WHITE PAPER / OKTOBER 2026

Grip op de Cyberbeveiligingswet

Veilige externe documentuitwisseling voor gemeenten: van zorgplicht naar aantoonbare grip.

Een white paper voor CISO's, informatiebeveiligers, privacy officers en I&A-managers van gemeenten en gemeenschappelijke regelingen

01
Beleid
Wat, waarom en voor wie?

02
Toegang
Wie, hoe en hoe lang?

03
Gebruik
Werkt de complete taak?

04
Bewijs
Wat kunnen we aantonen?

Wat de wet vraagt, een stappenplan voor de eerste 90 dagen, een werkblad en een zelftest.

SAMENVATTING

Van zorgplicht naar aantoonbare grip

Sinds 15 augustus 2026 is elke gemeente een essentiële entiteit onder de Cyberbeveiligingswet. De vraag is niet alleen of u beveiligt, maar ook of u het kunt laten zien.

Gemeenten delen dagelijks gevoelige informatie met partijen buiten de eigen organisatie: jeugddossiers met zorgaanbieders, bouwtekeningen met aannemers, bezwaardossiers met advocaten. Op dat moment verlaat informatie de beheerde omgeving. Versleuteld transport helpt, maar beantwoordt niet wie mocht ontvangen, onder welke voorwaarden en wat u achteraf kunt vaststellen.

Deze white paper behandelt externe documentuitwisseling als een bestuurlijk proces, met een eigenaar, vastgelegde regels en een plek in de risicoanalyse. Begin met één bestandsstroom met een hoog risico, doorloop het stappenplan en breid daarna uit. Software ondersteunt de uitvoering; de verantwoordelijkheid blijft bij de gemeente.

Vraag	Wat u vastlegt
Eigenaarschap	Eén proceseigenaar voor externe documentuitwisseling, met een rapportagelijn naar het college.
Bestandsstromen	Welke informatie naar welke externe partijen gaat, via welk kanaal en met welke gevoeligheid.
Kanaal	Eén beheerde route voor vertrouwelijke en grote bestanden, met verificatie, geldigheid en logging.
Medewerkers	Een werkinstructie die in de praktijk werkt, ook voor ontvangers zonder account.
Bewijs	Een audit trail en een incidentdraaiboek waarmee u binnen 24 uur kunt reconstrueren.

In deze white paper

De Cyberbeveiligingswet voor gemeenten 02
Waar informatie de gemeente verlaat 04
Wat de wet vraagt van documentuitwisseling 05
Melden onder de Cbw en de AVG 06
Vier onderdelen van grip 07
Stappenplan voor de eerste 90 dagen 08
Werkblad en zelftest 10
Keuze, Msafe, werksessie en bronnen 13

Leesroute: gebruik de vier onderdelen van grip op pagina 7 om het gesprek te starten en het werkblad op pagina 10 om een besluit voor te bereiden.

01 / DE CYBERBEVEILIGINGSWET

Gemeenten zijn essentiële entiteit

De Cbw maakt cyberweerbaarheid een wettelijke zorgplicht met toezicht, meldplicht en bestuurlijke verantwoordelijkheid.

De Cyberbeveiligingswet is de Nederlandse uitwerking van de Europese NIS2-richtlijn en vervangt de Wbni. Ruim 8.000 organisaties in 18 sectoren vallen onder de wet, die op 15 augustus 2026 zonder overgangstermijn in werking trad. [1]

Gemeenten, provincies en waterschappen zijn ongeacht hun omvang aangemerkt als essentiële entiteit. Gemeenschappelijke regelingen beoordelen zelf of zij onder de wet vallen en zijn dan zelf verantwoordelijk voor naleving. [2][4]

Verplichting	Wat het betekent voor de gemeente
Registratie	Inschrijving in het landelijke entiteitenregister via het portaal van het NCSC.
Zorgplicht	Passende maatregelen op basis van een brede cyberrisicoanalyse, ook voor leveranciers. BIO2 krijgt een expliciete juridische basis als invulling. [2]
Meldplicht	Een significant incident binnen 24 uur melden bij het NCSC, met een uitgebreidere melding binnen 72 uur en een eindverslag binnen een maand.
Bestuur	Het college is risico-eigenaar, stelt middelen beschikbaar en volgt binnen twee jaar een verplichte training met certificaat. [3]

Toezicht en handhaving

De Rijksinspectie Digitale Infrastructuur (RDI) houdt risicogericht toezicht op gemeenten. De RDI zet eerst in op herstel en verbetering, maar kan handhaven met een last onder dwangsom of een bestuurlijke boete. Het NCSC voert voor gemeenten de CSIRT-taken uit. [2][4]

Ondersteuning

De Informatiebeveiligingsdienst (IBD) van de VNG blijft het aanspreekpunt voor BIO2, informatiebeveiliging en privacy. De VNG schreef haar leden vlak voor de invoering dat voor veel gemeenten aanvullende stappen nodig zijn. [2][3][8]

> "De Cyberbeveiligingswet legt de verantwoordelijkheid bij het bestuur. Dat is terecht. Maar een college kan alleen sturen op wat zichtbaar is. Wij willen gemeenten helpen om externe documentuitwisseling zichtbaar, beheersbaar en bewijsbaar te maken."
>
> Atze Zwirs, CEO Msafe

Beslisvraag: wie in uw gemeente kan vandaag uitleggen welke externe bestandsstromen onder de zorgplicht vallen en wie daarvan eigenaar is?

01 / IN ÉÉN OOGOPSLAG



FIGUUR 1 / DE CYBERBEVEILIGINGSWET VOOR GEMEENTEN. BRONNEN: [1][2][3][4].

02 / WAAR INFORMATIE DE GEMEENTE VERLAAT

Het risico zit op de grens

Interne systemen zijn meestal goed beveiligd. Het kwetsbare moment is het document dat naar een externe partij gaat.

Volgens het jaarverslag 2025 van de Autoriteit Persoonsgegevens kwamen er 44.374 datalekmeldingen binnen. Bijna driekwart betrof brieven en e-mails die niet bij de juiste persoon terechtkwamen. [5]

Kijk daarom naar complete bestandsstromen, niet naar losse tools. Neem ook inkomende documenten, doorsturen door ketenpartners en noodroutes mee. Waar beleid ophoudt, gaan medewerkers improviseren.

Domein	Externe partijen	Type informatie	Typisch risico
Sociaal domein	Zorgaanbieders, wijkteams, ketenpartners	Jeugd-, Wmo- en Participatiewetdossiers	Verkeerde ontvanger
Ruimte en vergunningen	Architecten, aannemers, omgevingsdienst	Bouwtekeningen, berekeningen	Te groot voor e-mail
Juridische zaken	Advocaten, rechtbank, bezwaarcommissie	Bezwaar- en beroepsdossiers	Geen bewijs van toegang
Bedrijfsvoering	Accountant, arbodienst, inschrijvers	Personeels- en aanbestedingsstukken	Versnipperde kanalen
Samenwerking	GR's, veiligheidsregio, GGD	Gedeelde dossiers	Onduidelijk eigenaarschap

Een bijlage is een kopie

Een e-mailbijlage geeft de ontvanger een zelfstandige kopie die u niet meer kunt intrekken. Of de bedoelde persoon het bestand opent, is niet vast te stellen. E-mail blijft nuttig voor communicatie, maar niet als gecontroleerde route voor vertrouwelijke dossiers.

Omwegen ontstaan uit nood

Is het goedgekeurde kanaal onduidelijk, niet beschikbaar of te omslachtig, dan wijken medewerkers uit naar gratis diensten voor grote bestanden. Die lossen het formaatprobleem op, maar niet het beheerprobleem: geen verificatie, geen centraal beleid, geen bruikbaar spoor.

Beslisvraag: voor welke bestandsstroom kunt u vandaag niet uitleggen wie toegang had en hoe lang?

03 / WET EN DOCUMENTUITWISSELING

Verbind verplichtingen aan maatregelen

De Cbw schrijft geen product voor. Een maatregel telt wanneer u kunt uitleggen welk risico hij afdekt en hoe u de werking toetst.

De onderwerpen uit artikel 21, lid 2 van de NIS2-richtlijn raken externe documentuitwisseling op zes plekken. BIO2 werkt deze onderwerpen voor overheden uit in concrete maatregelen. [6] [8]

Bepaal per onderwerp wat u vastlegt en hoe u het toetst. Een beleidsregel zonder werkbare route of een logbestand zonder eigenaar levert nog geen aantoonbare grip op.

Onderwerp (NIS2 art. 21 lid 2)	Wat het betekent voor documentuitwisseling
Risicoanalyse en beleid (a)	Externe bestandsstromen staan in de risicoanalyse, met een eigenaar per stroom.
Incidentafhandeling (b)	U reconstrueert snel wat is gedeeld, met wie en wanneer.
Toeleveringsketen (d)	De leverancier is beoordeeld op certificering, locatie, toegang en exit.
Cyberhygiëne en training (g)	Medewerkers weten welk kanaal ze wanneer gebruiken.
Cryptografie (h)	Bestanden zijn versleuteld tijdens transport en opslag, volgens beleid.
Toegang en authenticatie (i, j)	Alleen de geverifieerde ontvanger krijgt toegang; medewerkers loggen in met MFA of SSO.

Een bruikbare bewijsketen

Leg per maatregel vast:

Verplichting of risico › Ingerichte maatregel › Toets op werking › Beschikbare informatie › Beoordeelde afwijking

Onderscheid beleidsvoornemens van afspraken die aantoonbaar worden toegepast.

Een platform, certificaat of audit trail ondersteunt delen van uw beheersomgeving. Het maakt een gemeente niet automatisch compliant met alle verplichtingen.

03 / MELDEN ONDER DE CBW EN DE AVG

Twee termijnen, één vraag: wat is er gedeeld?

Bij een incident lopen de Cbw-meldplicht en de AVG-meldplicht naast elkaar. Houd de regimes uit elkaar, maar bereid één reconstructie voor.



FIGUUR 2 / MELDTERMIJNEN ONDER DE CBW EN DE AVG. BRONNEN: [2][4][7].

Leg de geldende termijnen vast in het incidentdraaiboek en laat de bevoegde functie beoordelen welk regime van toepassing is. Indicatief overzicht, geen juridisch advies.

04 / HET CONTROLEMODEL

Vier onderdelen van grip

"Het is versleuteld" zegt of u beveiligt. Een toezichthouder vraagt ook hoe u dat aantoont.

Het model hieronder is ons eigen managementmodel. Het helpt teams om samen het gesprek te voeren. Het is geen norm, geen certificeringsmodel en geen beschrijving van een geautomatiseerde productwerking.

01

Beleid

Wat, waarom en voor wie?

02

Toegang

Wie, hoe en hoe lang?

03

Gebruik

Werkt de complete taak?

04

Bewijs

Wat kunnen we aantonen?

FIGUUR 3 / VIER ONDERDELEN VAN GRIP. EIGEN MODEL, GELIJK AAN DE MANAGEMENTGIDS "GRIP OP VEILIGE BESTANDSDELING".

Beleid: bepaal de bedoeling

Welke informatie is nodig, wie beslist daarover en welke route past bij het risico? Leg regels en uitzonderingen vast per type informatie, met een eigenaar, gekoppeld aan BIO2 en de risicoanalyse.

Gebruik: toets het echte werk

Laat afzenders en externe ontvangers de complete taak uitvoeren, ook met grote bestanden en zonder account. Waar de goedgekeurde route stokt, ontstaan omwegen via e-mail of gratis diensten.

Toegang: maak voorwaarden concreet

Bepaal wie toegang krijgt, hoe contactgegevens en identiteit worden gecontroleerd en wanneer toegang eindigt. Medewerkers loggen in met MFA of SSO; toegang volgt vertrek en rolwijziging.

Bewijs: toets en verbeter

Verbind instellingen, tests, relevante loggegevens en besluiten. Een exporteerbare audit trail en een draaiboek laten binnen 24 uur zien wie wat met wie deelde, wanneer en onder welk beleid.

Het zwakste onderdeel bepaalt waar u begint. Een uitgebreide audit trail compenseert geen onduidelijk doel of een bestand bij de verkeerde ontvanger.

05 / DE EERSTE 90 DAGEN

Van besluit naar aantoonbaar resultaat

Zes stappen in drie fasen, elk met een eigenaar en een concreet bewijsstuk.

Het plan hieronder is ons eigen organisatiemodel. Pak urgente risico's en bestaande wettelijke plichten direct op: het schema biedt geen juridische uitsteltermijn.

Wk 1–4

Beleggen

Eigenaarschap + bestandsstromen

Wk 4–10

Inrichten

BIO2-koppeling + één kanaal

Wk 8–12+

Borgen

Medewerkers + aantonen

FIGUUR 4 / DE EERSTE 90 DAGEN. EIGEN ORGANISATIEMODEL. AAN HET EIND VAN ELKE FASE EEN BESLUIT.

#	Stap	Eigenaar	Bewijsstuk
1	Eigenaarschap beleggen	Gemeentesecretaris, CISO	Collegebesluit of memo met scope en rapportagelijn
2	Bestandsstromen in kaart	CISO, privacy officer	Overzicht met eigenaar per stroom (werkblad p. 10)
3	Koppelen aan BIO2 en risico	CISO, FG	Geactualiseerde risicoanalyse en classificatie
4	Eén gecontroleerd kanaal	I&A, inkoop, CISO	Inrichting, leveranciersbeoordeling, verwerkersovereenkomst
5	Medewerkers meenemen	Teamleiders, HR, communicatie	Werkinstructie, trainingsregistratie, gebruikscijfers
6	Aantonen en verbeteren	CISO, controller	Kwartaalrapportage, incidentdraaiboek, zelftestscore

Bewaar per fase besluiten, eigenaren, testresultaten en afwijkingen. Breid uit op basis van aangetoonde werking, niet alleen op basis van planning.

05 / ZES STAPPEN UITGEWERKT

Begin klein, bouw een dossier

Kies de bestandsstroom met het hoogste risico, vaak het sociaal domein, en doorloop daarvoor alle zes stappen.

1 / Beleg eigenaarschap

Wijs een proceseigenaar aan die inhoud, techniek en uitvoering verbindt. Agendeer het onderwerp bij het college als onderdeel van de Cbw-aanpak en leg vast hoe u rapporteert in de planning-en-controlcyclus.

2 / Breng bestandsstromen in kaart

Inventariseer per afdeling met wie u deelt, welke informatie en via welk kanaal. Begin bij het sociaal domein en vergunningverlening: daar zitten de gevoeligste en de grootste bestanden.

3 / Koppel aan BIO2 en risico

Bepaal per stroom het betrouwbaarheidsniveau en de bijbehorende BIO2-maatregelen. Neem externe documentuitwisseling expliciet op in de cyberrisicoanalyse. De handreikingen van de IBD zijn een bruikbare referentie.

4 / Richt één kanaal in

Spreek af dat vertrouwelijke en grote bestanden via één beheerde route gaan, met vaste regels voor verificatie, geldigheid en logging. Zorg dat de route werkt voor ontvangers zonder account. Beoordeel de leverancier op certificering, locatie, toegang en exit.

5 / Neem medewerkers mee

Maak veilig delen de makkelijkste route, bijvoorbeeld via Outlook en SSO. Schrijf een korte werkinstructie en start met een pilot in één team. Security awareness ondersteunt, maar deelname alleen bewijst nog niet dat de route wordt gevolgd.

6 / Toon aan en verbeter

Exporteer periodiek activiteitenlogs en bespreek afwijkingen. Leg in een draaiboek vast hoe u binnen 24 uur, 72 uur en een maand meldt. Rapporteer per kwartaal aan het college en herhaal de zelftest jaarlijks.

Praktijkoefening: laat een afzender en een externe ontvanger samen één overdracht uitvoeren zonder begeleiding. Verbeter de eerste stap waarop zij vastlopen.

06 / WERKBLAD

Welke bestanden verlaten uw gemeente?

Vul per afdeling de belangrijkste externe bestandsstromen in. De eerste regel is een fictief voorbeeld.

Afdeling	Externe partij	Informatie	Kanaal	L/M/H	Eigenaar	Aantoonbaar?
Jeugd	Zorgaanbieder	Jeugdhulpdossier	E-mailbijlage	H	Teamleider	Nee, geen logging

Hulpvragen

- Welke afdelingen sturen wekelijks bestanden met persoonsgegevens naar buiten?
- Waar worden bestanden te groot voor e-mail, en wat doen medewerkers dan?
- Welke externe partijen ontvangen informatie zonder dat zij een account hebben?

Eigen werkblad voor intern gebruik. Gebruik fictieve of geminimaliseerde gegevens in voorbeelden.

06 / ZELFTEST

Wat kunt u vandaag aantonen?

Twaalf stellingen over één bestandsstroom. Een onbekend antwoord vraagt om onderzoek.

Score per stelling: Ja = 2, Deels = 1, Nee = 0. De test staat ook online op msafe.co/nl/veilige-documentuitwisseling-gemeenten.

Stelling	Ja	Deels	Nee
01 / Beleid			
1. Er is een benoemde eigenaar voor externe documentuitwisseling; het college is geïnformeerd.	○	○	○
2. Vastgelegd is welke informatie via welk kanaal mag, gekoppeld aan BIO2 en de risicoanalyse.	○	○	○
3. De leverancier is beoordeeld op certificering, locatie en exit, en contractueel geborgd.	○	○	○
02 / Toegang			
4. Medewerkers die extern delen, loggen in met MFA of via SSO.	○	○	○
5. Externe ontvangers worden geverifieerd voordat zij een bestand openen.	○	○	○
6. Toegang eindigt op tijd: bestanden hebben een geldigheid en vertrek of rolwijziging trekt toegang in.	○	○	○
03 / Gebruik			
7. Vertrouwelijke en grote bestanden gaan via één beheerd kanaal, niet via e-mailbijlagen.	○	○	○
8. Afzender en externe ontvanger ronden een overdracht zelfstandig af, ook zonder account.	○	○	○
9. Medewerkers weten via een korte werkinstructie welk kanaal ze wanneer gebruiken.	○	○	○
04 / Bewijs			
10. Per uitwisseling is terug te zien wie wat met wie deelde en wanneer.	○	○	○
11. Activiteitenlogs zijn exporteerbaar en worden periodiek beoordeeld.	○	○	○
12. Bij een incident is binnen 24 uur te reconstrueren wat gedeeld is.	○	○	○

Totaalscore: _____ / 24

Bestandsstroom / eigenaar / datum: _____

06 / UITSLAG

Lees de score per onderdeel

De totaalscore geeft richting. Het onderdeel met de laagste score bepaalt waar u begint.

Kwetsbaar

0 tot 10 punten

Externe documentuitwisseling is nog geen beheerst proces. Start met stap 1 en 2: eigenaarschap en een overzicht van bestandsstromen.

Op weg

11 tot 18 punten

De basis staat, maar is nog niet volledig aantoonbaar. Werk eerst het onderdeel met de laagste score bij.

In control

19 tot 24 punten

Borg het in de planning-en-controlcyclus, rapporteer aan college en raad en herhaal de test jaarlijks.

Onderdeel	Score	Bij 3 punten of minder: begin hier
Beleid	___ / 6	Benoem een eigenaar, leg regels per type informatie vast, koppel aan BIO2 en beoordeel de leverancier.
Toegang	___ / 6	Koppel het kanaal aan identiteitsbeheer (SSO, MFA), verifieer ontvangers en laat toegang op tijd eindigen.
Gebruik	___ / 6	Breng gevoelige en grote bestanden onder in één kanaal dat werkt voor afzender en ontvanger, met een werkinstructie.
Bewijs	___ / 6	Zorg voor een exporteerbare audit trail en een draaiboek dat binnen 24 uur werkt.

Gebruik de totaalscore niet als geruststelling

Prioriteer op risico en afhankelijkheden. Een zwak onderdeel Toegang kan uitbreiding blokkeren, ook als de andere onderdelen goed scoren. Leg vooraf vast welke tekortkomingen kritiek zijn en wie restrisico mag accepteren.

Uw uitslag bespreken? Zie de gratis Cbw-werksessie op pagina 14.

Eigen zelftest voor intern gebruik. Geen gevalideerde audit, juridische norm of verklaring van naleving.

07 / WAAR MSAFE PAST

Een uitwisselingsplatform binnen uw proces

Msafe richt zich op veilige, gecontroleerde en aantoonbare externe bestandsuitwisseling. De waarde moet blijken in uw eigen bestandsstroom.

Msafe Secure File Transfer brengt identiteitskoppeling, deelregels en activiteitsinformatie samen rond externe uitwisseling. De actuele leveranciersinformatie beschrijft SSO via Microsoft Entra ID en SCIM, verificatie van ontvangers, delen via web en Outlook, Easy Download voor ontvangers zonder account en exporteerbare activiteitenlogs. [9]

Msafe is sinds 2012 actief, ISO/IEC 27001:2022-gecertificeerd door DEKRA en host data in Nederland. Controleer de beschikbaarheid, licentie en configuratie van de functies die u nodig heeft. SSO, SCIM en de Outlook-add-in horen bij Enterprise en Unlimited. [9]

Managementvraag	Wat u vraagt in een demo of pilot
Zijn onze regels uitvoerbaar?	Toon de deelregels en beleidstoewijzing in ons eigen scenario.
Werkt het voor externe partijen?	Laat een ontvanger zonder account openen en verifiëren.
Kunnen we snel ingrijpen?	Test een fout, een intrekking en de grens na een eerdere download.
Kunnen we reconstrueren?	Bekijk en exporteer activiteitsinformatie; leg velden en beperkingen vast.

Waar u op let bij de keuze

- Versleuteling tijdens transport en opslag
- Verificatie van de ontvanger, ook zonder account
- Geldigheid en intrekbare toegang
- Exporteerbare audit trail
- Grote bestanden (tot 1 TB bij Enterprise)
- Outlook-integratie en SSO
- Certificering van de leverancier
- Hostinglocatie en subverwerkers
- Verwerkersovereenkomst volgens de AVG
- Afspraken over exit en verwijdering

Leveranciersinformatie gecontroleerd op 26 oktober 2026. Intrekken stopt verdere toegang via de dienst, maar haalt een eerder gedownloade kopie niet terug. Deze white paper is geen onafhankelijke productaudit; de gemeente blijft verantwoordelijk voor naleving.

08 / CBW-WERKSESSIE VOOR GEMEENTEN

Breng één bestandsstroom mee

In 60 minuten brengt u samen met een specialist van Msafe in kaart welke bestanden uw gemeente verlaten, wie ze ontvangt en wat u daarvan kunt aantonen.

De werksessie is gratis voor gemeenten en Cbw-plichtige gemeenschappelijke regelingen. Ze is bedoeld voor CISO's, informatiebeveiligers, privacy officers en I&A-managers. We werken met het External Data Control Canvas en scoren uw situatie van 0 tot 4 op de vier onderdelen van grip uit deze white paper. [10]

Het canvas blijft van uw gemeente, ook als u verder niets met Msafe doet. Gebruik het werkblad en de zelftest uit deze white paper als voorbereiding: dan gaat de sessie direct over uw eigen situatie.

U ontvangt binnen twee werkdagen	Waarvoor u het gebruikt
Ingevuld canvas	Overzicht van externe bestandsstromen, partijen en kanalen.
Scorekaart	Score van 0 tot 4 op beleid, toegang, gebruik en bewijs.
Top 3 verbeteracties	Met eigenaar en termijn, bruikbaar voor college en P&C-cyclus.

> "Gemeenten hoeven niet te bewijzen dat ze de perfecte tool hebben. Ze moeten kunnen laten zien dat ze grip hebben: wie wat deelt, met wie en onder welke voorwaarden. Dat is waar bewijsbaarheid om draait."
>
> Hennie Jansen, CCO Msafe

Plan de werksessie via msafe.co/nl/contact en vermeld "Cbw-werksessie gemeente".

Een werksessie is een gezamenlijke verkenning, geen audit of juridisch advies.

BRONNEN EN REDACTIONELE BASIS

Onderbouwing en verder lezen

Peildatum onderzoek: 26 oktober 2026. Wetgeving en officiële bronnen zijn onderscheiden van leveranciersinformatie.

De vier onderdelen van grip, het stappenplan, het werkblad en de zelftest zijn eigen praktische bijdragen. Het zijn geen wettelijke normen of gevalideerde audits.

Deze white paper geeft algemene informatie. De volledige regels, actuele productvoorwaarden en uw eigen situatie bepalen de juiste toepassing.

[1] Rijksoverheid
Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten vanaf 15 augustus 2026 van kracht, 7 juli 2026.

[2] VNG
Cyberbeveiligingswet, NIS2-richtlijn en Wet weerbaarheid kritieke entiteiten: nieuws en updates, 2026.

[3] iBestuur
Veel gemeenten moeten nog stappen zetten voor cyberwet, 14 augustus 2026.

[4] Gemeente.nu
Cyberbeveiligingswet van kracht: gemeenten moeten zich registreren bij het NCSC, september 2026.

[5] Autoriteit Persoonsgegevens
Jaarverslag 2025, via Binnenlands Bestuur: Meer klachten en datalekken, maar minder boetes, 7 april 2026.

[6] NIS2-richtlijn
Richtlijn (EU) 2022/2555, artikel 21: maatregelen voor het beheer van cyberbeveiligingsrisico's.

[7] AVG
Verordening (EU) 2016/679, artikelen 33 en 34: melding van inbreuken.

[8] Informatiebeveiligingsdienst
Ondersteuning en handreikingen BIO2 voor gemeenten.

[9] Msafe Secure File Transfer
Leveranciersinformatie: identiteit, verificatie, delen, activiteitenlogs, hosting en certificering.

[10] Msafe werksessie
Leveranciersinformatie: External Data Control Canvas en werkwijze.

Uitgegeven door Msafe B.V., IJsselstein | Oktober 2026 | © 2026 Msafe B.V. Figuren 3 en 4 zijn eigen modellen. Figuren 1 en 2 zijn vrij te delen met bronvermelding. Geen softwareschermafbeeldingen of echte incidentgegevens.