Spinware Solutions B.V.
veilig werken met de cloud

Informatiebeveiligingsbeleid

2024

Inhoudsopgave

1. Inleiding

Spinware Solutions erkent het cruciale belang van informatiebeveiliging in de moderne zakelijke omgeving, vooral in de context van de voortdurende digitalisering en automatisering van processen. Als een toonaangevend ICT-bedrijf streven we ernaar om de hoogste normen van integriteit, beschikbaarheid en beveiliging van geautomatiseerde gegevens te handhaven.

Dit informatiebeveiligingsbeleid vormt de basis van ons streven om de **vertrouwelijkheid**, **integriteit** en **beschikbaarheid** van gegevens te waarborgen, en om risico's te beheren die kunnen ontstaan door interne of externe bedreigingen.

Ons beleid is gebaseerd op internationale standaarden en best-practices op het gebied van informatiebeveiliging, zoals ISO/IEC 27001, NIST Cybersecurity Framework en GDPR. Door deze standaarden te volgen, kunnen we onze klanten verzekeren van een veilige en betrouwbare omgeving voor hun gegevens en systemen.

Er worden richtlijnen, procedures en verantwoordelijkheden in beschreven die van toepassing zijn op alle medewerkers, leveranciers en partners van Spinware Solutions. Het beoogt een cultuur van bewustzijn en naleving van informatiebeveiligingsprincipes te bevorderen, waarbij elke medewerker een actieve rol speelt in het beschermen van gevoelige informatie en het minimaliseren van risico's.

Het is een levend document dat regelmatig wordt herzien en bijgewerkt om te blijven voldoen aan veranderende bedreigingen, technologische ontwikkelingen en wettelijke vereisten. Door voortdurende evaluatie en verbetering van onze processen streven we naar een robuust en veerkrachtig informatiebeveiligingskader dat de kernwaarden van onze organisatie weerspiegelt en het vertrouwen van onze klanten behoudt.

1.1. Reikwijdte

Het beleid informatiebeveiliging ziet op de directie en alle werknemers van Spinware Solutions. Daarnaast is het beleid informatiebeveiliging ook van toepassing op door Spinware Solutions ingeschakelde derden.

Het beleid informatiebeveiliging dient in samenhang te worden gelezen met andere relevante documenten die raakvlakken hebben met informatiebeveiliging, zoals het privacybeleid.

2. Interne organisatie van informatiebeveiliging

2.1. Rollen en verantwoordelijkheden

De directie van Spinware Solutions is verantwoordelijk voor alle aspecten van het informatiebeveiligingsbeheer van Spinware Solutions en is als zodanig verantwoordelijk voor de bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie binnen het bedrijf.

De volgende functies hebben een specifieke verantwoordelijkheid:

Rollen	Verantwoordelijkheden
Directie Rudolf Philipse	• Verantwoordelijk voor alle aspecten van informatiebeveiliging en het beheersen van ICT-risico's binnen Spinware Solutions. • Jaarlijkse evaluatie en goedkeuring van het beleid informatiebeveiliging en gerelateerde processen, procedures en controles. • Reageren op informatiebeveiligingsincidenten en datalekken. • Verantwoordelijk voor het monitoren van de uitbestede IT-systemen • Implementeren en onderhouden van trainingsprogramma's voor informatiebeveiliging (bewustzijn).
Medewerkers	• Voldoen aan het beleid informatiebeveiliging en aanverwante processen, procedures, vereisten en controles. • Melden van eventuele (poging tot) inbreuken op de informatiebeveiliging of mogelijke tekortkomingen in de informatiebeveiliging.

De interne IT-diensten kunnen als volgt geformuleerd worden:

Zusterbedrijf Mulberry Garden levert het CRM-systeem (SpinOffice CRM) waar alle klantgegevens in worden opgeslagen. Alle data in het worden in een hosted-cloud opgeslagen bij Amazon Web Services (AWS) in Ierland. Voor integratie met externe partijen levert Mulberry Garden enkele API's zoals een WhatsApp integratie via MessageBird, Mollie t.b.v. betalingen en e-boekhouden voor de facturatie.

De medewerkers van Spinware Solutions werken op een Remote Desktop werkplek. Op deze werkplekken draaien applicaties waarvan de data in de cloud wordt opgeslagen (Microsoft 365 en SpinOffice CRM).

De Remote Desktop omgeving wordt gehost in een datacenter in Rotterdam. Alle servers staan achter een firewall die zorgt voor bescherming. Op alle servers is antivirussoftware geïnstalleerd: alle inkomende mails worden gescand voordat ze beschikbaar worden gesteld aan de gebruiker.

Samson IT levert een telefoon- en internet omgeving nodig. Voor telefonie wordt gebruikgemaakt van het product Xelion en voor internet wordt gebruik gemaakt van het netwerk van KPN. De telefonie is geïntegreerd in het CRM-systeem.

2.2. Jaarlijkse herziening

Dit informatiebeveiligingsbeleid zal jaarlijks of vaker worden herzien als er significante wijzigingen optreden om blijvende geschiktheid, adequaatheid en effectiviteit te waarborgen. Tevens zullen de IT-inrichting en beheersing jaarlijks worden geëvalueerd.

3. Personele zaken

De medewerking van alle medewerkers op het gebied van informatiebeveiliging is essentieel.

3.1. Screening

Het is belangrijk dat Spinware Solutions haar betrouwbare reputatie behoudt. Spinware Solutions zal daarom bij aanvang van het dienstverband een screening uitvoeren. Onderdeel van de screening zijn een verklaring omtrent gedrag (VOG) en een referentiecontrole.

3.2. Opdracht- en arbeidsovereenkomsten

Alle opdracht- en arbeidsovereenkomsten bevatten clausules met betrekking tot vertrouwelijkheid, intellectueel eigendom en gegevensbescherming. Dit geldt ook voor ingeschakelde derden.

3.3. Eed of belofte

Spinware Solutions verplicht haar medewerkers om de eed of belofte af te leggen. De eed/belofte is een moreel-ethische verklaring en bevat verklaringen op het gebied van onder meer het centraal stellen van het klantbelang, geen misbruik maken van kennis, geheimhouding van hetgeen is toevertrouwd en het maken van een zorgvuldige belangenafweging.

3.4. Training en awareness

Alle personen werkzaam bij Spinware Solutions ontvangen passende educatie en training en regelmatige updates met betrekking organisatiebeleid en -procedures, voor zover relevant voor hun functie.

Jaarlijks krijgen alle medewerkers trainingen op maat. Daarnaast worden persoonsgebonden trainingen aangeboden om het personeel structureel te ontwikkelen.

Nieuwe ontwikkelingen qua beleid en organisatie worden op diverse wijzen gecommuniceerd. Kleine wijzigingen worden door middel van mail verspreid. Grotere wijzigingen middels interne presentaties. Nieuwe procedures of beleid worden op een passende wijze gecommuniceerd.

3.5. Einde van dienstverband en intrekken rechten

Wanneer de rol van een werknemer of opdrachtnemer binnen Spinware Solutions verandert, of wanneer het dienstverband van de werknemer wordt beëindigd, geldt het volgende:

- Kennis wordt overgedragen aan een opvolger of aan een collega;
- Verantwoordelijkheden worden opnieuw toegewezen en toegangsrechten worden ingetrokken (indien nodig); en
- De werknemer/opdrachtnemer moet alle eigendommen van het bedrijf inleveren op de laatste dag van het dienstverband.

4. Hardware en software

4.1. Inkoop

De directie van Spinware Solutions beslist over de aankoop, het gebruik, de vervanging en de verwijdering van IT-apparatuur en software. Spinware Solutions houdt een overzicht bij van alle uitbestedingspartners die een kritieke of belangrijke functie in de organisatie ondersteunen.

4.2. Het gebruik van hardware

Medewerkers mogen de IT-voorzieningen alleen gebruiken voor werk-gerelateerde activiteiten. Elke gebruiker is verantwoordelijk voor het correcte gebruik van de toegewezen hardware.

Verliezen, diefstal, schade, manipulatie of andere incidenten die de informatiebeveiliging in gevaar brengen, moeten zo snel mogelijk worden gemeld aan de directie van Spinware Solutions, zodat hier passende actie op kan worden genomen.

4.2.1. Algemene voorschriften

Ten aanzien van hardware gelden de volgende algemene regels:

- Desktopcomputers, laptops, tablets en andere mobiele apparaten (ook persoonlijke apparaten waarop gegevens van Spinware Solutions staan) moet worden beschermd door een wachtwoord of pincode.
- Versleuteling moet zijn ingeschakeld op computers (ook persoonlijke apparaten waarop gegevens van Spinware Solutions staan).
- Desktopcomputers, laptops, tablets en andere mobiele apparaten (ook persoonlijke apparaten waarop gegevens van Spinware Solutions staan) moet een antivirus/anti-malware tool hebben (geïnstalleerd en bijgewerkt).
- Gebruikers kunnen de benodigde software installeren zolang deze over de juiste licentie beschikt en op geen enkele manier schadelijk is voor de beveiliging en privacy van de laptop. Gebruik van software zonder licentie is illegaal en dus niet toegestaan.

4.2.2. Wachtwoordbeleid

Alle hardware waarop gegevens van Spinware Solutions zijn opgeslagen (ook in het geval van *bring-your-own-device*), dienen adequaat te worden beveiligd. In principe wordt er geen hardware gebruikt waar gegevens worden opgeslagen. Alle informatie staat in de cloud.

Medewerkers dienen gebruik te maken van een sterk wachtwoord, dat niet met anderen gedeeld mag worden. Een sterk wachtwoord bevat de volgende elementen:

- Tenminste 8 tekens;
- Complexiteit = aan;
- Twee-factor authenticatie dient te zijn ingesteld

4.3. Retourneren van hardware

Aan het einde van het dienstverband (op de laatste werkdag) dient de vertrekkende medewerker of opdrachtnemer hardware die toebehoort aan Spinware Solutions te retourneren. Alle persoonlijke gegevens mogen voor het inleveren worden verwijderd, maar bedrijfsdocumenten moeten op de hardware worden achtergelaten.

4.4. Installeren updates software

In updates van software worden veelal de laatst bekende zwakheden ten aanzien van informatiebeveiliging opgelost. Het is derhalve van belang dat medewerkers altijd de laatste versie van de door hen gebruikte software installeren. Deze installatie dient zo snel mogelijk na het uitkomen van de update te worden geïnstalleerd, maar uiterlijk binnen 24 uur.

5. Dataclassificatieschema

5.1. Classificatieniveaus

Spinware Solutions heeft een dataclassificatieschema (BIV) opgesteld dat gebaseerd is op de risico's aan de hand waarvan alle IT-systemen en data worden ingedeeld in:

- Geheim
- Vertrouwelijk
- Publiek

5.1.1. Geheim

De dataclassificatie 'geheim' is van toepassing op de meest gevoelige bedrijfsinformatie waarvan ongeoorloofde openbaarmaking zwaarwegende gevolgen kan hebben voor Spinware Solutions, haar klanten, haar zakelijke partners en haar dienstverleners. Spinware Solutions loopt een hoog risico op aanzienlijk financieel verlies, wettelijke aansprakelijkheid, wantrouwen of schade van het publiek, als 'geheime' gegevens worden bekendgemaakt, gecompromitteerd of verloren gaan. Voorbeelden zijn:

- Persoonlijke gegevens, waaronder persoonlijk identificeerbare informatie zoals nationale identificatienummers, paspoortnummers en rijbewijsnummers;
- Financiële gegevens, inclusief financiële rekeningnummers;
- Zakelijk materiaal, zoals documenten of gegevens die uniek of specifiek intellectueel eigendom zijn;
- Verificatiegegevens, inclusief cryptografiesleutels, naam-gebruiker paren of andere identificatiesequenties.

Gegevens die zijn geclassificeerd als 'geheim' kennen vaak wettelijke vereisten, zoals bijvoorbeeld opgenomen in de Algemene verordening gegevensbescherming (AVG).

5.1.2. Vertrouwelijk

De classificatie 'vertrouwelijk' is van toepassing op gemiddeld-gevoelige bedrijfsinformatie waarvan ongeoorloofde openbaarmaking een matig of beperkt risico kan hebben op financieel verlies, wettelijke aansprakelijkheid, publiek wantrouwen of schade aan Spinware Solutions, haar klanten, haar zakelijke partners en haar dienstverleners, indien deze gegevens worden bekendgemaakt, aangetast of verloren.
Voorbeelden zijn:

- E-mails die kunnen worden verwijderd of publiekelijk geopenbaard zonder een crisis te veroorzaken;
- Documenten en bestanden die geen 'geheim' gecategoriseerde gegevens bevatten.

Met uitzondering van gegevens die 'publiek' of 'geheim' zijn, kunnen alle gegevens binnen Spinware Solutions standaard worden geclassificeerd als 'vertrouwelijk'.

5.1.3. Publiek

De classificatie ‘publiek’ is van toepassing op informatie die niet kritisch is voor de activiteiten van Spinware Solutions en die door het management van Spinware Solutions is goedgekeurd voor openbaarmaking. Per definitie bestaat er niet zoiets als ongeoorloofde openbaarmaking van deze informatie en deze kan zonder potentiële schade worden verspreid. Er is geen of een onbeduidend risico op financieel verlies, wettelijke aansprakelijkheid, wantrouwen of schade aan Spinware Solutions, haar klanten, zakelijke partners en dienstverleners, als deze gegevens worden bekendgemaakt, gecompromitteerd of verloren gaan.

5.2. Beveiligingsmaatregelen per classificatieniveau

5.2.1. Geheim en vertrouwelijk

- Toegang tot en gebruik van ‘geheim’ en ‘vertrouwelijk’ geclassificeerde gegevens voldoet aan een (zeer) strikt *need-to-know* principe; alleen indien toegang tot de gegevens noodzakelijk is voor het uitvoeren van de werkzaamheden, kan toegang worden verkregen.
- Als ‘geheim’ en ‘vertrouwelijk’ geclassificeerde gegevens worden opgeslagen op een computer, laptop, tablet, mobiele telefoon of een ander systeem, dan moet het systeem voldoen aan de door Spinware Solutions goedgekeurde datatoegang en opslagbeveiliging. Wanneer de gebruiker niet actief gebruik maakt van de ‘geheime’ of ‘vertrouwelijke’ informatie, dient de gebruiker zich op het apparaat uit te loggen, een wachtwoord-beveiligde schermbeveiliging te activeren of anderszins de toegang tot de beperkte informatie te beperken.
- Wanneer ‘geheim’ geclassificeerde informatie via een extern communicatienetwerk moet worden verzonden, mag deze alleen in gecodeerde vorm worden verzonden.
- Gegevensdragers met ‘geheime’ en ‘vertrouwelijke’ informatie moeten volledig gewist zijn voordat dat medium opnieuw wordt toegewezen aan een andere gebruiker of wordt weggegooid. Het is niet voldoende om de gegevens van de media te verwijderen. Er moet een methode worden gebruikt die alle gegevens volledig wist.

5.2.3. Publiek

- Er is geen toegangsbeperking tot gegevens die zijn geclassificeerd als ‘publiek’.

6. Toegangscontrole

6.1. Systeem toegang

Toegang tot systemen is gebaseerd op gebruikersnaam en wachtwoord, en - indien van toepassing - ook op twee-factor authenticatie.

Alleen geautoriseerde gebruikers die toegang tot systemen nodig hebben voor de uitvoering van hun werkzaamheden, krijgen toegang tot (een deel van) systemen die vertrouwelijke informatie bevatten. Toegang wordt verleend volgens het principe '*need-to-know, need-to-have*': elke gebruiker krijgt de rechten en toegang tot middelen die nodig zijn om hun zakelijke werkzaamheden goed te kunnen uitvoeren.

7. Fysieke en omgevingsbeveiliging

7.1. Toegang tot het gebouw

Het kantoor van Spinware Solutions bevindt zich in een bedrijfspand op de 1e verdieping. De ingang van het pand is toegankelijk middels de centrale voordeur. Deze deur te openen door middel van een token of een persoonlijke toegangscode.

De directie beheert de uitgave van tokens en toegangscodes. Er is een overzicht welke medewerker welke tools heeft.

De volgende aanvullende maatregelen gelden:

- Het kantoor moet worden afgesloten op het moment dat er geen medewerkers meer aanwezig zijn;
- Medewerkers laten hun apparaten die toegang kunnen geven tot bedrijfsinformatie en -gegevens op kantoor niet open achter.

Spinware Solutions heeft geen gegevens op de lokale computers staat, alle informatie staat in de cloud. Op kantoor zijn geen gegevens van klanten aanwezig. Er zijn geen fysieke dossiers aanwezig.

7.2. Clean desk

Aan het einde van de dag of wanneer medewerkers niet met documenten werken, dienen papier en andere gegevensdragers veilig (achter slot) te worden opgeborgen.

8. Operationele beveiliging

Dit hoofdstuk beschrijft de aspecten met betrekking tot de goede en veilige werking van de IT-voorzieningen.

8.1. Bescherming tegen virussen en malware

Er worden verschillende beheersmaatregelen genomen met betrekking tot de bescherming tegen schadelijke software.

Firewall
Op de kantoorlocatie wordt gebruikt gemaakt van een fortigate Next Gen firewall met active fortigaurd updates vanuit het Foritgate platform. Hiermee worden actief DNS, & SSL beperking gedaan. Tevens zijn de ingaande porten naar de printers op IP-adres beveiligd.

Het Xelion platform heeft zeer beperkte toegang voor alles dat geen VOIP-telefonie is door middel van een up2date Linux firewall.

8.2. E-mail beveiliging

Alle zakelijke e-mailadressen mogen alleen worden gebruikt voor zakelijke doeleinden van Spinware Solutions. Het gebruik van corporate e-mailadressen voor niet-geautoriseerde advertenties, externe activiteiten, spam, politieke campagnes en ander gebruik dat geen verband houdt met de activiteiten van Spinware Solutions is verboden.

Het is ten strengste verboden om de e-mailadressen te gebruiken voor het verspreiden van berichten die als aanstootgevend, racistisch, obsceen of anderszins in strijd met de wet en ethiek worden beschouwd.

Wanneer een gebruiker zijn/haar relatie met het bedrijf beëindigt, moet het bijbehorende account worden.

Spinware Solutions maakt gebruik van Microsoft 365 voor het e-mailbeheer. Alle e-mailberichten komen binnen bij Microsoft 365 waar een eerste scan wordt uitgevoerd. Alle berichten komen daarna in het CRM-systeem binnen, dit is waar de medewerkers van Spinware Solutions de e-mails vervolgens afhandelen.

8.3. Internetgebruik

Internettoegang is hoofdzakelijk voor zakelijke doeleinden, enig beperkt internetgebruik is toegestaan als hierbij geen merkbare consumptie van de capaciteit plaatsvindt en de productiviteit van het werk niet wordt beïnvloed.

Toegang tot pornografische sites, pokersites, andere gaming-sites, hack-sites en andere risicovolle sites is verboden. Het initiëren of meewerken aan aanvallen zoals denial of service, spam, vissen, fraude, hacking, distributie van twijfelachtig materiaal, inbreuk op auteursrechten en anderen zijn vanzelfsprekend ten strengste verboden.

8.4. Gegevensopslag en -bewaring

Alle data en documenten van Spinware Solutions worden opgeslagen in de cloud van Microsoft 365 en het CRM-systeem SpinOffice.

8.5. Back-up & recovery

Alle data en documenten van Spinware Solutions worden opgeslagen in de cloud van Microsoft 365 en het CRM-systeem SpinOffice.

Back-up & recovery Microsoft 365

Back-up & recovery SpinOffice CRM

Er wordt dagelijks automatisch een kopie gemaakt van de database. De back-ups zijn opgeslagen bij Amazon Web Services, binnen de EU. Voor meer informatie verwijzen wij naar de back-up en data recovery informatie van de desbetreffende partner. (www.spinoffice-crm.com/nl/betrouwbaarheid/)

9. Communicatiebeveiliging

9.1. Informatieoverdracht

Gegevens kunnen op verschillende manieren worden uitgewisseld, bijvoorbeeld:

- Door middel van fysieke drager;
- Via communicatiesystemen;
- Via e-mail.

9.1.1. Fysieke drager

Hoewel het niet de voorkeur heeft, kunnen gegevens worden getransporteerd door middel van fysieke drager, zoals een USB-stick. Na het gebruik van een fysieke drager voor het overbrengen van media, moet de drager nauwkeurig worden gewist of vernietigd.

Deze manier van informatieoverdracht wordt nagenoeg niet meer gebruikt.

9.1.2. Communicatiesystemen

In het geval van gegevensuitwisseling tussen systemen die worden gebruikt door Spinware Solutions, klanten en/of andere derde partijen, worden afspraken gemaakt over onder andere wederzijdse erkenning van systemen, de procedure voor uitwisseling en beveiliging.

9.1.3. E-mail

De uitwisseling van geheime of vertrouwelijke gegevens via e-mail moet zoveel mogelijk worden beperkt, tenzij voldoende gegevensbeschermingsmaatregelen zijn overwogen. Daarbij kan worden gedacht aan versleuteling van verzonden documenten.

10. Dienstverleners

10.1. Samenwerkingsafspraken dienstverleners

Spinware Solutions maakt gebruik van verschillende dienstverleners. Een overzicht van alle partijen met wie Spinware Solutions samenwerkt, bij wie Spinware Solutions inkoopt of aan wie Spinware Solutions uitbesteedt, worden bijgehouden in een separaat overzicht.

Spinware Solutions maakt met alle partijen met wie zij samenwerkt de benodigde afspraken en stelt deze op schrift, waar nodig in overeenstemming met de wettelijke uitbestedingsregels en/of de voorschriften uit de Algemene verordening gegevensbescherming (AVG).

Onderdeel van de samenwerking met leveranciers, is inzage in de informatiebeveiliging. Spinware Solutions legt van de leveranciers ten minste de volgende gegevens vast (gebaseerd op de ISO 27002 – 2022 standaard) en beoordeelt deze bij aanvang van de dienstverlening. Tevens wordt periodiek gecontroleerd of de gegevens nog juist zijn en nog voldoen aan de eisen die Spinware Solutions stelt aan de informatiebeveiliging.

1. Over welke security certificeringen en assurance verklaringen beschikt de leverancier?
2. Beschikt de leverancier over een actueel informatiebeveiligings- en Business Continuity Management (BCM)-beleid? Welke security- en BCM-standaarden zijn hierin opgenomen? Kan het informatiebeveiligings- en BCM-beleid gedeeld worden met Spinware Solutions?
3. Hoe ziet de informatiebeveiligingsorganisatie eruit? Welke functionarissen/afdelingen voor informatiebeveiliging zijn actief (zoals bijv. CISO en een SOC)? Is er een formeel autorisatiebeleid en -proces ingericht?
4. Heeft de leverancier in contracten met onderaannemers vastgelegd dat zij aan een vergelijkbaar niveau van informatiebeveiliging moeten voldoen? Is informatie over de data, systemen en diensten beschikbaar in een (of meer) register(s)?
5. Is de logische toegangsbeveiliging aantoonbaar ingericht?
6. Zijn informatiebeveiliging en rapportages daarover inbegrepen in de overeenkomst/SLA?
7. Beschikt de leverancier over een formeel incidentenmanagementproces waarbij klanten onverwijld worden geïnformeerd?
8. Heeft de leverancier actuele (IT)-herstelplannen inclusief Business Continuity- en Disaster Recovery Plannen? Zijn deze plannen in de afgelopen 12 maanden getest? Beschikt de leverancier over exit-plannen met de onderaannemers?
9. Beschikt de leverancier over een formeel privacy beleid, is deze beschikbaar en wordt deze aantoonbaar nageleefd?
10. Heeft de leverancier in haar organisatie een *Secure Development Life Cycle*? Is een penetratietest onderdeel van deze cyclus en hoe vaak wordt een dergelijke test uitgevoerd? Worden bevindingen uit de test opgelost op basis van de ernst van de bevindingen?
11. Beschikt de organisatie van de leverancier over een security awareness programma?
12. Heeft de leverancier een fysiek veiligheidsbeleid en wordt toegang tot kritieke ruimtes (serverruimtes, datacenters, etc.) gemonitord op evt. ongeautoriseerde toegang?
13. Hoe is de (fysieke/virtuele) scheiding (van de verschillende klanten) op netwerkniveau ingericht?
14. Voldoen de gebruikte versleuteling technologieën aan de gewenste en gecontracteerde beveiligingsniveaus en is hierbij rekening gehouden met het type, sterkte en kwaliteit van het versleutelingsalgoritme? Welke crypto standaarden heeft de leverancier in gebruik? Is hiernaast sleutelbeheer ingericht?

15. Maakt de leverancier gebruik van gescheiden omgevingen voor ontwikkeling, test, acceptatie en productie. Zijn deze voor iedere klant gescheiden (fysiek of logisch)?
16. Heeft de leverancier change management procedures en waarborgen dat alleen geautoriseerd wijzigingen worden geïmplementeerd en hoe zijn security aspecten van deze wijzigingen aangetoond?

10.2. Evaluatie prestatie dienstverleners

Periodiek evalueert Spinware Solutions de samenwerking met dienstverleners. Dit doet Spinware Solutions ten minste jaarlijks.

11. Beveiligingsincidenten

Spinware Solutions heeft onderstaande procedure ingesteld voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten en zwakke plekken in de beveiliging, zodra ze zijn gerapporteerd.

De lessen die worden getrokken uit de afgehandelde incidenten worden gebruikt om de beveiliging waar mogelijk structureel te verbeteren.

Indien een vervolgprocedure na een informatiebeveiligingsincident juridische maatregelen omvat (civiel- of strafrechtelijk), wordt het bewijsmateriaal verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd. De directie zal deze taken op zich nemen en indien noodzakelijk hiervoor externe expertise inschakelen.

11.1. Procedure beveiligingsincident

Binnen de organisatie van Spinware Solutions wordt de volgende procedure gehanteerd ten aanzien van een beveiligingsincident.

- Constatering van de inbreuk door:
  - Een medewerker: iedere werknemer die een beveiligingsincident vermoedt dient dit terstond bij de directie te melden;
  - Een klant: een klant stuurt een bericht of neemt telefonisch contact op. Degene bij Spinware Solutions die de melding van de klant ontvangt, dient dit terstond bij de directie te melden;
  - Een derde partij: een derde partij stuurt een bericht of neemt telefonisch contact op. Degene bij Spinware Solutions die de melding van de derde partij ontvangt, dient dit terstond bij de directie te melden;
- De directie (en eventueel een ingeschakelde derde) doen onderzoek naar de omvang en de technische aspecten van de inbreuk:
  - Welke inbreuk op de beveiligingsmaatregelen heeft plaatsgevonden en wanneer?
  - Welk onderdeel van het IT-systeem is betrokken en/of welke apparatuur? Eventueel: waar is de apparatuur verloren/gestolen?
  - Welke gegevens zijn (mogelijk) betrokken?
  - Wat zijn de (verwachte) consequenties van het incident?
- De directie (en eventueel een ingeschakelde derde) zorgt ervoor dat er maatregelen worden getroffen om de beveiliging te herstellen;
- De directie bepaalt aan de hand van de in paragraaf 11.2.1 en 11.2.2 genoemde criteria of een melding moet worden gedaan aan de Autoriteit Persoonsgegevens en/of de betrokkene(n);
- Indien besloten wordt om een melding te doen, dan worden die gegevens gemeld die zijn opgenomen in paragraaf 11.2.1 en 11.2.2; en
- Spinware Solutions bewaart een overzicht van de inbreuk (feiten, gegevens en communicatie omtrent de inbreuk) in de administratie van Spinware Solutions. Ook andere interne beveiligingsincidenten worden intern geregistreerd, los van of de inbreuk wordt gemeld aan de toezichthouder en/of de betrokkene(n).

Indien Spinware Solutions gebruik maakt van leveranciers, zullen altijd afspraken worden gemaakt over het melden van datalekken die bij een leverancier optreden. Uitgangspunt hierbij is dat de

leverancier aan Spinware Solutions alle informatie over het beveiligingsincident verstrekt, waarna de (eventuele) melding door Spinware Solutions zal worden gedaan.

11.2. Inbreuk in verband met persoonsgegevens

Op grond van de AVG is er sprake van een „inbreuk in verband met persoonsgegevens" in geval van een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

11.2.1. Melding aan Autoriteit Persoonsgegevens

Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt Spinware Solutions deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat zij er kennis van heeft genomen, aan de Autoriteit Persoonsgegevens tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Of de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, hangt af van de volgende factoren:

- Het type inbreuk (bijvoorbeeld onrechtmatige toeging of verlies van gegevens);
- De aard, gevoeligheid en hoeveelheid persoonsgegevens;
- Eenvoudige identificatie van individuen (hoe gemakkelijk is het om aan de hand van de data een natuurlijk persoon te identificeren);
- De ernst van consequenties voor individuen;
- Speciale kenmerken van het individu (kinderen en kwetsbare groepen brengen een hoger risico met zich mee); en
- Het aantal getroffen personen.

Indien de melding aan de Autoriteit Persoonsgegevens niet binnen 72 uur plaatsvindt, geeft Spinware Solutions een goede onderbouwing voor de vertraging. In de melding wordt ten minste het volgende omschreven of meegedeeld:

- de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevens¬ registers in kwestie;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die Spinware Solutions heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

11.2.2. Mededeling aan betrokkene(n)

Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt Spinware Solutions de betrokkene de inbreuk in verband met persoonsgegevens onverwijld mee.

De mededeling aan de betrokkene bevat een omschrijving, in duidelijke en eenvoudige taal:

- de aard van de inbreuk in verband met persoonsgegevens;
- de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevens¬ registers in kwestie;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die Spinware Solutions heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

De mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:

- Spinware Solutions heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;
- Spinware Solutions heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;
- de mededeling zou onevenredige inspanningen vergen. In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

Ook de Autoriteit Persoonsgegevens kan Spinware Solutions ertoe te verplichten de inbreuk in verband met persoonsgegevens aan de betrokkene te melden.

12. Compliance

12.1. Identificatie van toepasselijke wetgeving

Spinware Solutions streeft ernaar te voldoen aan toepasselijke wet- en regelgeving. De verantwoordelijke voor compliance binnen Spinware Solutions monitort of de regelgeving wijzigt, zodat deze tijdig kan worden geïmplementeerd en Spinware Solutions kan overleggen met haar dienstverleners over doorvoering van de wijzigingen in hun dienstverlening.

12.2. Audits

Audits kunnen worden gebruikt om te controleren of de informatiebeveiligings-maatregelen effectief zijn. Auditrapporten worden gebruikt om de correcte werking van deze maatregelen te bevestigen en om eventuele zwakke punten op te sporen.

Waar mogelijk zal Spinware Solutions ook gebruikmaken van audit-rapporten die zij krijgt aangeleverd door dienstverleners, zodat Spinware Solutions ook een oordeel kan vormen over de interne (informatiebeveiliging)processen en beheersing van deze dienstverleners.