Informatiebeveiligingsbeleid Weverslo

Versie: 1

Datum: 23 mei 2018

Vastgesteld door: Gé Peterink

Vastgesteld op: 23 mei 2018

Vaststelling beleid

Dit informatiebeveiligingsbeleid treedt in werking direct na vaststelling. Het beleid wordt iedere twee jaar en in ieder geval na een wijziging van wet- of regelgeving rond informatiebeveiliging geëvalueerd en zo nodig herzien. De meest actuele versie van dit beleid is te vinden in het handboek op de schijf.

Privacybeleid Weverslo

Weverslo heeft de wijze waarop zij de bescherming van de privacy van persoonsgegevens waarborgt, vastgelegd in informatiebeveiligingsbeleid. Daarin is aangegeven hoe alle persoonsgegevens waarover Weverslo beschikt, worden beveiligd en gerespecteerd.

Basis van het beleid is dat Weverslo alleen persoonsgegevens gebruikt die met goedkeuring van betrokkenen zijn verworven. Deze worden alleen en uitsluitend worden gebruikt voor het doel waarmee ze zijn verworven en voor de communicatie tussen betrokkenen en Weverslo.

In afwijking van de basisregel verstrekt Weverslo alleen persoonsgegevens aan betrokkenen aan wie zij dat wettelijk verplicht is zoals:

- het beschikbaar hebben van een openbaar grafregister volgens de Wet op de Lijkbezorging;
- gegevens van medewerkers ten behoeven van fiscale en verzekeringsinstanties.

De wijze waarop de informatiebeveiliging gestalte krijgt is uitgewerkt in uitvoeringsmaatregelen gericht op:

- Beleid en organisatie
- Documentenbeheer
- Medewerkers instructie
- ICT
- Uitwisseling en communciatie

Klik hier om de beleidsnotitie informatiebeveiligingsbeleid Weverslo te lezen.

Inhoudsopgave

1. Strategisch beleid informatiebeveiliging 3
1.1. Leiderschapsverklaring 3
1.2. Beleidsverklaring 3
2. Tactisch beleid informatiebeveiliging 5
2.1. Beleid en organisatie 5
2.2. Gegevens en documenten 5
2.3. Algemene Verordening Gegevensbescherming (AVG) 5
2.4. Medewerkers en bewustzijn 6
2.5. Fysieke maatregelen 7
2.6. Logische toegang 7
2.7. ICT 7
2.8. Uitwisseling en communicatie 8
2.9. Leveranciers met raakvlakken tot ICT 8
2.10. Continuïteit 8
2.11. Controle en naleving 8
2.12. Incidenten 9

1. Strategisch beleid informatiebeveiliging

1.1. Leiderschapsverklaring

De directie stelt het informatiebeveiligingsbeleid op, zorgt dat het bij de medewerkers bekend is en geeft leiding aan de uitvoering ervan. Het informatiebeveiligingsbeleid geeft richting en beschrijft de principes op basis waarvan Weverslo omgaat met informatie, inclusief persoonsgegevens.
Het informatiebeveiligingsbeleid legt de doelstelling van informatiebeveiliging vast, samen met de verantwoordelijkheden. De directie neemt zijn verantwoordelijkheid bij het realiseren van een passend niveau van informatiebeveiliging en privacy binnen Weverslo. Hiervoor worden mogelijkheden en middelen ter beschikking gesteld, passend bij het vereiste niveau van beveiliging en privacy.
De werking van deze beleidsnotitie omvat de Stichting Meditatienatuur Nederland, de Natuurbegraafplaats Weverslo en het Landgoed Weverslo. Deze organisaties worden hierna aangeduid als Weverslo.

1.2. Beleidsverklaring

Elke medewerker moet zich houden aan de beleidsregels inzake zorgvuldig omgaan met persoonsgegevens binnen Weverslo. Zorgvuldigheid, vertrouwen en kwaliteit van dienstverlening zijn hierbij belangrijke kernwaarden. Binnen alle bedrijfsprocessen van Weverslo vervult de informatievoorziening een cruciale rol. Weverslo wil daarom op een verantwoorde manier met informatie omgaan, wat betekent dat de kwaliteit van informatievoorziening onder controle moet zijn. Omdat Weverslo veel met persoonsgegevens te maken heeft en dient te voldoen aan de Algemene Verordening Gegevensbescherming, valt de bescherming van de rechten van natuurlijke personen ten aanzien van hun persoonsgegevens onder deze verantwoorde manier van omgaan met informatie. Een organisatiebrede aanpak van informatiebeveiliging, inclusief de bewaking van (ten aanzien van de betrokkenen) rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens, vervult hierin een sleutelrol.

Wanneer informatiebeveiliging onvoldoende aandacht krijgt, loopt Weverslo onnodige risico's. Deze kunnen onder meer leiden tot financiële schade, juridische gevolgen en imagoverlies.

Informatiebeveiliging richt zich op de belangrijkste kwaliteitsindicatoren van de informatievoorziening, namelijk:

- Beschikbaarheid - Is de informatie voorhanden op het moment dat het nodig is?
- Integriteit - Is de informatie correct en compleet?
- Vertrouwelijkheid - Komt de informatie alleen onder ogen van diegenen die het daadwerkelijk onder ogen mogen krijgen?

Informatie kent een drietal verschijningsvormen:

- Fysieke informatie: Informatie die zich in documenten, rapporten, contracten, procedures, werkafspraken en vele andere afgedrukte of geschreven documentatie bevindt;
- Digitale informatie: Informatie die zich in informatiesystemen bevindt, die elektronisch wordt verstuurd of opgeslagen ligt op digitale gegevensdragers;
- Niet-tastbare informatie: Datgene wat zich bij medewerkers in het hoofd bevindt, en wat enerzijds niet gedocumenteerd is (en daarmee de beschikbaarheid van informatievoorziening raakt) en wat anderzijds geheim gehouden moet worden (wat de vertrouwelijkheid van informatievoorziening raakt).

Hoewel de nadruk van dit beleid ligt op de digitale informatievoorziening, vallen ook de fysieke en niet-tastbare informatie binnen het bereik van het informatiebeveiligingsbeleid en de bijbehorende maatregelen.
Het vereiste kwaliteitsniveau van de informatievoorziening wordt bereikt door een passend stelsel van maatregelen, waarmee de beschikbaarheid, integriteit en vertrouwelijkheid van informatie worden gewaarborgd. De pijlers van deze maatregelen zijn mensen, processen en techniek. Maatregelen worden in het informatiebeveiligingsproces genomen naar aanleiding van de analyse van die risico's. De keuze van de passende maatregelen vindt plaats op basis van reële risico's (en de beoordeling daarvan) die Weverslo en de cliënten lopen.

De doelstelling van informatiebeveiliging en het bijbehorende stelsel van maatregelen is het waarborgen van de continuïteit van de bedrijfsvoering, het voorkomen van beveiligingsincidenten en het minimaliseren van schade en gevolgen wanneer een incident zich onverhoopt toch voordoet. Dit informatiebeveiligingsbeleid maakt de genomen maatregelen toetsbaar en geeft Weverslo duidelijkheid bij het beleggen van taken, bevoegdheden en verantwoordelijkheden.

Het is de verantwoordelijkheid van alle medewerkers van Weverslo zich aan de beschreven maatregelen te houden en proactief te werken aan de verbetering van de kwaliteit van de informatievoorziening en het waarborgen van de informatiebeveiliging. Dit wordt tevens verlangd van externe (contract)partijen die invloed hebben op het niveau van informatiebeveiliging binnen het kantoor.

Het informatiebeveiligingsbeleid wordt periodiek door de directie opnieuw bekeken en de werking van de beschreven maatregelen wordt met regelmaat getoetst en geëvalueerd. Tussentijdse beoordeling van het beleid en maatregelen kan worden uitgevoerd bij significante wijzigingen in de bedrijfsvoering of bij externe ontwikkelingen, zoals relevante wijzigingen in wet- en regelgeving.

Dit strategische beleid is verder uitgewerkt op tactisch niveau in het volgende hoofdstuk.

2. Tactisch beleid informatiebeveiliging

In dit hoofdstuk is het tactisch beleid informatiebeveiliging uitgewerkt.
Het is onderverdeeld in de volgende paragrafen:

- Beleid en organisatie;
- Gegevens en documenten;
- Algemene Verordening Gegevensbescherming (AVG);
- Medewerkers en bewustzijn;
- Fysieke maatregelen;
- Logische toegang;
- ICT;
- Uitwisseling en communicatie;
- Leveranciers met raakvlakken tot ICT;
- Continuïteit;
- Controle en naleving;
- Incidenten.

2.1. Beleid en organisatie

- Dit informatiebeveiligingsbeleid is opgesteld, vastgesteld door de directie en bekendgemaakt;
- Het beleid wordt periodiek geactualiseerd;
- De directie is eindverantwoordelijk voor de informatiebeveiliging van Weverslo en:
    - bevordert de informatiebeveiliging binnen de organisatie;
    - adviseert gevraagd en ongevraagd daarover;
    - stimuleert het bewustzijn van de medewerkers op dit gebied;
    - organiseert de invoering van aanvullende maatregelen;
    - rapporteert hierover aan de besturen.

2.2. Gegevens en documenten

Van alle (categorieën) informatie die door Weverslo wordt verwerkt en/of geproduceerd is bekend:

- Wie de eigenaar/verantwoordelijke is en;
- Of deze informatie ‘publiek’, ‘intern vertrouwelijk’ of ‘geheim’ is. Publieke informatie is voor iedereen toegankelijk; Intern vertrouwelijke informatie alleen voor medewerkers van het kantoor en geheime informatie alleen voor een beperkte groep binnen het kantoor.

2.3. Algemene Verordening Gegevensbescherming (AVG)

Weverslo gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van cliënten en andere betrokkenen. Weverslo houdt zich hierbij aan de volgende uitganspunten:

- *Rechtmatigheid, behoorlijkheid, transparantie*: Persoonsgegevens worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is;

- *Doelbinding*: Weverslo verwerkt persoonsgegevens voor uitdrukkelijk omschreven en gerechtvaardigde doelen;
- *Dataminimalisatie*: Weverslo verwerkt alleen de gegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. Persoonsgegevens worden niet op meer plaatsen bewaard en verwerkt dan noodzakelijk voor dit doel;
- *Bewaartermijn*: Persoonsgegevens worden niet langer bewaard dan nodig. Het bewaren van persoonsgegevens kan nodig zijn voor het doel waarvoor zij zijn verzameld, voor het uitoefenen van wettelijke taken en het nakomen van wettelijke verplichtingen of het uitvoeren van overeenkomsten;
- *Integriteit en vertrouwelijkheid*: Weverslo gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor gegevens zijn verzameld. Daarbij zorgt Weverslo voor een passende beveiliging van persoonsgegevens;
- *Delen met derden*: In het geval van samenwerking met externe partijen waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt Weverslo afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. Weverslo controleert deze afspraken jaarlijks;
- *Subsidiariteit*: Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokkene zoveel mogelijk beperkt;
- *Proportionaliteit*: De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot het met de verwerking te dienen doel;
- *Rechten van de betrokkene*: Weverslo honoreert alle rechten van cliënten en andere betrokkenen ten aanzien van de verwerking van diens persoonsgegevens.

En verder:

- De verplichte registraties van gegevensverwerkingen worden bijgehouden, in overeenstemming met de eisen uit de AVG;
- Er is een werkende procedure voor het bijhouden en melden van datalekken, zoals beschreven in de AVG;
- Met alle leveranciers die binnen de AVG als Verwerker worden gekenmerkt zijn verwerkingsovereenkomsten afgesloten conform de eisen van de AVG.

2.4. Medewerkers en bewustzijn

- De directie heeft geverifieerd dat medewerkers geschikt zijn voor de betreffende rollen;
- De medewerkers hebben duidelijke en complete informatie gekregen over informatiebeveiliging, de geldende regels en over het van hun verwachte gedrag. Ze begrijpen hun verantwoordelijkheden;
- De directie draagt er zorg voor dat medewerkers zich bewust zijn van de mate waarin de informatie waarmee zij werken beschikbaar, integer en vertrouwelijk moet zijn, welke risico's er bestaan, waardoor hier niet aan voldaan zou worden, en welke maatregelen genomen zijn om die risico's te beheersen;
- De directie heeft formele afspraken gemaakt met medewerkers over wat van die medewerkers wordt verwacht en over de mogelijke sancties indien een medewerker zich niet houdt aan die afspraken.

2.5. Fysieke maatregelen

Er wordt gebruik gemaakt van specifieke fysieke beveiligingsmaatregelen, passend bij de aard van de te beschermen informatie:

- De toegang tot de werkruimtes is alleen toegestaan aan bevoegd personeel en er zijn fysieke beveiligingsmaatregelen genomen om dit te bewaken bijvoorbeeld met behulp van sloten;
- Personeel bergt vertrouwelijke informatie na gebruik goed op en apparatuur wordt, indien niet gebruikt, vergrendeld;
- Passende maatregelen zijn genomen om in geval van stroomuitval de dienstverlening te kunnen voortzetten;
- Apparatuur, waarop informatie wordt verwerkt of is opgeslagen, wordt conform voorschriften van de leverancier onderhouden, door bevoegd personeel;
- Specifieke maatregelen zijn genomen en er zijn regels opgesteld om veilig om te kunnen gaan met bedrijfsmiddelen (laptops, tablets, etc.) buiten het kantoor;
- Informatiedragers inclusief papieren documenten met vertrouwelijke informatie, die niet meer nodig zijn, worden vernietigd (bijvoorbeeld door middel van een shredder) of afgevoerd door een gespecialiseerd vernietigingsbedrijf;
- Alleen onomkeerbaar geschoonde apparatuur mag buiten het notariskantoor worden hergebruikt.

2.6. Logische toegang

- Vastgesteld is welke medewerkers met welke rollen toegang mogen hebben tot welke informatie en systemen;
- Medewerkers krijgen gebruikersnamen en wachtwoorden, met de bijbehorende rechten;
- Medewerkers delen hun wachtwoorden met niemand en zorgen ervoor dat ze aan niemand bekend kunnen raken;
- Bij wijziging van rollen worden de toegangsrechten zo nodig aangepast;
- Bij beëindiging van de inzet van een medewerker worden toegangsrechten ingetrokken;
- Periodiek worden uitgegeven toegangsrechten gecontroleerd op correctheid, zodat onterecht uitgedeelde rechten kunnen worden ingetrokken.

2.7. ICT

Er zijn specifieke regels over hoe wordt omgegaan met encryptie (versleutelingstechnieken) voor het beschermen van gegevens:

- Mobiele apparatuur (laptops, tablets, smartphones) is altijd versleuteld;
- usb-sticks worden niet gebruikt.

Verder geldt het volgende:

- Het omgaan met de ICT-omgeving is op passende wijze gedocumenteerd, zodat Weverslo niet afhankelijk is van de kennis van één of een aantal personen die alles in het hoofd hebben zitten;
- Wijzigingen op de IT-omgeving worden alleen beheerst doorgevoerd waarbij ook aandacht is voor de informatiebeveiliging;
- Antivirussoftware wordt op alle computersystemen toegepast en up-to-date gehouden;
- Regelmatig wordt gecontroleerd dat back-ups van belangrijke informatie zijn gemaakt. Regelmatig wordt getest dat back-ups gelukt zijn en dat data daadwerkelijk terug te zetten zijn;

- Alle besturingssystemen op computerapparatuur (werkplekken, mobiele apparatuur, servers, netwerkapparatuur, firewalls) en de geïnstalleerde gebruikersprogramma's worden structureel voorzien van updates en patches, zodat de kwetsbaarheid van de IT-omgeving wordt beperkt. Dit wordt door Notis verzorgd.

2.8. Uitwisseling en communicatie

- Het computernetwerk van Weverslo wordt gemonitord, beheerd en beveiligd om informatie te beschermen. Dit gebeurt ook door Martijn Fleurkens , die een realtime monitoromgeving hiervoor heeft;
- Over de uitwisseling van informatie tussen Weverslo en cliënt worden afspraken gemaakt en nagekomen, waarbij de cliënt bepaalt of diens gegevens bijvoorbeeld onversleuteld via e-mail mogen worden verzonden. De cliënt wordt aangeraden om gegevensuitwisseling te laten plaatsvinden via expliciet veilige kanalen, zoals een digitaal uitwisselplatform;
- Ook met leveranciers en andere partijen worden dergelijke afspraken gemaakt en nagekomen;
- Bij e-mails wordt gezorgd dat e-mailadressen van anderen niet zonder toestemming zichtbaar zijn voor geadresseerden;
- Bij e-mails met vertrouwelijke gegevens is extra aandacht voor juiste adressering en dat de juiste bijlage bij de e-mail zit.

2.9. Leveranciers met raakvlakken tot ICT

- Met leveranciers die toegang tot informatie van Weverslo krijgen, worden formele afspraken gemaakt over het nemen van specifieke informatiebeveiligingsmaatregelen, het rapporteren van beveiligingsincidenten en de controlemogelijkheden door Weverslo hierop. Als de betreffende informatie persoonsgegevens betreft, wordt een verwerkingsovereenkomst afgesloten conform in paragraaf 2.3 Algemene Verordening Gegevensbescherming (AVG) gesteld;
- Met de leverancier is afgesproken dat bovenbedoelde afspraken ook gelden voor door die leverancier ingeschakelde onderaannemers en dat de leverancier verantwoordelijk is voor de nakoming van haar onderaannemers;
- Bij aanschaf of ontwikkeling van nieuwe informatiesystemen of IT-voorzieningen, worden specifieke beveiligingseisen opgesteld, waar het product en het ontwikkelproces aan moeten voldoen. Denk hierbij aan beveiligd ontwikkelproces, beveiliging van communicatie en opslag (encryptie), patching, logische toegang, privacy by default, privacy by design etc.).

2.10. Continuïteit

- Er is een bedrijfscontinuïteitsplan opgesteld en daarin is ook aandacht voor de continuïteit van de informatiebeveiliging;
- Het bedrijfscontinuïteitsplan wordt periodiek getest en indien nodig geactualiseerd naar aanleiding van de tests.

2.11. Controle en naleving

- Op het gebied van informatiebeveiliging voldoet Weverslo minimaal aan het gestelde in:
    - De Wet op de Lijkbezorging;

  - Algemene Verordening Gegevensbescherming (AVG);
  - Uitvoeringswet Algemene Verordening Gegevensbescherming (nu nog wetsvoorstel);
  - Wet Computercriminaliteit II
  - Comptabiliteitswet
  - Archiefwet
  - Wet SUWI
  - Wet op de identificatieplicht
  - Wet Elektronisch Bestuurlijk Verkeer (WEBV)
  - Wet GBA en wet BRP
  - Wet Werk en Bijstand
  - Registratiewet
  - Wet Openbaarbaarheid van Bestuur
  - Algemene wet bestuursrecht
  - Algemene wet rijksbelastingen
  - Richtlijnen van het Nationaal Cyber Security Centrum (NCSC);
- De directie ziet toe op het naleven van wettelijke verplichtingen m.b.t. intellectueel eigendom, auteursrechten en gebruiksrechten;
- Van registraties zijn classificatie en bewaartermijnen vastgelegd;
- De directie toetst de naleving van dit beleid;
- De informatiebeveiliging van Weverslo wordt periodiek onafhankelijk beoordeeld en de resultaten worden aan de directie gerapporteerd.

2.12. Incidenten

- Informatiebeveiligingsincidenten worden volgens een vaste werkwijze
  - Gemeld bij het aanspreekpunt;
  - Vastgelegd (in een register voor informatiebeveiligingsincidenten en datalekken);
  - Behandeld;
- Hiervan wordt geleerd en die kennis wordt gebruikt om herhaling te voorkomen.

2.13 Andere documenten

De reeds eerder opgestelde documenten, zoals de regels en richtlijnen voor gebruikers, het Handboek, het CRM en het gebruik van internet via het interne netwerk, blijven van kracht.