Verwerkersovereenkomst

Tussen de gemeente Loon op Zand en

<<Bedrijf>>

Ten behoeve van

<<Onderwerp>>

Verwerkersovereenkomst

Verwerkersovereenkomst van de gemeente Loon op Zand met de (nader in te vullen) verwerker
Het College van Burgemeester en Wethouders van de gemeente Loon op Zand, verder te noemen
de verwerkingsverantwoordelijke, ten deze rechtsgeldig vertegenwoordigd door de <heer of mevrouw> <persoonsnaam> (AFDELINGSHOOFD),
en
<Bedrijf, afdeling>, gevestigd te <plaatsnaam>, verder te noemen de verwerker, ten deze rechtsgeldig vertegenwoordigd door de <de heer of mevrouw>, <persoonsnaam> , <functie>,
verklaren te zijn overeengekomen een verwerkersovereenkomst als bedoeld in artikel 14 tweede
lid van de Wet Bescherming persoonsgegevens en, vanaf 25 mei 2018, als bedoeld in artikel 28,
derde lid, van de Algemene Verordening Gegevensbescherming (hierna: AVG), tussen de verwerkingsverantwoordelijke en de verwerker. Waar in deze verwerkersovereenkomst termen
worden gebruikt die overeenstemmen met definities uit artikel 4 AVG, wordt aan deze termen de betekenis van de definities uit de AVG toegekend.

Artikel 1 Definities
1.1 Bijlagen: aanhangsels bij deze verwerkersovereenkomst, die na door beide partijen te zijn geparafeerd, deel uitmaken van deze verwerkersovereenkomst.
1.2 Normen en standaarden: de door de verwerkingsverantwoordelijke vastgestelde normen en standaarden ter zake van methoden, technieken, procedures, projecten, productiekenmerken en documentatievoorschriften welke bij de uitvoering van de werkzaamheden door de verwerker zullen worden gevolgd als vastgelegd in bijlage 1 <door gemeente bij te voegen>.
1.3 Toezichthouder: de Autoriteit Persoonsgegevens (AP) is het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder is aangesteld voor het toezicht op het verwerken van persoonsgegevens.
1.4. (Verwerkings)verantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
1.5. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, in opdracht van de verwerker, is een sub-verwerker.

Artikel 2 Ingangsdatum en duur
2.1 Deze verwerkersovereenkomst gaat in op het moment van ondertekening en duurt voort zolang de verwerker als verwerker van persoonsgegevens optreedt in het kader van de door de verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens voor <nader in te vullen omschreven doel>

Artikel 3 Onderwerp van deze verwerkersovereenkomst

3.1 De verwerker verwerkt de door of via verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens uitsluitend in opdracht van de verwerkingsverantwoordelijke in het kader van de uitvoering van <contract, nummer>; dit is de onderliggende hoofdovereenkomst. De door de verwerker uit te voeren werkzaamheden waar deze verwerkersovereenkomst betrekking op heeft, worden nader, uitputtend, omschreven in bijlage 2. Verwerker zal de persoonsgegevens niet voor enig ander doel verwerken, behoudens afwijkende wettelijke verplichtingen.

3.2 De verwerker verbindt zich om in het kader van die werkzaamheden de door of via de verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens zorgvuldig te verwerken.

Artikel 4 Verplichtingen verwerker

4.1 De verwerker verwerkt gegevens ten behoeve van de verwerkingsverantwoordelijke, in overeenstemming met diens schriftelijke instructies.

4.2 De verwerker heeft geen zeggenschap over de ter beschikking gestelde persoonsgegevens. Zo neemt hij geen beslissingen over ontvangst en gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over de persoonsgegevens verstrekt onder deze verwerkersovereenkomst komt nimmer bij de verwerker te berusten.

4.3 De verwerker zal bij de verwerking van persoonsgegevens in het kader van de in artikel 3 genoemde werkzaamheden, handelen in overeenstemming met de toepasselijke wet- en regelgeving betreffende de verwerking van persoonsgegevens. De verwerker zal alle redelijke instructies van de contactpersoon, als bedoeld in artikel 12.2, opvolgen, behoudens afwijkende wettelijke verplichtingen. Indien deze afwijkende wettelijke verplichtingen er zijn wordt de verwerkingsverantwoordelijke hiervan, voorafgaand aan de verwerking, schriftelijk op de hoogte gebracht door de verwerker.

4.4 De verwerker zal te allen tijde op eerste verzoek van de contactpersoon, als bedoeld in artikel 12.2, door verwerkingsverantwoordelijke ter beschikking gestelde persoonsgegevens met betrekking tot deze verwerkersovereenkomst ter hand stellen.

4.5 De verwerker stelt de verwerkingsverantwoordelijke te allen tijde in staat om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG, meer in het bijzonder de rechten van betrokkenen, zoals, maar niet beperkt tot een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens, het uitvoeren van een gehonoreerd aangetekend verzet en het uitvoeren van overdracht van gegevens aan een betrokkene dan wel, indien technisch mogelijk, aan een andere verwerkingsverantwoordelijke.

4.6 De verwerker werkt op verzoek van verwerkingsverantwoordelijke te allen tijde mee aan een gegevensbeschermingseffectbeoordeling(PIA).

4.7 De verwerker zet zich op verzoek van de verwerkingsverantwoordelijke naar vermogen in om mee te werken aan het bieden van ontwerp infrastructuur, software, inrichting van software en interfaces die het beschermen van persoonsgegevens afdwingen of makkelijk toepasbaar maken (privacy by design en privacy by default).

Artikel 5 Geheimhoudingsplicht

5.1 Personen in dienst van, dan wel werkzaam ten behoeve van de verwerker, evenals de verwerker zelf, zijn verplicht tot geheimhouding met betrekking tot de persoonsgegevens waarvan zij kennis kunnen nemen, behoudens voor zover een bij, of krachtens de wet gegeven voorschrift tot verstrekking verplicht. De

medewerkers van de verwerker tekenen hiertoe een geheimhoudingsverklaring.
5.2 Indien de verwerker op grond van een wettelijke verplichting gegevens dient te verstrekken, zal de verwerker de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal de verwerker de verwerkingsverantwoordelijke onmiddellijk, voorafgaand aan de verstrekking, ter zake informeren. Tenzij wettelijke bepalingen dit verbieden.

Artikel 6 Meldplicht datalekken en beveiligingsincidenten
6.1 De verwerker zal de verwerkingsverantwoordelijke zo spoedig mogelijk - doch uiterlijk binnen 24 uur na de eerste ontdekking - informeren over alle (vermoedelijke) inbreuken op de beveiliging alsmede andere incidenten die op grond van wetgeving moeten worden gemeld aan de toezichthouder of betrokkene, onverminderd de verplichting de gevolgen van dergelijke inbreuken en incidenten zo snel mogelijk ongedaan te maken dan wel te beperken, al dan niet onder verbeurte van een boete in geval van niet-nakoming, conform artikel 10.4 van deze verwerkersovereenkomst. Verwerker zal voorts, op het eerste verzoek van de verwerkingsverantwoordelijke, alle inlichtingen verschaffen die de verwerkingsverantwoordelijke noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft verwerker in ieder geval de informatie aan de verwerkingsverantwoordelijke zoals omschreven in bijlage 3.
6.2 De verwerker beschikt over een gedegen plan van aanpak betreffende de omgang met en afhandeling van inbreuken en zal de verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in het plan. Verwerker stelt de verwerkingsverantwoordelijke op de hoogte van materiele wijzigingen in het plan van aanpak.
6.3 De verwerker zal het doen van meldingen aan de toezichthouder(s) overlaten aan de verwerkingsverantwoordelijke.
6.4 De verwerker zal alle noodzakelijke medewerking verlenen aan het zo nodig, op de kortst mogelijke termijn, verschaffen van aanvullende informatie aan de toezichthouder(s) en/of betrokkene(n). Daarbij verschaft verwerker in ieder geval de informatie, zoals beschreven in bijlage 3, aan de verwerkingsverantwoordelijke.
6.5 De verwerker houdt een gedetailleerd logboek bij van alle (vermoedens van) inbreuken op
de beveiliging, evenals de maatregelen die in vervolg op dergelijke inbreuken zijn genomen waarin minimaal de informatie zoals bedoeld in bijlage 3 is opgenomen, en geeft daar op eerste verzoek van de verwerkingsverantwoordelijke inzage in.

Artikel 7 Beveiligingsmaatregelen en controle
7.1 De verwerker neemt alle passende technische en organisatorische maatregelen om de persoonsgegevens welke worden verwerkt ten dienste van de verwerkingsverantwoordelijke te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige verwerking. De wijze van beveiliging wordt nader omschreven in bijlage 1.
7.2 De verwerkingsverantwoordelijke is te allen tijde gerechtigd de verwerking van persoonsgegevens te (doen) controleren. De verwerker is verplicht de verwerkingsverantwoordelijke, de Autoriteit Persoonsgegevens, of, de onder geheimhouding, controlerende instantie in opdracht van verwerkingsverantwoordelijke toe te laten en verplicht medewerking te verlenen zodat de controle daadwerkelijk uitgevoerd kan worden.
7.3 De verwerkingsverantwoordelijke zal de controle slechts (laten) uitvoeren na een

voorafgaande schriftelijke melding aan de verwerker.
7.4 De verwerker verbindt zich om binnen een door de verwerkingsverantwoordelijke te bepalen termijn de verwerkingsverantwoordelijke, of de door de verwerkingsverantwoordelijke ingeschakelde derde, te voorzien van de verlangde informatie. Hierdoor kan de verwerkingsverantwoordelijke, of de door de verwerkingsverantwoordelijke ingeschakelde derde, zich een oordeel vormen over de naleving door de verwerker van deze verwerkersovereenkomst. De verwerkingsverantwoordelijke, of de door de verwerkingsverantwoordelijke ingeschakelde derde, is gehouden alle informatie betreffende deze controles vertrouwelijk te behandelen.
7.5 Verwerker staat er voor in, de door de verwerkingsverantwoordelijke of ingeschakelde derde, aangegeven aanbevelingen ter verbetering binnen de daartoe door de verwerkingsverantwoordelijke te bepalen redelijke termijn uit te voeren.
7.6 De verwerker rapporteert jaarlijks over de opzet en werking van het stelsel van maatregelen en procedures, gericht op naleving van deze verwerkersovereenkomst.
7.7 Naast rapportages door de verwerker en controles door de verwerkingsverantwoordelijke of controlerende instantie in opdracht van de verwerkingsverantwoordelijke, kunnen beide partijen ook overeenkomen gebruik te maken van een Third Party Memorandum (TPM) opgesteld door een onafhankelijke externe deskundige.
7.8 De redelijke kosten van de controle worden gedragen door de partij die de kosten maakt, tenzij uit de controle blijkt dat de verwerker enig punt uit deze verwerkersovereenkomst niet heeft nageleefd. In dat geval worden de kosten van de controle gedragen door de verwerker.

Artikel 8 Inschakeling derden
8.1 De verwerker is slechts gerechtigd de uitvoering van de werkzaamheden geheel of ten dele uit te besteden aan derden na voorafgaande, duidelijk gespecificeerde, schriftelijke toestemming van de verwerkingsverantwoordelijke.
8.2 De verwerkingsverantwoordelijke kan aan de schriftelijke toestemming voorwaarden verbinden, op het gebied van geheimhouding en ter naleving van de verplichtingen uit deze verwerkersovereenkomst.
8.3 De verwerker blijft in deze gevallen te allen tijde aanspreekpunt en verantwoordelijk voor de naleving van de bepalingen uit deze verwerkersovereenkomst. De verwerker garandeert dat deze derden schriftelijk minimaal dezelfde plichten op zich nemen als tussen de verwerkingsverantwoordelijke en de verwerker zijn overeengekomen en zal de verwerkingsverantwoordelijke, op diens verzoek, inzage verschaffen in de overeenkomsten met deze derden waarin deze plichten zijn opgenomen.
8.4 De verwerker mag de persoonsgegevens uitsluitend verwerken in Nederland. Doorgifte naar
andere landen is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van de verwerkingsverantwoordelijke en met inachtneming van de toepasselijke wet- en regelgeving.
8.5 De verwerker houdt een actueel register bij van de door hem ingeschakelde derden en onderaannemers waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van de derden of onderaannemers zijn opgenomen, alsmede eventuele door de verwerkingsverantwoordelijke gestelde aanvullende voorwaarden. Dit register zal als bijlage 5 aan deze verwerkersovereenkomst worden toegevoegd en zal door de verwerker actueel worden gehouden.

Artikel 9 Wijziging en beëindigen verwerkersovereenkomst

9.1 Wijziging van deze verwerkersovereenkomst kan slechts schriftelijk plaatsvinden middels een door beide partijen geaccordeerd voorstel.

9.2 Zodra de samenwerking is beëindigd, zal de verwerker naar keuze van de verwerkingsverantwoordelijke (i) alle of een door verwerkingsverantwoordelijke bepaald gedeelte van haar in het kader van deze verwerkersovereenkomst ter beschikking gestelde persoonsgegevens aan de verwerkingsverantwoordelijke ter beschikking stellen (ii) de persoonsgegevens die hij van de verwerkingsverantwoordelijke heeft ontvangen op alle locaties vernietigen, in welke vorm dan ook en toont dit aan, tenzij partijen iets anders overeenkomen. De verantwoordelijk kan zo nodig nadere eisen stellen aan de wijze van beschikbaarstelling, waaronder eisen aan het bestandsformaat, dan wel vernietiging. Deze werkzaamheden moeten, binnen nader overeen te komen redelijke termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt.

9.3 De verwerker zal te allen tijde het vorig lid, zodanig uitvoeren dat er geen sprake is van verlies van functionaliteit of (delen van) de gegevens.

9.4 Verwerkingsverantwoordelijke en verwerker treden met elkaar in overleg over wijzigingen in deze verwerkersovereenkomst als een wijziging in regelgeving of een wijziging in de uitleg van regelgeving daartoe aanleiding geven.

9.5 Indien een partij tekortschiet in de nakoming van een overeengekomen verplichting, kan de andere partij haar in gebreke stellen waarbij de nalatige partij alsnog een redelijke termijn voor de nakoming wordt gegund. Blijft nakoming ook dan uit dan is de nalatige partij in verzuim. Ingebrekestelling is niet nodig wanneer voor de nakoming een fatale termijn geldt, nakoming blijvend onmogelijk is of indien uit een mededeling dan wel de houding van de andere partij moet worden afgeleid dat deze in de nakoming van haar verplichting zal tekortschieten.

9.6 De verwerkingsverantwoordelijke is gerechtigd, onverminderd hetgeen daartoe bepaald is in de verwerkersovereenkomst en de daarmee samenhangende hoofdovereenkomst, en onverminderd hetgeen overigens in de wet is bepaald, de uitvoering van deze verwerkersovereenkomst door middel van een aangetekend schrijven op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang geheel of gedeeltelijk te ontbinden, nadat verwerkingsverantwoordelijke constateert dat:

a) verwerker (voorlopige) surseance van betaling aanvraagt; of

b) verwerker zijn faillissement aanvraagt of in staat van faillissement wordt verklaard; of

c) de onderneming van verwerker wordt ontbonden; of

d) verwerker zijn onderneming staakt; of

e) sprake is van een ingrijpende wijziging in de zeggenschap over de activiteiten van de onderneming van verwerker die maakt dat het in alle redelijkheid niet van de verwerkingsverantwoordelijke kan worden verwacht dat zij de verwerkersovereenkomst in stand houdt; of

f) op een aanmerkelijk deel van het vermogen van verwerker beslag wordt gelegd (anders dan door verantwoordelijke); of

g) de andere partij aantoonbaar tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze verwerkersovereenkomst en die ernstige toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een daartoe strekkende schriftelijke ingebrekestelling dan wel een van de overige situaties bedoeld in artikel 9.5 zich voordoet.

9.7 Verwerker informeert ogenblikkelijk de verwerkingsverantwoordelijke indien een faillissement dreigt dan wel surseance van betaling, zodat de

verwerkingsverantwoordelijke tijdig kan beslissen de persoonsgegevens terug te vorderen alvorens faillissement wordt uitgesproken.
9.8 Verwerkingsverantwoordelijke is gerechtigd deze verwerkersovereenkomst en de hoofdovereenkomst per direct te ontbinden indien verwerker te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van ontwikkelingen in de wet en/of de rechtspraak aan de verwerking van de persoonsgegevens worden gesteld.
9.9 Indien de verwerkersovereenkomst voortijdig wordt beëindigd is artikel 9 lid 2 en 3 van overeenkomstige toepassing.

Artikel 10 Aansprakelijkheid
10.1 Indien de verwerker tekortschiet in de nakoming van de verplichting uit deze verwerkersovereenkomst kan verwerkingsverantwoordelijke hem in gebreke stellen. Verwerker is echter onmiddellijk in gebreke als de nakoming van desbetreffende verplichting anders dan door overmacht binnen de overeengekomen termijn, reeds blijvend onmogelijk is. Ingebrekestelling geschiedt schriftelijk, waarbij aan de verwerker een redelijke termijn wordt gegund om alsnog haar verplichtingen na te komen. Deze termijn is een fatale termijn. Indien nakoming binnen deze termijn uitblijft, is verwerker in verzuim.
10.2 Verwerker is aansprakelijk op grond van het bepaalde in artikel 49 Wbp en/of artikel 82 AVG, voor schade of nadeel voortvloeiende uit het niet nakomen van deze verwerkersovereenkomst, daaronder begrepen wanneer bij de verwerking niet wordt voldaan aan de specifiek tot verwerkingsgerichte verplichtingen van de AVG, of buiten de rechtmatige instructies van verwerkingsverantwoordelijke is gehandeld.
10.3 Verwerker vrijwaart verwerkingsverantwoordelijke voor schade of nadeel voor zover ontstaan door werkzaamheid van de verwerker.
10.4 Indien verwerker de in artikel 6 lid 1 van deze verwerkersovereenkomst neergelegde verplichting niet of niet-tijdig nakomt en de toezichthouder de verwerkingsverantwoordelijke dientengevolge een bestuurlijke boete oplegt, is verwerker aansprakelijk en zal verwerkingsverantwoordelijke een contractuele boete ter hoogte van hetzelfde bedrag opleggen aan verwerker. Deze boete is niet vatbaar voor verrekening en opschorting en laat de rechten van verwerkingsverantwoordelijken op nakoming en schadevergoeding onverlet.

Artikel 11 Toepasselijk recht
11.1 Op deze verwerkersovereenkomst en op alle geschillen die daaruit mogen voortvloeien of
daarmee mogen samenhangen, is het Nederlands recht van toepassing.

Artikel 12 Overige bepalingen
12.1 Deze verwerkersovereenkomst kan worden aangehaald als 'Verwerkersovereenkomst uitvoering < >.
12.2 De afdeling <afdelingsnaam> van de gemeente Loon op Zand treedt namens de verwerkingsverantwoordelijke op als contactpersoon.

Voor akkoord,

Verwerkingsverantwoordelijke		Verwerker	
Naam:		Naam:	

Functie:		Functie:	
Handtekening		Handtekening	

Bijlage 1: Beschrijving beveiliging ter uitwerking van artikel 1 lid 2

1. Normenstelsel (kies a of b)

a. De informatiebeveiliging vindt plaats volgens algemeen erkende normen, namelijk: (vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS)

b. De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm zoals de BIG of de BIR of vergelijkbaar.

2. De toereikendheid van de informatiebeveiliging blijkt uit:

a. Certificering;

b. Periodieke externe controles zoals audits of TPM's (bijv. ISAE3xxx SOC type II);

c. Een Assurance rapport met conclusie over de bevindingen van de auditor;

d. Eigen controles of eigen mededelingen.

3. Uit de certificering of periodieke externe controles of uit de audits of uit de eigen controles blijkt of kan afgeleid worden dat de beveiliging voldoet aan of gelijkwaardig is met de toelichting (bijlage 4) en de daarin omschreven elementen.

LET OP: gemotiveerd afwijken is toegestaan!

Bijlage 2: Omschrijving werkzaamheden ter uitwerking van artikel 3 lid 1

1. De werkzaamheden van de verwerker (de verleende diensten en de bijbehorende verwerking).

Bijvoorbeeld:
- Hosting bestaande uit activiteiten zoals…
- Back-ups maken en restoren
- Applicatiebeheer bestaande uit activiteiten zoals…
- Technisch beheer bestaande uit activiteiten zoals…
- Database beheer bestaande uit activiteiten zoals…
- Helpdesk bestaande uit activiteiten zoals…
- Communicatievoorziening (zoals berichtenverkeer)
- Archiefbeheer
- Vernietiging van gegevensdragers
- Printing, scanning, kopieren (lease van Multifunctionals)
- Inhoudelijke werkzaamheden die namens de gemeente worden uitgevoerd zoals:

o Uitgifte parkeervergunningen
o Voeren salarisadministratie
o Bijvoorbeeld: uitvoeren bepaalde gemeentelijke taken uit de Jeugdwet, WMO, participatiewet

Indien de werkzaamheden in de hoofdovereenkomst specifiek omschreven zijn, kan dit lijstje achterwege blijven. Of hier verwijzen naar de hoofdovereenkomst. De achtergond van de beschrijving is dat je voldoende duidelijk maakt wat er beveiligd moet worden. Het is de bedoeling dat de zinnen afgemaakt worden met specifieke omschrijvingen!

2. Omschrijving van de werkzaamheden van de derden (subverwerkers) als deze er zijn, als bedoeld in artikel 8.

Bijvoorbeeld:
- Hosting bestaande uit activiteiten zoals…
- Back-ups maken en restoren
- Applicatiebeheer bestaande uit activiteiten zoals…
- Technisch beheer bestaande uit activiteiten zoals…
- Database beheer bestaande uit activiteiten zoals…
- Helpdesk bestaande uit activiteiten zoals…
- Communicatievoorziening (zoals berichtenverkeer)
- Onderhoud aan multifunctionals

De achtergond van de beschrijving is dat er voldoende duidelijk gemaakt wordt wat er beveiligd
moet worden. Ook hier geldt dat de zinnen afgemaakt worden met specifieke omschrijvingen!

3. Categorieën personen en soorten persoonsgegevens

Algemene omschrijving van de categorien personen waar de gegevens die verwerkt worden

betrekking op hebben zoals: personeelsleden, burgers, inschrevenen, vergunning aanvragers, voorziening aanvragers (clienten).
Is er bij de verwerkte gegevens sprake van gegevens van gevoelige aard als bedoelt in de beleidsregels datalekken van de AP:22?

• Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp. Het gaat hierbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag. Het Burgerservicenummer (bsn) valt ook onder bijzondere persoonsgegevens.

• Gegevens over de financiële of economische situatie van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.

• (Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene. Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.

• Gebruikersnamen, wachtwoorden en andere inloggegevens. De mogelijke gevolgen voor betrokkenen hangen af van de verwerkingen en van de persoonsgegevens waar de inloggegevens toegang toe geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.

• Gegevens die kunnen worden misbruikt voor (identiteits)fraude. Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het bsn.
Is er sprake van de verwerking van gegevens over kwetsbare groepen zoals:

• minderjarigen;

• mensen die te maken hebben met stalking;

• die in een blijf-van-mijn-lijfhuis verblijven.

Voor bepaalde categorieën van betrokkenen:
• kinderen en mensen met een verstandelijke handicap.

Bijlage 3: Inlichtingen om incidenten te beoordelen ter uitwerking van art. 6 lid 1 en 5

De verwerker zal alle inlichtingen verschaffen die de verwerkingsverantwoordelijke noodzakelijk
acht om het incident te kunnen beoordelen. Daarbij verschaft verwerker in ieder geval de volgende informatie aan de verwerkingsverantwoordelijke:

- wat de (vermeende) oorzaak is van de inbreuk;
- wat het (vooralsnog bekende en/of te verwachten) gevolg is;
- wat de (voorgestelde) oplossing is;
- contactgegevens voor de opvolging van de melding;
- aantal personen waarvan gegevens betrokken zijn bij de inbreuk (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij de inbreuk);
- een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;
- het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
- de datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is: de periode waarbinnen de inbreuk heeft plaatsgevonden);
- de datum en het tijdstip waarop de inbreuk bekend is geworden bij verwerker of bij een door hem ingeschakelde derde of onderaannemer;
- of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
- wat de reeds ondernomen maatregelen zijn om de inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken.

Bijlage 4: Toelichting: Maatregelen op basis van de BIG ten aanzien van een Verwerker

Passende technische en organisatorische maatregelen

De Baseline informatiebeveiliging Rijksdienst (BIR) 2012 biedt een normenkader voor de beveiliging van de informatiehuishouding van de Rijksoverheid. De voor de overheid verplichte standaarden ISO27001/ISO27002 met aanvullingen zijn opgenomen in de BIR. Afgelopen jaar heeft Digitale Checklisten een GAP-analyse op basis van de BIR uitgevoerd. Uit deze analyse blijkt dat Digitale Checklisten de volgende passende technische en organisatorische maatregelen heeft genomen:

4.1 Beveiligingsbeleid

1. Directie richting en ondersteuning bieden voor Informatiebeveiligingsvoorschriften overeenkomstig de bedrijfsmatige eisen en relevante wetten en voorschriften.
2. Een document met informatiebeveiligingsbeleid behoort door het lijnmanagement te worden goedgekeurd en gepubliceerd en kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen. Het VIR:2007, VIRBI en BIR zijn vastgesteld rijksbreed beleid, het lijnmanagement is verantwoordelijk voor de invulling en uitvoering hiervan.
3. Het informatiebeveiligingsbeleid behoort met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.

4.2 Organisatie van informatiebeveiliging

1. Beheren van de informatiebeveiliging binnen de organisatie.
2. De directie behoort actief beveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.
3. Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit verschillende delen van de organisatie met relevante rollen en functies.
4. Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd.
5. Er behoort een goedkeuringsproces voor nieuwe IT-voorzieningen te worden vastgesteld en geïmplementeerd.
6. Eisen voor vertrouwelijkheid of geheimhoudingsovereenkomst die een weerslag vormen van de behoefte van de organisatie aan bescherming van informatie behoren te worden vastgesteld en regelmatig te worden beoordeeld.
7. Er behoren geschikte contacten met relevante overheidsinstanties te worden onderhouden.
8. Er behoren geschikte contacten met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties te worden onderhouden.
9. De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheersdoelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich significante wijzigingen voordoen in de implementatie van de beveiliging.
10. Beveiligen van de informatie en IT-voorzieningen van de organisatie handhaven waartoe externe partijen toegang hebben of die door externe partijen worden verwerkt of beheerd, of die naar externe partijen wordt gecommuniceerd.

11. De risico's voor de informatie en IT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend.
12. Alle geïdentificeerde beveiligingseisen behoren te worden behandeld voordat klanten toegang wordt verleend tot de informatie of bedrijfsmiddelen van de organisatie.
13. In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of IT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan IT-voorzieningen waarbij sprake is van toegang, behoren alle relevante beveiligingseisen te zijn opgenomen.

4.3 Beheer van bedrijfsmiddelen

1. Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.
2. Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden.
3. Alle informatie en bedrijfsmiddelen die verband houden met IT-voorzieningen behoren een eigenaar te hebben in de vorm van een aangewezen deel van de organisatie.
4. Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met IT-voorzieningen.
5. Bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt. Het VIRBI:2012 noemt classificatie " Rubricering" en beschrijft hoe de rubricering van informatie moet geschieden
6. Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.
7. Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd.

4.4 Personele beveiliging

1. Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.
2. De rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers ten aanzien van beveiliging behoren te worden vastgesteld en gedocumenteerd overeenkomstig het beleid voor informatiebeveiliging van de organisatie.
3. Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoren te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en behoren evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.
4. Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging behoren te zijn vastgelegd.
5. Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun

verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen, en het risico van een menselijke fout te verminderen.

6. De directie behoort van werknemers, ingehuurd personeel en externe gebruikers te eisen dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de organisatie.
7. Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.
8. Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die inbreuk op de beveiliging hebben gepleegd.
9. Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers ordelijk de organisatie
10. De verantwoordelijkheden voor beëindiging of wijziging van het dienstverband behoren duidelijk te zijn vastgesteld en toegewezen.
11. Alle werknemers, ingehuurd personeel en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband, contract of overeenkomst.
12. De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en IT-voorzieningen behoren te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoort na wijziging te worden aangepast.

4.5 Fysieke beveiliging

1. Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie.
2. Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en IT-voorzieningen bevinden.
3. Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.
4. Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.
5. Er behoort fysieke bescherming tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vormen van natuurlijke of menselijke calamiteiten te worden ontworpen en toegepast.
6. Er behoren een fysieke bescherming en richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast

.

7. Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, behoren te worden beheerst en indien mogelijk worden afgeschermd van IT voorzieningen, om onbevoegde toegang te voorkomen.
8. Het voorkomen van verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten. Plaatsing en bescherming van apparatuur
9. Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd.
10. Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.

11. Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd conform de norm NEN 1010.
12. Apparatuur behoort op correcte wijze te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.
13. Apparatuur buiten de terreinen behoort te worden beveiligd waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie.
14. Alle apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd.
15. Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.

4.6 Beheer van communicatie en bedienprocessen

1. Waarborgen van een correcte en veilige bediening van IT voorzieningen
2. Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben.
3. Wijzigingen in IT voorzieningen en informatiesystemen behoren te worden beheerst.
4. Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
5. Faciliteiten voor ontwikkeling, testen en productie behoren te zijn gescheiden om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.
6. Een geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij.
7. Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.
8. De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.
9. Het risico van systeemstoringen tot een minimum beperken.
10. Het gebruik van middelen behoort te worden gecontroleerd en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen, om de vereiste systeemprestaties te bewerkstelligen.
11. Er behoren aanvaardingscriteria te worden vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er behoort een geschikte test van het systeem of de systemen te worden uitgevoerd tijdens ontwikkeling en voorafgaand aan de acceptatie.
12. Beschermen van de integriteit van programmatuur en informatie.
13. Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.
14. Als gebruik van "mobile code" is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde "mobile code"' functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en behoort te worden voorkomen dat onbevoegde 'mobile code' wordt uitgevoerd.
15. Handhaven van de integriteit en beschikbaarheid van informatie en IT voorzieningen.

16. Er behoren back-upkopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig het vastgestelde back-upbeleid.
17. Bewerkstelligen van de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur

.
18. Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.
19. Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten.
20. Er behoren procedures te zijn vastgesteld voor het beheer van verwijderbare media.
21. Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.
22. Er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik.
23. Systeemdocumentatie behoort te worden beschermd tegen onbevoegde toegang.
24. Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met enige externe entiteit.
25. Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.
26. Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.
27. Media die informatie bevatten behoren te worden beschermd tegen onbevoegde toegang, misbruik of corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.
28. Informatie die een rol speelt bij elektronische berichtuitwisseling behoort op geschikte wijze te worden
29. Beleid en procedures behoren te worden ontwikkeld en geïmplementeerd om informatie te beschermen die een rol speelt bij de onderlinge koppeling van systemen voor bedrijfsinformatie.
30. Bewerkstelligen van de beveiliging van diensten voor e-commerce, en veilig gebruik ervan.
31. Informatie die een rol speelt bij e-commerce en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en modificatie.
32. Informatie die een rol speelt bij onlinetransacties behoort te worden beschermd om onvolledige overdracht, onjuiste routing, onbevoegde wijziging van berichten, onbevoegde openbaarmaking, onbevoegde duplicatie of weergave van berichten te voorkomen.
33. De betrouwbaarheid van de informatie die beschikbaar wordt gesteld op een openbaar toegankelijk systeem behoort te worden beschermd om onbevoegde modificatie te voorkomen.
34. Ontdekken van onbevoegde informatieverwerkingsactiviteiten.
35. Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.
36. Er behoren procedures te worden vastgesteld om het gebruik van IT voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.
37. Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.

38. Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd.
39. Storingen behoren in logbestanden te worden vastgelegd en te worden geanalyseerd en er behoren
40. De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

4.7 Toegangsbeveiliging

1. Beheersen van de toegang tot informatie.
2. Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.
3. Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen.
4. Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.
5. De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.
6. De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.
7. De directie behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces.
8. Voorkomen van onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en IT-voorzieningen.
9. Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden 10. Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd.
11. Er behoort een 'clear desk'-beleid voor papier en verwijderbare opslagmedia en een 'clear screen'-beleid voor IT-voorzieningen te worden ingesteld.
12. Het voorkomen van onbevoegde toegang tot netwerkdiensten.
13. Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze specifiek bevoegd zijn.
14. Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen.
15. Automatische identificatie van apparatuur behoort te worden overwogen als methode om verbindingen vanaf specifieke locaties en apparatuur te authenticeren.
16. De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst.
17. Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.
18. Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de organisatie overschrijden, behoren de toegangsmogelijkheden voor gebruikers te worden beperkt, overeenkomstig het toegangsbeleid en de eisen van bedrijfstoepassingen (zie 11.1).
19. Netwerken behoren te zijn voorzien van beheersmaatregelen voor netwerkroutering, om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoepassingen.
20. Voorkomen van onbevoegde toegang tot besturingssystemen.
21. Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure.

22. Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.
23. Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.
24. Het gebruik van hulpprogrammatuur waarmee systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd behoort te worden beperkt en behoort strikt te worden beheerst.
25. Inactieve sessies behoren na een vastgestelde periode van inactiviteit te worden uitgeschakeld.
26. De verbindingstijd behoort te worden beperkt als aanvullende beveiliging voor toepassingen met een verhoogd risico.
27. Voorkomen van onbevoegde toegang tot informatie in toepassingssystemen.
28. Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid.
29. Gevoelige systemen behoren een eigen, vast toegewezen (geïsoleerde) computeromgeving te hebben.
30. Waarborgen van informatiebeveiliging bij het gebruik van draagbare computers en faciliteiten voor telewerken.
31. Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.
32. Er behoren beleid, operationele plannen en procedures voor telewerken te worden ontwikkeld en geïmplementeerd.

4.8 Verwerving, onderhoud en ontwikkeling

1. Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.
2. Analyse en specificatie van beveiligingseisen In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen.
3. Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen.
4. Gegevens die worden ingevoerd in toepassingen behoren te worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn.
5. Er behoren validatiecontroles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken.
6. Er behoren eisen te worden vastgesteld, en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.
7. Gegevensuitvoer uit een toepassing behoort te worden gevalideerd, om te bewerkstelligen dat de verwerking van opgeslagen gegevens op de juiste manier plaatsvindt en geschikt is gezien de omstandigheden.
8. Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen.
9. Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.
10. Er behoort sleutelbeheer te zijn vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.

11. Beveiliging van systeembestanden bewerkstelligen.
12. Er behoren procedures te zijn vastgesteld om de installatie van programmatuur op productiesystemen te beheersen.
13. Testgegevens behoren zorgvuldig te worden gekozen, beschermd en beheerst.
14. De toegang tot broncode van programmatuur behoort te worden beperkt.
15. Beveiliging van toepassingsprogrammatuur en -informatie handhaven.
16. De implementatie van wijzigingen behoort te worden beheerst door middel van formele procedures voor wijzigingsbeheer.
17. Bij wijzigingen in besturingssystemen behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie.
18. Wijzigingen in programmatuurpakketten behoren te worden ontmoedigd, te worden beperkt tot noodzakelijke wijzigingen , en alle wijzigingen behoren strikt te worden beheerst.
19. Er behoort te worden voorkomen dat zich gelegenheden voordoen om informatie te laten uitlekken.
20. Uitbestede ontwikkeling van programmatuur behoort onder supervisie te staan van en te worden gecontroleerd door de organisatie.
21. Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden.
22. Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden.

4.9 Beheer van incidenten

1. Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.
2. Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
3. Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en -diensten behoort te worden geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren.
4. Bewerkstelligen dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.
5. Er behoren leidinggevende verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.
6. Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gecontroleerd.
7. Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

4.10 Bedrijfscontinuïteitsbeheer

1. Tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.
2. Er behoort een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie te worden ontwikkeld en bijgehouden, voor de naleving van eisen voor informatiebeveiliging die nodig zijn voor de continuïteit van de bedrijfsvoering

3. Gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden, behoren te worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor informatiebeveiliging.
4. Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vereiste niveau en in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen.
5. Er behoort een enkelvoudig kader voor bedrijfscontinuïteitsplannen te worden gehandhaafd om te bewerkstelligen dat alle plannen consistent zijn, om eisen voor informatiebeveiliging op consistente wijze te behandelen en om prioriteiten vast te stellen voor testen en onderhoud.
6. [R] Er worden minimaal jaarlijks oefeningen en/of testen gehouden om de bedrijfscontinuïteitsplannen en mate van readiness van de organisatie te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.

4.11 Naleving

1. Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseisen.
2. Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, behoren expliciet te worden vastgesteld, gedocumenteerd en actueel te worden gehouden voor elk informatiesysteem en voor deze organisatie.
3. Er behoren geschikte procedures te worden geïmplementeerd om te bewerkstelligen dat wordt voldaan aan de wettelijke en regelgevende eisen en contractuele verplichtingen voor het gebruik van materiaal waarop intellectuele eigendomsrechten kunnen berusten en het gebruik van programmatuur waarop intellectuele eigendomsrechten berusten.
4. Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.
5. De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.
6. Gebruikers behoren ervan te worden weerhouden IT voorzieningen te gebruiken voor onbevoegde doeleinden.
7. Cryptografische beheersmaatregelen behoren overeenkomstig alle relevante overeenkomsten, wetten en voorschriften te worden gebruikt
8. Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie.
9. Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.
10. Informatiesystemen worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijv. kwetsbaarheidsanalyses en penetratietesten. Zie ook 12.6.1.1.
11. Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren
12. Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren
13. Toegang tot hulpmiddelen voor audits van informatiesystemen behoort te worden beschermd om mogelijk misbruik of compromittering te voorkomen.

Bijlage 5: Omschrijving werkzaamheden ter uitwerking van artikel 8 lid 5

Verwerker maakt bij de uitvoering van de verwerkersovereenkomst gebruik van de derden/onderaannemers die in deze bijlage zijn vermeld. De verwerker zal deze bijlage conform artikel 8 van deze verwerkersovereenkomst bijwerken indien er wijzigingen plaatsvinden in de ingeschakelde derden/onderaannemers en deze lijst onverwijld ter beschikking stellen aan de verwerkingsverantwoordelijke.

[PARTIJ 1]	
Vestigingsplaats:	
Inschrijvingsnummer handelsregister:	
Beschrijving van de werkzaamheden:	
Voorwaarden van de verwerkingsverantwoordelijke gesteld aan toestemming:	

[PARTIJ 2]	
Vestigingsplaats:	
Inschrijvingsnummer handelsregister:	
Beschrijving van de werkzaamheden:	
Voorwaarden van de verwerkingsverantwoordelijke gesteld aan toestemming:	