoen aan zakelijke eisen van informatiebeveiliging. Verlies van beschikbaarheid, integriteit en vertrouwelijkheid van informatie leidt direct of indirect altijd tot een kostenpost. Kostenposten zijn niet alleen herstelkosten maar ook imagoschade.

3. Het voldoen aan interne kwaliteitseisen.

Wanneer niet volledig wordt voldaan aan wet- en regelgeving en/of wanneer niet volledig wordt voldaan aan de zakelijke eisen van informatiebeveiliging, loopt Complan Valens bv een risico. Het doel van informatiebeveiliging is niet het elimineren van deze risico's, maar het herkennen van deze risico's, het nemen van maatregelen tegen deze risico's en het accepteren van een bepaald niveau van restrisico.

Informatiebeveiliging verschaft inzicht in beveiligingsrisico's en beveiligingsincidenten. Door maatregelen te implementeren tracht Complan Valens bv het risiconiveau en het aantal incidenten te reduceren. Doel hiervan is het bereiken van een risicobewuste, beheersbare bedrijfsvoering.

3.2 REIKWIJDTE

Dit beleid is van toepassing op alle bedrijfsprocessen, informatiesystemen, netwerken, toepassingen, locaties en medewerkers onder de noemer Complan Valens bv en alle gelieerde werkmaatschappijen.

3.3 DEFINITIES

Component	:	Alles wat voor Complan Valens bv een waarde vertegenwoordigt, in de vorm van fysieke objecten of informatie; synoniem met bedrijfsmiddel en asset.
Beveiligingsstandaard	:	Standaardniveau van beveiliging.
Eigenaar, Eigendom	:	Als er wordt gesproken over eigenaar of eigendom van een component wordt hiermee bedoeld de verantwoordelijkheid voor de werking ervan.
Beschikbaarheid	:	De mate waarin geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot componenten.
Integriteit	:	De mate van correctheid en volledigheid van informatie en informatieverwerking.
Vertrouwelijkheid	:	De mate waarin informatie beschermd moet worden tegen ongeautoriseerde openbaarmaking.
Incident	:	Een gebeurtenis met ongewenste gevolgen; bijvoorbeeld een beveiligingsincident.
Dreiging	:	De kans dat een bepaald incident zich voor doet.

Kwetsbaarheid	:	De verwachte (financiële) impact van een incident.
Risico	:	De combinatie van dreiging en kwetsbaarheid op een bepaalde component.
Restrisico	:	Het risiconiveau dat achterblijft na het nemen van maatregelen; de aanname hierbij is dat risico's, hoe klein ook, altijd blijven bestaan.
Datalek	:	Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.

4 MANAGEMENTSYSTEEM

4.1 MANAGEMENTPROCES

Het managementproces is ingericht op basis van de 'Deming Circle' (Plan – Do – Check – Act). De 'Deming Circle' bevat de volgende aspecten:

- Plan: detectie en inventarisatie van beveiliging- en privacy risico's en het opstellen van maatregelen.
- Do: de implementatie van relevante (nieuwe) maatregelen.
- Check: controleren van de effectiviteit van de geïmplementeerde maatregelen.
- Act: daar waar noodzakelijk bijsturen van het managementproces en de genomen maatregelen.

Voor de opzet van het managementproces hanteert Complan Valens bv het geïntegreerd Management Systeem Governance model van voor Informatiebeveiliging en privacy. Dit model is gebaseerd op de NEN 7510:2011 en de richtsnoeren voor de beveiliging van persoonsgegevens zoals deze zijn opgesteld door de Autoriteit Persoonsgegevens (AP).

4.2 MANAGEMENTVERANTWOORDING

Beheersing van kwaliteit en informatiebeveiliging en privacy aspecten wordt bereikt door een stelsel van organisatorische en technische maatregelen. Deze maatregelen betreffen: een strategisch beleid, richtlijnen, procedures, gedragscodes, werkinstructies, een organisatie en controles. Medewerkers dienen bewust te worden gemaakt van het belang van deze maatregelen en daar waar nodig geïnstrueerd te worden.

Hierbij neemt Complan Valens bv het volgende standpunt in: Complan Valens bv treft al die maatregelen die noodzakelijk en in economische zin rendabel zijn om de veiligheid van de informatie en het personeel te waarborgen, aan de relevante wet- en regelgeving te voldoen, de continuïteit van de bedrijfsvoering te waarborgen en om de reputatie te beschermen.

De directie van Complan Valens bv is verantwoordelijk voor de werking van het managementsysteem en zal via delegatie naar medewerkers de taken en verantwoordelijkheden beleggen voor de implementatie en beheer van maatregelen voortkomend uit dit beleid.

4.3 MEDEWERKERSVERANTWOORDING

Alle medewerkers van Complan Valens bv hebben de verantwoording tot naleving van dit beleid en opvolging van de maatregelen welke voortvloeien uit dit beleid. Identificatie van incidenten of non compliance t.a.v. dit beleid dienen gemeld te worden aan de leidinggevende.

4.4 BEOORDELING EN CORRIGERENDE MAATREGELEN

Complan Valens bv zal de maatregelen welke voortkomen uit dit beleid periodiek controleren middels controles en interne en externe audits t.a.v. (kosten)effectiviteit. Jaarlijks zal de directie het managementsysteem beoordelen op basis van verzamelde gegevens en informatie. Input voor deze beoordeling is o.a.:

- Registratie van incidenten en non-compliance issues
- Registraties van controle, interne en externe audits
- Klanttevredenheidsonderzoeken
- Leveranciersbeoordelingen
- Risicoanalyse output
- Privacy Impact Assessments
- Medewerkerscompetenties
- Bewustwording en training
- Wet- & regelgeving

Op basis van de (tussentijdse) beoordelingen zullen waar mogelijk corrigerende en of preventieve maatregelen worden doorgevoerd. Corrigerende en preventieve maatregelen kunnen ook voortkomen uit overleggen en bijbehorende rapportages. Op een dusdanige wijze dat de kans op herhaling geminimaliseerd wordt. Of waardoor de doeltreffendheid van het managementsysteem wordt verbeterd en het geleverde product of dienst beter aansluit op de eisen van de klant.

4.5 DOCUMENTATIE

4.5.1 Gedocumenteerde informatie

Complan Valens bv draagt zorg voor de verplichte documentatie die binnen de scope van het informatiebeveiliging en privacy managementsysteem vallen. Daarnaast wordt bepaald welke aanvullende documentatie benodigd is om de effectiviteit van het managementsysteem te borgen. Gedocumenteerde informatie kan zich zowel in het managementsysteem als in operationele systemen bevinden.

4.5.2 Classificatie van gegevens

Voor een effectieve bescherming van de informatie is vereist dat de waarde van de informatie voor de onderneming bekend is. Classificatie van informatie in termen van vereiste vertrouwelijkheid, integriteit en beschikbaarheid:

- informeert het management en medewerkers over wat moet worden beschermd en hoe informatiemiddelen op een standaard manier kunnen worden beschermd;
- toont de waarde van middelen aan medewerkers, zodat het bewustzijn van beveiliging binnen hun dagelijkse werkzaamheden wordt gestimuleerd;
- stelt Complan Valens bv in staat te voldoen aan eventuele wettelijke en contractuele verplichtingen.

De eigenaar van de informatie blijft verantwoordelijk voor het up-to-date houden van de identificatie van informatiemiddelen en de toegekende waarde van elk van de geïdentificeerde middelen.

5 AANPAK VAN INFORMATIEBEVEILIGING / PRIVACY

5.1 INFORMATIEBEVEILIGING / RISICOMANAGEMENT

5.1.1 Risicobewustzijn

Risicobewustzijn van alle medewerkers van Complan Valens bv is de sleutel tot een effectieve informatiebeveiliging. Risicobewustzijn wordt volledig ondersteund door de directie van Complan Valens bv en zal gestimuleerd worden door middel van training en publicaties via onder meer het Intranet. Het risicobewustzijn wordt ook ondersteund door het opstellen en naleven van reglementen en zal indien nodig ook aandacht krijgen in functiebeschrijvingen en arbeidscontracten of inhuurovereenkomsten.

5.1.2 Risico-identificatie

Via een vastgestelde methodiek worden mogelijke dreigingen, informatiebeveiliging en privacy risico's geïdentificeerd en geïndexeerd. Het management zal de resultaten hieruit voortkomend beoordelen en 'zo kosten effectief mogelijk' maatregelen implementeren ter vermindering van het risico tot een acceptabel niveau.

5.2 BEPERKTE TOEGANG

Toegang tot informatie en IT-faciliteiten zal op basis van 'need to know' worden beperkt zodat gebruikers toegang krijgen tot datgene wat noodzakelijk is voor het uitvoeren van de functie. Dit is één van de essentiële principes van veilig informatiebeheer. Toegang tot informatiesystemen wordt geïnitieerd door de leidinggevende van de medewerker op basis van toegekende autorisaties en de medewerkersrol. Na het accorderen door de informatie- of informatiesysteemeigenaar zullen de autorisaties worden toegekend.

5.3 INFORMATIE EIGENDOM

ICT middelen die aan Complan Valens bv medewerkers beschikbaar worden gesteld, dienen voor zakelijke doeleinden toegepast te worden. Opgeslagen en verwerkte informatie van of voor Complan Valens bv op systemen van de onderneming blijft te allen tijde eigendom van Complan Valens bv. De internationale en lokale privacywetgeving zal gehandhaafd worden wanneer een beroep wordt gedaan op eigendomsrechten.

5.4 ICT-INFRASTRUCTUUR

Complan Valens bv heeft een ICT-infrastructuur geïmplementeerd voor de eigen bedrijfsonderdelen en locaties die onderlinge interne communicatie en samenwerking met partners, klanten en medewerkers op afstand mogelijk maakt. Deze ICT-infrastructuur is voor een deel in beheer en eigendom van Complan Valens bv en voor een deel in beheer en/of eigendom van een aantal externe partijen zoals o.a. INUXI. Voor bepaalde diensten wordt gebruik gemaakt van externe publieke netwerken zoals het internet. Hierdoor zijn er diverse beveiligingsmaatregelen en beheersmaatregelen geïmplementeerd om de beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen.

6 BELEIDSKADERS

6.1 VERTROUWEN EN VEILIGHEID

Vertrouwen is voor Complan Valens bv de basis om met onze medewerkers, relaties en partners samen te werken. Dit vertrouwen vraagt om openheid van Complan Valens bv over de gegevens die wij van onze medewerkers en relaties vragen. Maar ook om veiligheid van diezelfde gegevens bij ons als werkgever of aanbieder van onze producten en diensten. Complan Valens bv gaat daarbij zorgvuldig om met gegevens en zorgt voor een passend niveau van beveiliging en zorgt ervoor dat elke verwerking van gegevens voldoen aan de toepasselijk wet- en regelgeving.

6.2 INFORMATIEBEVEILIGING

Informatie, informatiesystemen, toepassingen en netwerken van Complan Valens bv Holding B.V. dienen in voldoende mate beschikbaar te zijn, dienen volledige en juiste informatie te bevatten en dienen uitsluitend toegankelijk te zijn voor rechtmatige gebruikers. De informatie, informatiesystemen, toepassingen en netwerken moeten in staat zijn bedreigingen voor hun beschikbaarheid, integriteit en vertrouwelijkheid te weerstaan en moeten zich kunnen herstellen bij het optreden van incidenten en calamiteiten.

Om hieraan te kunnen voldoen zal Complan Valens bv het volgende doen:

- Complan Valens bv zal alle componenten op het gebied van hardware, software en informatie beschermen die onder haar beheer vallen. Dit wordt bereikt door het implementeren en beheren van een uitgebalanceerd pakket technische en organisatorische beveiligingsmaatregelen.
- Complan Valens bv zal in verhouding tot de risico's voor haar componenten effectieve en efficiënte beveiliging bieden.
- Complan Valens bv zal het informatiebeveiligingsbeleid op een consistente, tijdige, effectieve en efficiënte manier implementeren en beheren.
- Complan Valens bv zal voor alle bedrijfskritieke informatiesystemen, toepassingen en netwerken een systeembeveiligingsbeleid opstellen. Hierin komen aan bod:
    - De autorisaties voor het gebruik van het systeem;
    - Een beschrijving van beveiligingsmaatregelen die van toepassing zijn op het systeem;

    - De verantwoordelijkheden en bevoegdheden voor het systeem;
    - Een continuïteitsplan voor het systeem.
- Complan Valens bv zal zich inspannen om haar medewerkers (de gebruikers van informatiesystemen, toepassingen en netwerken) uitleg te geven over beveiliging en hun verantwoordelijkheden en om het noodzakelijke beveiligingsbewustzijn onder de medewerkers te creëren. Hiertoe zal een bepaalde vorm van training worden toegepast.
- Complan Valens bv zal aan alle medewerkers duidelijk maken dat onverantwoordelijke en/of ongepaste daden kunnen leiden tot disciplinaire maatregelen.

Waar van toepassing zal Complan Valens bv zich houden aan:

- Complan Valens bv zal zich houden aan Nederlandse en Europese wet- regelgeving.
- Gedrag en fatsoensnormen van het maatschappelijk verkeer.

6.3 GEGEVENS EN PRIVACY

Dit beleid is van toepassing op alle gegevens die Complan Valens bv verzamelt en verwerkt van medewerkers, relaties en partners van de Nederlandse Complan Valens bv vennootschappen. Complan Valens bv is de verantwoordelijke voor de verwerking van persoonsgegevens zoals beschreven in dit beleid. De verwerkingen van Complan Valens bv zijn niet aangemeld bij de Autoriteit Persoonsgegevens (AP)

6.3.1 Doeleinden

Complan Valens bv hecht veel waarde aan de bescherming van uw privacy. Je kunt er op vertrouwen dat wij:

- Werken naar de letter en geest van de privacywet- en regelgeving
- Gegevens veilig en zorgvuldig verwerken
- Gegevens niet doorgeven of verkopen aan derden voor commerciële of charitatieve doeleinden
- Wettelijke rechten respecteren
- Alleen samenwerken met partijen die dezelfde uitgangspunten hanteren
- Vragen over privacy eerlijk zullen beantwoorden

Persoonsgegevens zijn gegevens die ofwel direct over u gaan ofwel naar u te herleiden zijn. Denk hierbij aan uw naam, geboortedatum, adres etc. Wij verwerken deze gegevens om u op een goede wijze van dienst te kunnen zijn of om te voldoen aan onze wettelijke verplichtingen.

6.3.2 Toegang tot gegevens

Complan Valens bv schakelt bij de uitvoering van haar dienstverlening derden in. Voor zover deze derden bij het uitvoeren van de betreffende diensten en bedrijfsactiviteiten je gegevens verwerken, doen zij dit in hoedanigheid van Bewerker voor Complan Valens bv en heeft Complan Valens bv de vereiste technische en organisatorische maatregelen getroffen om te verzekeren dat je gegevens uitsluitend voor bovenstaande doeleinde worden gebruikt. Uitsluitend indien Complan Valens bv hiertoe wettelijk is verplicht, worden persoonsgegevens verstrekt aan toezichthouders, fiscale autoriteiten en opsporingsinstanties. Persoonsgegevens kunnen in dit kader ook worden doorgegeven naar landen buiten de Europese Economische Ruimte (EER). Complan Valens bv zal in dergelijke gevallen passende maatregelen nemen die redelijkerwijs nodig zijn om te waarborgen dat gegevens zo goed mogelijk worden beschermd.

6.3.3 Beveiliging van gegevens

Je mag van ons verwachten dat Complan Valens bv er alles aan zal doen om jullie privacy te waarborgen. Uiteraard houden wij ons aan de wet- en regelgeving. Alle Complan Valens bv-medewerkers hebben geheimhoudingsplicht die ook ten aanzien van jullie gegevens geldt. Complan Valens bv gaat uiterst zorgvuldig om met je persoonsgegevens. Wij hebben verschillende technische en organisatorische maatregelen genomen om je persoonsgegevens te beveiligen. Zo beveiligen wij onze systemen en applicaties volgens de gelden standaarden voor informatiebeveiliging. De Complan Valens bv heeft een NEN7510 certificering. Dit betekent dat een externe audit heeft plaatsgevonden om de ICT processen en de beheersmaatregelen op het gebied van informatiebeveiliging te toetsen op basis van de NEN7510-norm. Bovendien bewaren wij de verzamelde gegevens niet langer dan noodzakelijk is. Hoe lang dat precies is, kan in verschillende wetten zijn vastgelegd en hangt af van het specifieke gegeven en het doel waarvoor wij jullie gegevens verwerken.

6.3.4 Vragen en verzoeken om inzage, correctie en verwijdering

Wanneer u informatie wilt, over uzelf, kunnen wij u deze informatie pas geven als voldoende duidelijk is wie u bent (identificeren) en ook daadwerkelijk de persoon bent die u zegt te zijn (authenticeren). Wij

verstrekken geen gegevens over de telefoon of via e-mail zonder dat wij zeker weten dat wij u aan de telefoon hebben of een e-mail van uw e-mailadres afkomstig is.

U heeft een aantal rechten met betrekking tot uw persoonsgegevens:

- Recht op inzage in door ons van u vastgelegde gegevens.
- Recht op indienen van een verzoek tot correctie of verwijdering van uw gegevens
- Recht om bezwaar te maken (verzet) tegen bepaalde wijze van gebruik van uw gegevens.

In sommige gevallen kunnen of mogen wij geen wijziging of verwijdering doorvoeren. Bijvoorbeeld als dat in strijd met de wet is. Een verzoek tot inzage of correctie kunt u indienen bij onze Privacy Officer via e-mail privacy@complan.nl. De Privacy Officer zal binnen 10 werkdagen met een reactie komen.

7 KWALITEITSBEWAKING

7.1 COMMUNICATIE

In de communicatie van dit beleid staat centraal de bewustwording van het eigen personeel (en ingehuurde derden), de naleving van de regels en richtlijnen. Om dit te bewerkstelligen zullen er gedragsregels opgesteld en gecommuniceerd worden zodat medewerkers weten wat er van hun verwacht wordt, welke risico´s er zijn en welke rechten en plichten ze hebben. Veranderingen en aanpassingen in het management systeem worden door het management beoordeeld en intern gecommuniceerd, indien nodig ook naar relevante externe partijen.

Het management bepaalt:

- wat gecommuniceerd wordt;
- wanneer gecommuniceerd wordt;
- met wie gecommuniceerd wordt;
- wie de communicatie uitvoert en;
- welke processen door de communicatie beïnvloedt worden.

7.2 BORGING

Borging vindt plaats door middel van vastlegging van de overeengekomen werkwijze in procesbeschrijvingen, richtlijnen, een gedragscode, procedures, werkinstructies en tooling. Deze dienen voor alle medewerkers toegankelijk te zijn en zullen via het Intranet verspreid worden, zodat in het geval van incidenten en calamiteiten deze snel en eenduidig toegankelijk zijn.

7.3 GELDIGHEID EN EVALUATIE

De directie is eigenaar van dit beleidsdocument. Het beheer, opstellen en actueel houden van het beleidsdocument is de verantwoordelijkheid van de Information Security & Privacy Officer in samenspraak met directie van Complan Valens bv.

Dit beleid is drie jaar geldig en wordt minimaal een keer per jaar geëvalueerd met het oog op:

- De toereikendheid en de tactische en operationele uitvoering ervan;
- De stand van de techniek (beveiliging en bedreiging);
- Voortschrijdend inzicht;
- Veranderende wet- en regelgeving of organisatie.

Op grond van de jaarlijkse beoordeling, veranderende wet- en regelgeving of door andere omstandigheden, kan dit beleid tussentijds bijgesteld worden.

7.4 NALEVING

Naleving van het beleid wordt gecontroleerd. Niet naleving van het beleid kan disciplinaire maatregelen tot gevolg hebben, conform lokale regel- en wetgeving.

8 VERWIJZINGEN DOCUMENTEN

- Overzicht relevante wet- en regelgeving
- Informatiebeveiliging en Privacy handboek
- Informatie classificatie en labelling