Beleidsproces

Informatiebeveiligingsbeleid
Inclusief beleid datalekken

SIG

Creatiedatum	9 mei 2018
Herzieningsdatum	
Evaluatiedatum	31 december 2019
Versie	1
Status	Concept
Auteur	Astrid Reulen, aanspreekpunt “AVG SIG”
Opdrachtgever	Jan Kroft, bestuurder

Inhoud

1. Inleiding

Met ingang van 25 mei 2018 is de AVG van kracht. Dit beleid regelt het dataverkeer persoonsgegevens. De wet is veelomvattend. Naast dit beleid zullen er meerdere beleidsstukken vervaardigd worden in de loop van het jaar rondom de beveiliging van gegevens.

Binnen de SIG zijn voor de beveiliging van informatie veel maatregelen getroffen. Enerzijds omdat eerdere wetgeving omtrent privacy dat van ons vroeg maar anderzijds omdat we het belangrijk vinden dat er ook zorgvuldig omgegaan wordt. Dit heeft de SIG dan ook altijd gepoogd te doen, echter de AVG heeft hierin regels verder aangescherpt. Dat vraagt om herziening beleid waardoor veel beleid wat hierop al was, vervalt omdat dit in dit beleid wordt samengevoegd. In dit document wordt een overzicht gepresenteerd van het te voeren beleid op het gebied van:

- Algemene maatregelen
- Hardware en systeemprogrammatuur
- Informatiesystemen
- Werkplekken
- Logische toegangsbeveiliging
- Continuïteitsbeheer
- Datalekken

Definitie "persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon; (bron:AVG, artikel4)
Per 1-2-2017 is voor de gehele Carante Groep samenwerking een functionaris gegevensbescherming aangesteld.
Een van de verantwoordelijkheden van de functionaris gegevensbescherming is het beoordelen, melden en afhandelen van datalekken

2. Algemene beleidsafspraken betreffende informatiebeveiligingsorganisatie

- Taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiligingsmaatregelen zijn toegewezen aan de afdeling ICT en de verantwoordelijk netwerkbeheerders.
- Voor elk onderdeel van de informatie(voorziening) is bepaald wie de verantwoordelijke is. Hiervoor is een schema bekend.
- Informatiebeveiligingstaken zijn bij de afdeling ICT belegd en vastgesteld in een taakbeschrijving.
- Informatiebeveiliging staat qua onderwerp als vast item op de agenda van het CTO en MT.
- Regelmatig worden reviews en audits gehouden.
- Taken, bevoegdheden en verantwoordelijkheden zijn vastgelegd en er worden controles op uitgevoerd.
- Een risicomemorandum geeft per informatiesysteem aan welke bedreigingen niet of niet geheel worden afgedekt.
- Een procedure die de vertrouwelijkheid van voornoemd memorandum regelt is aanwezig.

- Er zijn procedures die het beheer van informatiebeveiliging meetbaar laat verlopen. De administratieve organisatie en interne controle is hierop aangepast.

3. Personeel

3.1 Aanname en arbeidsvoorwaarden

- Er zijn arbeidsvoorwaarden waarin de rechten en plichten in relatie tot informatiebeveiliging zijn opgenomen. Taken, verantwoordelijkheden en bevoegdheden in het kader van de informatiebeveiliging zijn bij iedere medewerker eenduidig bekend.
- Iedere medewerker is geheimhoudingsplichtig.

3.2 Vervanging en functiewijziging

- Medewerkers die vanwege arbeidsvoorwaarden, werkomstandigheden, privé-problemen of anderszins, tot een risicofactor zijn geworden, worden opgevangen.
- Planning van werkzaamheden zorgt ervoor dat geen onverantwoorde leemten, functievermengingen of cumulaties optreden zodanig dat beoogde functiescheidingen wegvallen. In relevante gevallen is een en ander met derden contractueel geregeld (afroepbare reservecapaciteit).
- Procedures zorgen voor een autorisatie- en authenticatiebeheer in geval medewerkers op vertrouwens- en kwetsbare functies van functie veranderen dan wel het dienstverband beëindigen.
- Procedures regelen dat bij nieuwe of gewijzigde functies vóór openstelling en bij bestaande functies periodiek een afweging gemaakt wordt of sprake is van een vertrouwens- of kwetsbare functie. In de procedures is een functie-indelingslijst opgenomen.
- Medewerkers met specifieke of unieke kennis of specialismen delen deze kennis met anderen, zodanig dat er in deze zin geen kwetsbare functies kunnen ontstaan.
- Bij afwezigheid van medewerkers op kwetsbare posities wordt voor vervanging gezorgd.

3.3 Opleiding en ervaring

- Regelmatig worden activiteiten uitgevoerd die het beveiligingsbewustzijn bevorderen en op peil houden.
- Medewerkers zijn voor het vervullen van hun functie adequaat opgeleid. Daartoe zijn de voor een functie geldende opleidingseisen vastgelegd.
- Elke medewerker is bekend met en getraind in de omgang met op het netwerk aangesloten apparatuur.
- Lokaal systeembeheer is bekend met algemene en platformspecifieke beveiligingsaspecten.
- Daartoe bevoegden zijn bekend met de voorzieningen die in de beveiligde ruimten zijn aangebracht en weten deze te hanteren.

3.4 Externen

- Externe medewerkers en personeel van derden (leveranciers) werkzaam binnen de SIG moeten een geheimhoudingsverklaring ondertekenen.

- In contracten met externe bedrijven wordt een clausule opgenomen waarin geheimhoudingsplicht wordt benoemd en afspraken hierover worden gemaakt.
- De afdeling bepaalt zelf of voor een externe medewerker die toegang heeft tot kritische ruimtes/ gegevens/ applicaties, aanvullende eisen (b.v. antecedentenonderzoek en geheimhoudingsverklaring) gesteld moeten worden.

4 Archieven

- De SIG draagt er zorg voor dat documenten toegankelijk worden gearchiveerd.
- Documenten met vertrouwelijke gegevens worden gearchiveerd in af te sluiten ruimtes.
- Archivering vindt plaats in overeenstemming met de wettelijke eisen.
- Er is een sluitende uitleenregistratie.

5 Gegevensuitwisseling met derden

Het betreft hier een uitwisseling van intern opgeslagen gegevens tussen de SIG en andere instanties. De uitwisseling kan zowel elektronisch als op papier (dossiers) vastgelegde gegevens betreffen.

- Vastgelegd is onder wiens verantwoordelijkheid de uitwisseling plaats vindt en welke betrouwbaarheidseisen hieraan zijn verbonden.
- Vastgelegd is welke beveiligingsmaatregelen aan beide kanten zijn genomen.
- Met name wordt gelet op de exclusiviteit van de gegevens.
- Er vindt controle plaats op naleving van de gestelde betrouwbaarheidseisen.

6 Hardware en systeemprogrammatuur.

6.1 Aanschaf

Aanschaf van apparatuur en systeemprogrammatuur vindt plaats:

- Op basis van een specificatie van de eisen waaraan het aan te schaffen product dient te voldoen.
- Bij geselecteerde leveranciers.
- Bij aflevering van het aangeschafte product wordt gecontroleerd of het overeenkomt met het gevraagde.
- De aanschaf, aflevering en het product worden geregistreerd ten behoeve van het configuratiemanagement.
- Verzoeken hiertoe kunnen alleen via bestuurder of clustermanager.

6.2 Installatie

Het plaatsen en installeren/ inrichten van apparatuur en systeemprogrammatuur vindt plaats:

- Volgens de voorschriften van de fabrikant / leverancier. Voor zowel de installatie van nieuwe hardware als software geldt dat als eerste de meegeleverde instructies gelezen worden alvorens het apparaat of de software wordt geïnstalleerd. De gestelde eisen worden in acht genomen.
- Nadat er controle is geweest op beschikbaarheid van updates, patches en/of nieuwere drivers.
- Uitsluitend door ICT-medewerkers of onder begeleiding van ICT-medewerkers in het geval van personeel van een leverancier.

- Installatie en uitlevering c.q. plaatsing van werkstations bij de medewerkers van de SIG vindt plaats in afstemming met de gebruiker.

6.3 Testen

Nieuwe (en bestaande) apparatuur en systeemprogrammatuur wordt onderworpen aan de test- en acceptatieprocedure:

- Er wordt vastgesteld of het geleverde voldoet aan de bij aanschaf gestelde eisen.
- Acceptatie van het geleverde wordt gedaan door de verantwoordelijk manager.
- Er wordt vastgesteld of het geleverde functioneert in samenhang met de reeds aanwezige componenten van de technische infrastructuur.
- Ontwikkelen en testen vindt alleen plaats vinden met gefingeerde of geanonimiseerde kopieën van productiegegevens en niet met gegevensdragers waarop (originele) productiegegevens staan.
- Testresultaten worden vastgelegd in een testrapport.

6.4 Onderhoud

- Aangewezen cruciale apparatuur wordt als zodanig gedocumenteerd in het in benodigde beschrijving op intranet, het onderhoudsplan en het continuïteitsplan en wordt voorzien van een onderhoudscontract met de fabrikant/ leverancier indien er geen vervangende apparatuur voorhanden c.q. op voorraad voor is.
- Uitgevoerde onderhouds- en reparatiewerkzaamheden worden geregistreerd in daarvoor bestemde logboeken.
- Onderhoud en reparatie in computerruimten mogen alleen uitgevoerd worden door gevoegd ICT-personeel of onder toezicht van ICT-personeel.
- Onderhoud en reparatie worden uitgevoerd volgens de voorschriften van leveranciers.
- Storingen buiten werktijden worden de eerst volgende werkdag door de ICT-medewerkers opgepakt. Er is geen oproeprooster voor het vaste ICT-personeel.

6.5 Beheer

- Originele systeemdocumentatie en bronprogrammatuur wordt opgeborgen in daartoe geëigende en goed afgesloten (brandwerende) kasten en ruimten.
- Programmalicenties worden nageleefd.
- Gebruik van illegale programmatuur is niet toegestaan.
- Licentieovereenkomsten worden opgeslagen in de kluis.
- In- en uitvoer en verplaatsing van apparatuur is voorbehouden aan personeel van de ICT-afdeling. De ICT-medewerkers zijn bekend met en kunnen omgaan met beveiligde ruimten en de hierin aangebrachte voorzieningen.
- Het functioneren van apparatuur en systeemprogrammatuur wordt continu bewaakt door systeem- en netwerkbeheerders al of niet met behulp van (geautomatiseerde) tools.
- Alle storingen worden geregistreerd volgens de vaste procedure.
- Afgehandelde problemen worden indien van toepassing terug gemeld aan de melder.
- Op ieder gewenst moment is er inzicht in systeem- en netwerkbelasting.
- Periodiek wordt gerapporteerd aan de verantwoordelijk manager wat de systeem en netwerkbelasting geweest is.

6.6 Afvoer en vernietiging

- In geval dat apparatuur terug moet naar de leverancier worden de aanwezige gegevensdragers vernietigd, tenzij het softwarematig mogelijk is de gegevens adequaat te wissen.
- Gegevensdragers worden alvorens te worden afgevoerd fysiek vernietigd.
- Papieren gegevensdragers (met bedrijfsgevoelige informatie) worden versnipperd.
- Methodiek en verantwoordelijkheid met betrekking tot af te voeren gegevensdragers is voor alle medewerkers van de ICT-afdeling duidelijk.

6.7 LAN/WAN

- Toegang tot fileservers verloopt gecontroleerd via een aanlogprocedure.
- De verantwoordelijken van informatiesystemen geven aan wie wanneer van welke faciliteiten en onder welke omstandigheden gebruik mag maken, vastgelegd in een autorisatiematrix.
- Illegale pogingen toegang tot het netwerk te verkrijgen (hacken) wordt vastgelegd en onderzocht volgens de vastgestelde procedure vanuit de Carante Groep.
- Teneinde kwetsbaarheid te verminderen is het netwerk opgesplitst in afzonderlijke domeinen.
- Bescherming voor virussen is afgevangen.
- Wachtwoorden zijn tijdens het transport over het netwerk versleuteld.
- Het aansluiten van apparatuur is voorbehouden aan medewerkers van de ICT-afdeling.
- Het aansluiten van modems op het netwerk is niet toegestaan.
- Richtlijnen en registratie van de op het netwerk aan te sluiten apparatuur (waaronder laptops), zijn vastgelegd.
- Het aansluiten op internet is niet toegestaan.

6.8 Gegevensdragers

- Regels met betrekking tot het gebruik, de behandeling en het beheer (en reconstructie) van gegevensdragers zijn vastgelegd.
- Alle gegevensdragers zijn direct identificeerbaar. Op de gegevensdragers is vermeld wat de herkomst, inhoud en actualiteit is.
- Uitgifte en toegang tot gegevensdragers is gerelateerd aan de functie en is vastgelegd binnen bevoegdhedenmatrices.
- Gegevensdragers worden opgeborgen in een kast of bureau wanneer deze niet gebruikt worden (clear desk-policy).
- Opslag, vervoer en gebruik vindt plaats volgens de door de leverancier van de gegevensdrager aangegeven wijze.
- Gegevensdragers worden tijdens transport beveiligd tegen verlies en diefstal.
- Gegevensdragers zijn afdoende beschermd tegen omstandigheden die tot onherstelbare schade en/of verlies leiden.
- Uitgifte en toegang tot gegevensdragers is gerelateerd aan een functie en vastgelegd in bevoegdhedenmatrix.
- Bij uitgifte van het toegangsrecht wordt de rechtmatigheid ten opzichte van de betreffende functie gecontroleerd.

7 Informatiesystemen

7.1 Beheer

- Op de afdeling is een beheerreglement bekend voor originele systeemdocumentatie en bronprogrammatuur met daarin een regeling voor het versiebeheer.
- Functiescheiding is aangebracht tussen het ontwikkelen, beheren en operationaliseren van applicatieprogrammatuur.
- Functiescheiding is aangebracht wat betreft het functionele applicatiebeheer en het technisch applicatiebeheer.
- Downloaden en uploaden van data door gebruikers is niet toegestaan.
- Bij het tot stand brengen van koppelingen tussen verschillende applicaties strekken de kwaliteits- en betrouwbaarheidseisen zich ook tot de koppelingen uit. Schriftelijk wordt vastgelegd welke koppelingen het betreft en tevens hoe en bij wie de verantwoordelijkheden zijn belegd.
- Voor wat betreft de aanschaf van informatiesystemen gelden dezelfde regels en procedures als voor aanschaf van systeemsoftware (zie hiervoor).

7.1 Testen

- Voor wat betreft het testen van informatiesystemen gelden dezelfde regels en procedures als voor systeemsoftware (zie hiervoor).

7.2 Aanvullende maatregelen

- De medicijnenverstrekkingsoverzichten komen vanuit één bron. Op basis van dit overzicht kan men gedurende de periode waarvoor de medicatie verstrekt is door de apotheek onder de verantwoordelijkheid van de huisarts van de cliënt, de medicijnverstrekking verrichten.

7.3 Gegevensverzamelingen

- Gegevens die worden ingevoerd en verwerkt wordt altijd eerst gevalideerd.
- Periodiek wordt er gecontroleerd op geldigheid en integriteit.
- Indien er fouten worden geconstateerd, worden deze volgens de procedures gecorrigeerd.

8 Werkplekken

- Teneinde onbevoegde kennisneming van gegevens te voorkomen is een clean desk policy ingevoerd. Er zijn procedures voor het opgeruimd achterlaten van werkplekken en bureaus.
- Deuren en kasten (met vertrouwelijke informatie) worden afgesloten bij het verlaten van de werkplek.
- PC’s worden niet onbeheerd achtergelaten. Bij het verlaten van de werkplek worden applicaties en netwerksessie afgesloten door middel van uitloggen of indien mogelijk het “locken” van het werkstation.
- Het aansluiten van apparatuur is voorbehouden aan medewerkers van de ICT-afdeling.
- Het via het netwerk aansluiten van PC’s op internet is niet toegestaan.

9 Logische toegangsbeveiliging

9.1 Gebruikersidentificatie en wachtwoorden

- Bij toegang tot het netwerk en applicaties is er uitsluitend sprake van persoongebonden gebruikersidentificatie. Algemene netwerkaccounts zijn niet toegestaan tenzij hierover andere afspraken zijn gemaakt in woonvoorzieningen.
- De regels die gehanteerd worden met betrekking tot het verlenen van toegang tot het netwerk en applicaties zijn vastgelegd.
- Op vaste tijden wordt gecontroleerd op geldigheid en rechtmatigheid van de verleende gebruikersidentificaties, toegangsrechten en bevoegdheden.
- Wachtwoordenbeleid: een wachtwoord bestaat uit minimaal 8 posities en moet tweemaandelijks worden vernieuwd.
- Wachtwoorden worden versleuteld opgeslagen.
- Gebruik van accounts en wachtwoorden vindt gereglementeerd plaats. Het reglement wordt bij de medewerker bekend gemaakt door middel van de gebruikersovereenkomst en de verspreiding van de huisregels PC-gebruik.

9.2 Antivirusmaatregelen

- Alle werkstations en netwerkservers zijn voorzien van residente anti-virusprogrammatuur.
- Wekelijks wordt gecontroleerd of updates en upgrades beschikbaar zijn, welke indien van toepassing direct geautomatiseerd worden verspreid.
- Gegevensdragers worden altijd op virussen gecontroleerd voordat deze worden gebruikt.
- De anti-virusprogrammatuur is zodanig geïnstalleerd dat de gebruiker niet in staat is deze uit te schakelen. De anti-virusprogrammatuur is zodanig geïnstalleerd dat bij constatering een melding aan de ICT-afdeling plaatsvindt.
- Periodiek wordt steekproefsgewijs gecontroleerd of de automatische verwerking van updates en upgrades plaats heeft gevonden.

10 Continuïteitsbeheer

10.1 Continuïteitsplan

- In het continuïteitsplan is vastgelegd welke stappen moeten worden ondernomen in het geval van een calamiteit. In het onderhoudsplan is opgenomen welke onderhoudswerkzaamheden hebben plaats gevonden en welke plaats gaan vinden op servers.
- Het beheer van het continuïteitsplan is belegd bij de afdeling ICT.
- Het initiëren en het uittesten van het continuïteitsplan wordt samen met de diepgang bepaald door het managementteam van de ICT-afdeling.
- Verantwoordelijk personen hebben het continuïteitsplan in hun bezit.

10.2 Back-up van gegevens en (systeem-)programmatuur

- Van alle gegevens-, transactie-, autorisatie- en loggingbestanden wordt dagelijks een back-up gemaakt.
- Back-ups worden gemaakt volgens procedure.
- Back-ups worden in een logboek geregistreerd.
- Er zijn escrow-voorzieningen getroffen wat betreft bronprogrammatuur van de applicaties. Back-ups worden gemaakt:

- Direct na aflevering van nieuwe of gewijzigde programmatuur.
- Voor dat wijzigingen worden aangebracht in nieuwe programmatuur.

10.3 Bewaartermijnen

- Bewaartermijnen voor de verschillende back-uptapes zijn vastgelegd.
- Er is een roulatieschema ter verversing van tapes die langer dan twee jaar bewaard worden om restorebaarheid zeker te stellen.

10.4 Bewaarlocatie

Back-ups van gegevensbestanden en programmatuur alsmede een kopie van de beschrijving van de beheerprocessen en procedures, worden:

- Zo snel mogelijk na het aanmaken overgebracht naar de bewaarlocatie(s).
- Bewaard in een brandwerende kluis, buiten de computerruimten.
- Bewaard op een tweede locatie volgens een beschreven roulatieschema in een ander gebouw.
- Back-ups worden onder geen beding in de privé-sfeer bewaard.

10.5 Recovery

Het terugzetten van back-ups van gegevens en programmatuur:

- Vindt plaats in opdracht van de verantwoordelijke van de betreffende gegevens of programmatuur.
- Is beschreven en wordt geregistreerd in een logboek.
- Periodiek worden restoreprocedures onder een continuïteitsscenario uitgevoerd.

13 Gebruik netwerkaccount

- Een account wordt automatisch vanuit Beaufort gegenereerd op basis van het personeelsnummer.
- Een aanvraag voor autorisatie voor gebruik van het netwerk (afdeling en applicaties) wordt uitsluitend in behandeling genomen als deze aanvraag is gedaan door:
  -Teamleider/leidinggevende indien deze een autorisatie volgens de regels betreft
  - Secretaris OR indien het een autorisatie voor een OR-lid betreft
  - Bestuurder of clustermanager indien het een autorisatie betreft die niet onder de vastgestelde regels valt
- Na goedkeuring zullen de gebruikersnaam en de bijbehorende rechten op het netwerk geëffectueerd worden. Gebruikersnaam en wachtwoord zijn persoonsgebonden. Het is daarom niet toegestaan om de gebruikersnaam en het wachtwoord aan collega's of derden beschikbaar te stellen. De gebruiker is persoonlijk verantwoordelijk voor hetgeen gedaan wordt onder zijn of haar gebruikersaccount.
- Iedere 90 dagen dient het IDM-wachtwoord te worden veranderd, het systeem geeft het tijdstip aan. Er wordt een historie van 10 eerder gebruikte wachtwoorden vastgehouden, die niet hergebruikt kunnen worden.
- Het wachtwoord moet bestaan uit minimaal 8 tekens en maximaal 128 tekens
- Het wachtwoord moet minsten **3** unieke karakters bevatten
- 1 kleine letter [a-z]
- 1 hoofdletter [A-Z]
- 1 cijfer [0-9]
- Het gebruik van speciale tekens in het wachtwoord is toegestaan [#,$,@, enz.].

- Bij het verlaten van de werkplek dient deze vergrendeld te worden of moet er uitgelogd worden uit het netwerk, zodat het voor derden niet mogelijk is om onder het ingelogde account het netwerk te gebruiken en/of databestanden te raadplegen, te kopiëren, te muteren en/of te wissen.
- Bij uitdiensttreding wordt het account automatisch geblokkeerd. Bij overplaatsing van een medewerker naar een andere afdeling dient dit direct door de clustermanager doorgegeven te worden aan de afdeling IT.

14 Gebruik E-mail en internet

Hieronder wordt vastgelegd welke regels er binnen de SIG gelden voor de omgang met e-mail en internetgebruik in relatie tot bescherming van digitaal dataverkeer van persoonsgegevens. Deze omvat gedragsregels ten aanzien van verantwoord e-mail en internetgebruik en regels over de wijze waarop controle op e-mail en internetgebruik plaatsvindt.

14.1 Regels e-mailgebruik

- Medewerkers mogen uitsluitend gebruik maken van het e-mailsysteem voor het ontvangen en versturen van persoonlijke e-mailberichten in situaties waar uitstel van deze communicatie niet mogelijk en onredelijk is en dit geen illegale activiteiten betreft.
- Het versturen van e-mailberichten moet voldoen aan de volgende voorwaarden:
- een correcte vermelding van afzender
- bij externe mail wordt automatisch een disclaimer meegestuurd
- duidelijke aanduiding van het onderwerp indien het een privé-mail betreft
- Het is niet toegestaan om naar of vanuit privé-mailadressen privacygevoelige informatie (persoonsgegevens) omtrent cliënten, medewerkers of vrijwilligers te verzenden;
- Het is niet toegestaan om zogenaamde “kettingbrieven” te versturen;
- E-mails met een bijlage waarvan de bestandsnaam eindigt op .pif .scr .bat of .vbs worden geblokkeerd in het systeem, omdat deze vaak virussen bevatten.
- E-mails met de bijlage waarvan de bestandsnaam eindigt op .zip en afkomstig zijn vanaf het Internet worden geblokkeerd. Indien u toch e-mails met zip-bijlages dient te ontvangen vanaf het internet, kan men de domeinnaam (bijvoorbeeld kpn.com) opgeven bij de Helpdesk. Deze kan dan hiervoor een uitzondering maken.
- Indien een e-mail die aan een medewerker gericht is, geblokkeerd wordt omdat het een virus bevat, ontvangt de medewerker hiervan een bericht (een zogenaamd Quarantine Report), hiermee kan de medewerker een bericht welke onterecht geblokkeerd wordt alsnog vrijgeven.

14.2 Regels internetgebruik

- Medewerkers mogen uitsluitend gebruik maken van het internetsysteem voor persoonlijke doeleinden in situaties waar uitstel van deze communicatie niet mogelijk en onredelijk is.
- Het is niet toegestaan om:
- Op wat voor manier dan ook deel te nemen aan chatboxen
- Internetsites bezoeken die geen functionele bijdrage leveren aan de werkzaamheden van de medewerker;
- Op internet in strijd met de wet te handelen
- Software en applicaties te downloaden en/of te installeren.

14.3 Controle e-mail en internetgebruik

De controle op e-mail en internetgebruik vindt in het kader van de wet bescherming persoonsgegevens plaats met als doel:

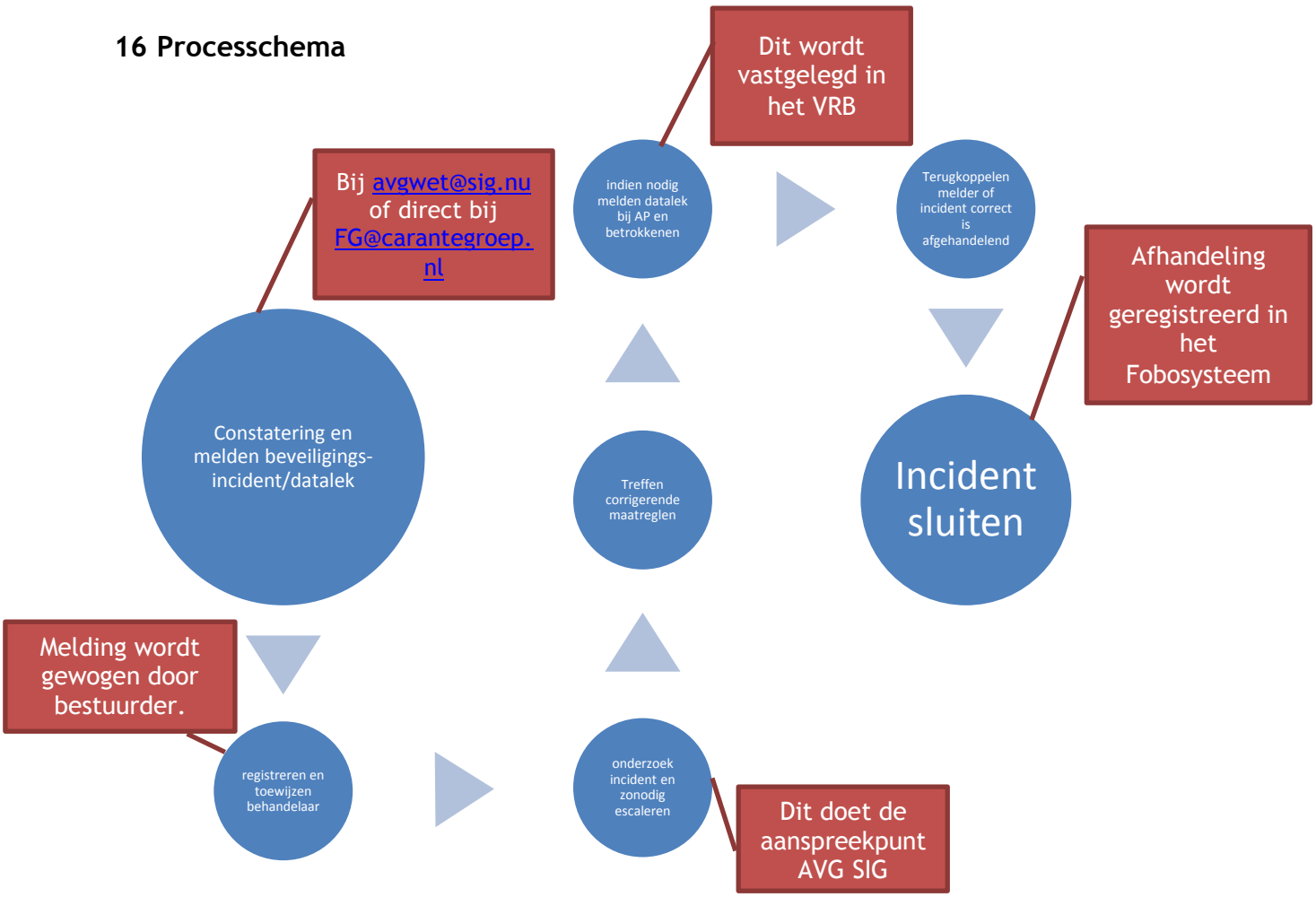
- Het tegengaan van virussen en andere schadelijke programma's in het kader van systeem- en netwerkbeveiliging. Het e-mail en internetgebruik wordt op geautomatiseerde wijze gecontroleerd.
- Controle in het kader van het tegengaan van "verboden gebruik" vindt in beginsel geanonimiseerd en steekproefsgewijs plaats. "Verboden" e-mail en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt. Er wordt hierbij gehandeld conform de AVG.

15 Proces datalek

Toepassingsgebied	Alle werkplekken van de SIG
Doel van het beleid	Het waarborgen van de continuïteit van de dienstverlening door een zo spoedig mogelijk herstel van het afgesproken kwaliteitsniveau, als hierop een afwijking wordt geconstateerd. Daarbij wordt ingegaan op hoe informatiebeveiliging incidenten, waaronder in het bijzonder meldingen van datalekken, worden afgehandeld.
Definities	**Foboverbetersysteem**: Het proces waarin we verstoringen van de kwaliteit zo snel mogelijk proberen op te lossen en de voortgang zo veel mogelijk willen garanderen. **Beveiligingsincident**: Afzonderlijke gebeurtenis of een serie ongewenste of onverwachte informatiebeveiligings-gebeurtenissen waarvan het waarschijnlijk is dat ze nadelige gevolgen voor de bedrijfsvoering van de organisatie hebbben en een bedreiging vormen voor de informatiebeveiliging. Voorbeelden van ICT-gerelateerde beveiligingsincidenten zijn: - Virusuitbraak (malware); - Diefstal of verlies van: - Apparatuur (bijv. PC/Mobiel/Laptop/andere hardware); - Persoonsgegevens (van cliënten of medewerkers) op informatiedragers (bijv. audiovisueel materiaal, Cd's, Dvd's, tapes, USB-sticks); - Inbraak op netwerk, applicaties (zoals hacken); - Uitval kritieke bedrijfsapplicaties die (veel) langer duren dan afgesproken in de samenwerkingsovereenkomsten. Beveiligingsincidenten kunnen ook niet ICT-gerelateerd zijn. Voorbeelden van niet ICT-gerelateerde beveiligingsincidenten zijn: - Diefstal of verlies van persoonsgegevens op papier; - Niet afgesloten ruimtes, kasten of bureaus met vertrouwelijke documenten; - Zichtbare notitieblaadjes met toegangsgegevens tot het netwerk of applicaties. **Datalek**: Een datalek, ook wel een inbreuk in verband met persoonsgegevens genoemd, is een inbreuk op de beveiligingsmaatregelen waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene zijn verbonden. Het doel van de meldplicht is om burgers te beschermen tegen risico's zoals identiteitsfraude, financiële verliezen, gemiste kansen in zaken of beroepsontwikkeling. Voorbeelden van datalekken zijn: - Diefstal of verlies van:

	- Persoonsgegevens (van cliënten of medewerkers) op informatiedragers (bijv. audiovisueel materiaal, Cd's, Dvd's, tapes, USB-sticks) ; - Virusbesmetting of een inbraak op netwerk, applicaties (zoals hacken) waarbij persoonsgegevens worden buitgemaakt; - Verzending van e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden; - Het verkeerd adresseren een of meer e-mail(s) die persoonsgegevens bevatten. Datalekken kunnen ook niet ICT-gerelateerd zijn. Voorbeelden van niet ICT-gerelateerde datalekken zijn: - Diefstal of verlies van persoonsgegevens op papieren documenten. - Het verkeerd adresseren van grote aantallen brieven die persoonsgegevens bevatten. - Het bij het vuilnis zetten van privacygevoelige dossiers met persoonsgegevens van cliënten of medewerkers, die vervolgens in de openbaarheid kunnen komen. *Uitzonderingen op de meldplicht* De meldingsplicht vervalt als de persoonsgegevens dermate zijn versleuteld of onbegrijpelijk gemaakt voor een ieder die geen recht heeft op kennisname van deze gegevens dat deze niet te lezen zijn. (art. 34a lid 6 Wbp/art. 34 lid 3 AVG). Dit moet per geval onderzocht worden, omdat de effectiviteit mede afhangt van het gebruikte algoritme en het moment / punt waarop de gegevens zijn versleuteld. Ook hoeft een datalek niet gemeld te worden wanneer de inbreuk een lage of geen impact op de persoonlijke levenssfeer heeft

16 Processchema



17 Activiteiten proces datalek

	Proces
Beschrijving	Het proces afhandelen beveiligingsincidenten omvat tevens het proces afhandelen en melden datalekken en bestaat uit de volgende processtappen: 1 Constateren en melden beveiligingsincident/datalek; 2 Registreren en toewijzen behandelaar; 3 Onderzoek incident en zonodig escaleren; 4 Treffen corrigerende maatregelen; 5 Melden datalek bij Autoriteit Gegevensbescherming (indien nodig) en betrokkenen (indien nodig); 6 Terugkoppeling melder of het incident correct is afgehandeld; 7 Incident sluiten.

Activiteit	**1. Constateren en melden beveiligingsincident/datalek**
Uitvoerende	Beveiligingsincidenten en datalekken kunnen op de volgende manieren worden opgemerkt: - waarneming door een bewerker/toeleverancier; - waarneming door een medewerker, cliënt, verwant, vrijwilliger - detectie door ICT-systeem (netwerk- en system-management-tools) bij CaranteGroep - waarneming door beheerders bij de CaranteGroep
Verantwoordelijke	
Beschrijving	Beveiligingsincidenten en datalekken, zowel ICT- als niet ICT-gerelateerd, kunnen via dit proces worden gemeld en afgehandeld. Incidenten kunnen op de volgende manier worden gemeld: Van een datalek wordt altijd een fobo gemaakt daarnaast kan er gemeld worden: Via e-mail avgwet@sig.nu Via telefoon; Face to Face. Ook kunnen beveiligingsincidenten/datalekken rechtstreeks gemeld worden bij Functionaris gegevensbescherming van Carante Groep. FG@carantegroep.nl
Activiteit	**2. Registreren melding en toewijzen behandelaar**
Uitvoerende	Aanspreekpunt AVG SIG
Verantwoordelijke	Bestuurder
Beschrijving	Aanspreekpunt “AVG SIG” ontvangt de melding. De melding staat geregistreerd in het fobosysteem. Het aanspreekpunt “AVG SIG” zal met de bestuurder de melding wegen en de behandelaar toewijzen. Dit zal vaak een teamleider zijn.
Activiteit	**3. Analyse incident en zo nodig escaleren**
Uitvoerende	Aanspreekpunt “AVG SIG”.
Verantwoordelijke	
Beschrijving	Het aanspreekpunt “AVG SIG” analyseert de melding. Hiervoor worden de ‘Beleidsregels voor toepassing van artikel 34a van de Wbp’ gehanteerd. Indien de melding een datalek is, wordt dit als zodanig vastgelegd in het VRB. Indien het een datalek betreft onderzoekt het aanspreekpunt “AVG SIG” - of sprake is van het lekken van gevoelige/bijzondere gegevens; - of sprake is van ‘aanmerkelijk risico op verlies of onrechtmatige verwerking waaraan nadelige gevolgen voor de persoonsgegevens en de persoonlijke levenssfeer van de betrokkene zijn verbonden’. Verder onderzoekt het aanspreekpunt “AVG SIG” welke organisaties getroffen zijn door het incident/datalek. Het escalatieschema is beknopt vanwege de manier waarop de organisatie de verantwoordelijkheid hiervoor heeft geregeld.
Activiteit	**4. Treffen maatregelen**
Uitvoerende	Aanspreekpunt “AVG SIG”
Verantwoordelijke	Bestuurder

Beschrijving	De maatregelen die getroffen worden zullen zoveel mogelijk in overleg met betrokkenen worden genomen. Maatregelen worden vastgelegd in het VRB alwaar verantwoording zal worden afgelegd over de uitvoering. De aard van de corrigerende maatregelen hangt af van het type incident/datalek (ICT- of niet ICT-gerelateerd, de schade van het incident, etc.).

Activiteit	**5. Melden datalek bij Autoriteit Gegevensbescherming (indien nodig) en betrokkenen (indien nodig)**
Uitvoerende	Coördinator informatiebeveiliging/Functionaris gegevensbescherming
Verantwoordelijke	Functionaris Gegevensbescherming en bestuurder SIG
Beschrijving	De Functionaris Gegevensbescherming meldt het datalek, na overleg met de bestuurder, bij het meldpunt datalekken bij de toezichthouder (Autoriteit Persoonsgegevens). Deze melding moet 'onverwijld' plaatsvinden, *niet later dan 72 uur na de ontdekking* van het incident. Deze melding moet worden gedaan via het door de toezichthouder aangeboden web formulier. De kennisgeving aan de toezichthouder moet naast deze gegevens ook de gevolgen van de inbreuk op de persoonsgegevens en de maatregelen die zijn voorgesteld of heeft getroffen om de inbreuk aan te pakken bevatten. Het aanspreekpunt "AVG SIG" of de bestuurder informeert de betrokkenen (bijv. cliënten of werknemers) die geraakt zijn door het datalek. Het managmentteam is hierbij betrokken in verband met een mogelijk reputatierisico. De berichtgeving kan bijvoorbeeld gedaan worden door betrokkene te bellen of via een brief. In uitzonderlijke situaties kan een bericht op de website worden geplaatst (als betrokkenen niet op een andere manier bereikt kunnen worden). De kennisgeving aan betrokkenen (zoals deelnemers of werknemers) moet in ieder geval de volgende informatie bevatten: de aard van de inbreuk in verband met persoonsgegevens, een telefoonnummer of webpagina waar meer informatie over de inbreuk kan worden verkregen en aanbevelingen om mogelijke negatieve gevolgen van de inbreuk voor betrokkenen te beperken.

Activiteit	**6. Terugkoppeling melder.**
Uitvoerende	Coördinator informatiebeveiliging/Functionaris gegevensbescherming of aanspreekpunt "AVG SIG"
Verantwoordelijke	Aanspreekpunt "AVG SIG"
Beschrijving	Na oplossen van het beveiligingsincident/datalek wordt de melder ingelicht dat het incident is opgelost en gevraagd of het incident kan worden afgesloten.

Activiteit	**7. Incident sluiten.**
Uitvoerende	Coördinator informatiebeveiliging/Functionaris gegevensbescherming
Verantwoordelijke	Kwaliteitsmanager/bestuurssecretaris Carante Groep
Beschrijving	Indien de melder akkoord is met de afhandeling van het incident/datalek sluit het aanspreekpunt "AVG SIG" het incident in het fobovolgsysteem.

Activiteit	8. Rapportage
Uitvoerende	Aanspreekpunt “AVG SIG”
Verantwoordelijke	Bestuurder
Beschrijving	Het aanspreekpunt “AVG SIG” houdt een overzicht bij van de datalekken en informatiebeveiligingsincidenten, met daarin onder meer de gevolgen hiervan en de herstelmaatregelen die zijn genomen. Dit overzicht mag uitsluitend de voor dit doel noodzakelijke gegevens bevatten. Deze rapportage zal per kwartaal worden opgesteld door de het aanspreekpunt “AVG SIG” en aangeleverd aan de bestuurder.

18 Documenten behorende bij proces

Soort document	Naam document	Extra gegevens
Extern	Beleidsregels voortoepassing van artikel 34a van de Wbp	Zie: https://cbpweb.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf

19 Applicaties behorende bij proces

Naam applicatie	Doel applicatie
Foboverbetersysteem	Registratie van beveiligingsincidenten en datalekken

20 Escalatieproces

Incident/datalek	betrokkenen	Urgentie
Datalek bij een verwerker/toeleverancier van Carante Groep F,I&A	FG CG AVG SIG Bestuurder	Hoog
Datalek waarbij persoonsgegevens zijn getroffen	AVG SIG Bestuurder	Hoog
Inbraak op het netwerk of een bedrijfsapplicatie	FG CG AVG SIG Bestuurder	Hoog
Uitbraak virus (malware)	FG CG AVG SIG Bestuurder	Hoog
Uitval kritieke bedrijfsapplicatie langer dan in afspraken is afgesproken	FG CG AVG SIG Bestuurder	Hoog
Uitval Firewall(s)	FG CG AVG SIG Bestuurder	Hoog
Uitval Virusprotectie	FG CG AVG SIG Bestuurder	Hoog

Incident/datalek	betrokkenen	Urgentie
Niet-functionerende beveiligingsmaatregel(en)	FG CG AVG SIG Bestuurder	Hoog
Verlies of diefstal apparatuur / informatiedrager(s) / papieren documenten met persoonsgegevens	AVG SIG Bestuurder	Hoog
Verlies of diefstal apparatuur zonder persoonsgegevens	AVG SIG Bestuurder	Midden
Niet afgesloten kasten of bureaus met vertrouwelijke documenten	AVG SIG Bestuurder	Midden
Zichtbare notitieblaadjes met toegangsgegevens	AVG SIG Bestuurder	Hoog