



Beveiligings- en Privacyrapport Beeldbank B.V.

Inzicht in de beveiligingsmaatregelen en gegevensbescherming bij Beeldbank B.V.

Versie:

V8.0

Datum:

September 2026





Inhoudsopgave

Beveiligings- en Privacyrapport Beeldbank B.V.....	1
Inzicht in de beveiligingsmaatregelen en gegevensbescherming bij Beeldbank B.V.....	1
1. Inleiding	5
1.1 Doel van het rapport	5
1.2 Relevante wetgeving en normen	5
Algemene Verordening Gegevensbescherming — AVG/GDPR	6
Uitvoeringswet AVG — UAVG	6
Europese AI-verordening — AI Act.....	6
Auteurswet, portretrecht en intellectuele eigendomsrechten	7
Nederlands contractenrecht en toepasselijk recht.....	7
ISO 27001:2022	7
NIS2-richtlijn	8
Verwerkersovereenkomst	8
Beheerovereenkomst en serviceafspraken	8
Algemene voorwaarden en gebruiksvoorwaarden	8
1.3 Scope en doelgroep.....	9
2. Over Beeldbank.....	10
2.1 Context en functionaliteit van Beeldbank	10
2.2 Gegevens die worden verwerkt en doeleinden	10
Beeld- en mediabestanden	10
Metadata en tags	11
Persoonsgegevens van afgebeelde personen	11
Gebruikersgegevens	11
Technische gegevens en loggegevens	11
Gegevens bij optionele AI-functionaliteiten.....	11
Doeleinden van de verwerking.....	12
2.3 Samenwerking met subverwerkers	12
2.4 Waarborging van beveiliging en privacy.....	12
3. Beveiligingsmaatregelen	14
3.1 Technische beveiliging	14
Toegangsbeheer en autorisatie	14
Authenticatie en veilige toegang.....	14



Versleuteling.....	14
Logging en monitoring.....	15
Capaciteitsbeheer	15
Patch- en updatebeheer.....	15
Kwetsbaarhedenbeheer	15
3.2 Veilige softwareontwikkeling en wijzigingsbeheer.....	15
Ontwikkelproces	16
OTAP-structuur	16
Broncodebeheer.....	16
3.3 Organisatorische beveiliging	16
Beleid en verantwoordelijkheden	16
Vertrouwelijkheid	16
Leveranciersbeheer	17
Bewustwording en veilig werken.....	17
3.4 Back-up en herstel.....	17
3.5 Bescherming tegen dreigingen.....	17
3.6 Incidentmanagement en opvolging	18
3.7 Continue verbetering binnen het ISO 27001-gecertificeerde ISMS.....	18
4. Privacy en verwerking van persoonsgegevens.....	19
4.1 Verwerkingsdoelen en categorieën betrokkenen.....	19
4.2 Rolverdeling en verantwoordelijkheden	20
4.3 Toegangsbeheer en beveiliging van persoonsgegevens.....	20
4.4 Bewaartermijnen en verwijderingsbeleid.....	21
4.5 Verwerking door subverwerkers	22
4.6 Meldplicht datalekken en beveiligingsincidenten	22
4.7 Rechten van betrokkenen.....	23
4.8 Gezichtsdetectie, embeddings en naamsuggesties.....	23
Belangrijke waarborgen	24
4.9 Back-ups en herstel	24
4.10 Privacy by design en dataminimalisatie	25
4.11 Samenvatting.....	25
5. Digitale toegankelijkheid.....	26
5.1 Context en richtlijnen	26
5.2 Gebruiksvriendelijkheid en toegankelijkheid binnen Beeldbank	26
5.3 Toegankelijkheid, privacy en veilige standaardinstellingen	27
5.4 Beperkingen en afhankelijkheden	27





5.5 Doorontwikkeling en verbetering	27
6. Compliance en risico's.....	29
6.1 Toetsing aan AVG, ISO 27001 en andere kaders.....	29
6.2 Risicomanagement en BIV-classificatie	29
6.3 Gegevensbeschermingseffectbeoordeling - DPIA	30
6.4 Beheer van informatiebeveiligingsincidenten	30
6.5 Continuïteitsplanning en beschikbaarheid	31
6.6 Exitstrategie en beëindiging van de dienstverlening	31
6.7 Samenwerking met leveranciers en subverwerkers.....	31
6.8 AI-functionaliteiten en compliance.....	32
6.9 Audits, beoordelingen en verbetermaatregelen	32
6.10 Samenvatting.....	33
7. Gebruik van subverwerkers.....	34
7.1 Leveranciersbeoordeling en beheersing	34
7.2 DigitalOcean	35
7.3 Google Cloud Storage	35
7.4 Google Vision API.....	36
7.5 Overige ondersteunende leveranciers	36
7.6 Verwerking binnen en buiten de Europese Economische Ruimte.....	36
7.7 Wijzigingen in subverwerkers	36
7.8 Exit en verwijdering bij subverwerkers	37
7.9 Samenvatting.....	37
8. Conclusie en aanbevelingen	38
8.1 Samenvatting van maatregelen en compliance	38
8.2 Toekomstige verbeterpunten en planning	38
8.3 Eindconclusie.....	39
9. Bijlagen en verwijzingen.....	40
9.1 Contractuele documenten Beeldbank	40
9.2 Subverwerkers en externe bewijsdocumentatie.....	41
9.3 Beschikbaarheid en actualisatie.....	42
9.4 Samenvatting.....	42





1. Inleiding

1.1 Doel van het rapport

Dit rapport geeft inzicht in de maatregelen die Beeldbank neemt op het gebied van informatiebeveiliging, privacy, continuïteit en gegevensbescherming. Het rapport is bedoeld om klanten, privacy officers, CISO's, ICT-managers en andere betrokkenen op een duidelijke manier te laten zien hoe Beeldbank omgaat met persoonsgegevens, klantdata, beveiligingsrisico's en wettelijke verplichtingen.

Beeldbank verwerkt namens haar klanten beeld- en mediabestanden, metadata, gebruikersgegevens en, afhankelijk van de inrichting door de klant, mogelijk ook persoonsgegevens van afgebeelde personen. Daarbij kan worden gedacht aan namen, portretrechten, toestemmingsinformatie, contactgegevens, gezichtsuitsneden of technische kenmerken die worden gebruikt voor optionele functies zoals gezichtsdetectie en naamsuggesties.

Het doel van dit rapport is om transparantie te bieden over:

- de technische en organisatorische beveiligingsmaatregelen van Beeldbank;
- de manier waarop Beeldbank invulling geeft aan privacy en gegevensbescherming;
- de wijze waarop Beeldbank werkt met leveranciers en subverwerkers;
- de uitgangspunten voor bewaartermijnen, verwijdering en exitprocedures;
- de invulling van ISO 27001:2022 binnen het gecertificeerde managementsysteem van Beeldbank;
- de verbetermaatregelen die Beeldbank neemt in het kader van continue verbetering.

Dit rapport is een verantwoordingsdocument. Het beschrijft hoe Beeldbank haar beveiligings- en privacymaatregelen heeft ingericht en welke beheersmaatregelen worden toegepast. Beeldbank is ISO 27001:2022 gecertificeerd. Certificaatnummer NL 3108.1.1, afgegeven door Brand Compliance B.V., geaccrediteerd door de Raad voor Accreditatie. De certificeringsaudit vond plaats op 25 en 27 augustus 2026 en leverde geen afwijkingen op. Het certificaat is te valideren via IAF CertSearch (iafcertsearch.org). De volgende audit in de cyclus staat gepland voor augustus 2027. Dit rapport is een toelichting op de maatregelen achter dat certificaat. Het certificaat zelf is op aanvraag beschikbaar. Dit sluit aan bij de verwerkersovereenkomst, waarin is vastgelegd dat Beeldbank passende technische en organisatorische maatregelen neemt en werkt volgens de beheersmaatregelen van ISO 27001.

1.2 Relevante wetgeving en normen

Beeldbank verwerkt persoonsgegevens en klantdata binnen de kaders van toepasselijke Europese en Nederlandse wet- en regelgeving. Daarnaast gebruikt Beeldbank algemeen aanvaarde normen voor informatiebeveiliging, privacybescherming, continuïteit en zorgvuldig gebruik van online diensten.

De belangrijkste wettelijke en normatieve kaders voor dit rapport zijn:





Algemene Verordening Gegevensbescherming — AVG/GDPR

De AVG is het belangrijkste wettelijke kader voor de verwerking van persoonsgegevens binnen Beeldbank. Binnen de dienstverlening is de klant in de meeste gevallen verwerkingsverantwoordelijke en treedt Beeldbank op als verwerker, tenzij schriftelijk anders is overeengekomen. Dit betekent dat de klant bepaalt voor welke doelen persoonsgegevens worden verwerkt en dat Beeldbank deze gegevens verwerkt volgens de instructies van de klant en de afspraken in de verwerkersovereenkomst.

De AVG is onder meer relevant voor:

- het opslaan en beheren van beeld- en mediabestanden;
- metadata en toestemmingsinformatie;
- gebruikersaccounts en toegangsbeheer;
- loggegevens en beveiligingsmonitoring;
- gezichtsdetectie, naamsuggesties en biometrische sjablonen wanneer deze functies zijn ingeschakeld;
- bewaartermijnen, verwijdering en rechten van betrokkenen.

Uitvoeringswet AVG — UAVG

De UAVG vult de AVG aan voor de Nederlandse situatie. Deze wet is relevant omdat Beeldbank wordt gebruikt door Nederlandse organisaties en omdat beeldmateriaal persoonsgegevens kan bevatten. De UAVG is vooral van belang bij de beoordeling van rechtmatigheid, bijzondere persoonsgegevens, uitzonderingen en nationale invulling van privacyregels.

In de verwerkersovereenkomst staat dat op de verwerking van persoonsgegevens door Beeldbank zowel de AVG als de UAVG van toepassing zijn.

Europese AI-verordening — AI Act

De Europese AI-verordening is relevant voor Beeldbank voor zover binnen de dienstverlening gebruik wordt gemaakt van AI-functionaliteiten, zoals automatische beeldanalyse, AI-tagging, gezichtsdetectie en naamsuggesties.

Binnen Beeldbank worden deze functies alleen ingezet ter ondersteuning van opslag, beheer, zoeken en organiseren van beeldmateriaal. Naamsuggesties vinden plaats met menselijke bevestiging. Dat betekent dat het systeem niet zelfstandig definitieve besluiten neemt over personen, maar gebruikers ondersteunt bij het herkennen, taggen of beheren van beeldmateriaal. De verwerkersovereenkomst benoemt deze automatische analyse expliciet als optionele functionaliteit binnen de Beeldbank-dienst.

Voor het rapport is vooral belangrijk om op te nemen dat Beeldbank:

- klantdata niet gebruikt om algemene AI-modellen te trainen zonder uitdrukkelijke toestemming;
- AI-functionaliteiten inzet binnen de uitvoering, beveiliging, ondersteuning en verbetering van de dienst;
- menselijke bevestiging toepast bij naamsuggesties;
- AI-functionaliteiten beoordeelt op privacyrisico's, transparantie, dataminimalisatie en beveiliging;
- klanten ondersteunt bij vragen over rechtmatig gebruik van AI-functionaliteiten.



In de algemene voorwaarden staat dat Beeldbank klantdata niet gebruikt voor het trainen van AI-modellen, machine learning-toepassingen of andere doeleinden buiten de uitvoering, beveiliging, ondersteuning en verbetering van de dienst, tenzij de klant daarvoor vooraf uitdrukkelijk toestemming heeft gegeven.

Auteurswet, portretrecht en intellectuele eigendomsrechten

Omdat Beeldbank wordt gebruikt voor opslag, beheer, publicatie en delen van beeldmateriaal, kunnen auteursrecht, portretrecht en andere intellectuele eigendomsrechten van toepassing zijn. De licentienemer is zelf verantwoordelijk voor de rechtmatigheid van de content die binnen Beeldbank wordt opgeslagen, beheerd, gedeeld of gepubliceerd.

Dit betekent dat de licentienemer zelf moet beoordelen of hij beschikt over de benodigde rechten, toestemmingen, licenties of andere grondslagen voor het gebruik van het beeldmateriaal. Daarbij kan het bijvoorbeeld gaan om toestemming van een fotograaf, toestemming van afgebeelde personen, afspraken over portretrecht of gebruiksrechten op beeldmateriaal.

Beeldbank faciliteert het veilig beheren, vinden, delen en publiceren van beeldmateriaal, maar beoordeelt niet zelfstandig of de door de licentienemer geplaatste content auteursrechtelijk, portretrechtelijk of anderszins rechtmatig mag worden gebruikt. Deze verantwoordelijkheid ligt bij de licentienemer als gebruiker en beheerder van de content.

Nederlands contractenrecht en toepasselijk recht

Op de overeenkomsten, diensten en rechtsverhoudingen tussen Beeldbank en klanten is Nederlands recht van toepassing. Dit is relevant voor onder meer aansprakelijkheid, beëindiging, exit, serviceafspraken, vertrouwelijkheid en geschillen.

In de algemene voorwaarden (<https://beeldbank.nl/algemene-voorwaarden/>) staat dat op alle overeenkomsten, diensten en rechtsverhoudingen tussen Beeldbank en de licentienemer uitsluitend Nederlands recht van toepassing is.

ISO 27001:2022

Beeldbank is ISO 27001:2022 gecertificeerd (certificaat NL 3108.1.1, Brand Compliance B.V.). ISO 27001:2022 is het belangrijkste normenkader voor informatiebeveiliging binnen dit rapport. De norm richt zich op het opzetten, beheren en continu verbeteren van een Information Security Management System, oftewel ISMS.

Beeldbank gebruikt ISO 27001:2022 als kader voor onder meer:

- informatiebeveiligingsbeleid;
- risicobeoordeling;
- toegangsbeheer;
- gebruik van MFA;
- patch- en updatebeleid;
- incidentmanagement;
- back-upbeleid;
- leveranciersbeheer;
- logging en monitoring;
- continuïteit;
- veilige softwareontwikkeling;
- periodieke evaluatie en verbetering.





Beeldbank hanteert een informatiebeveiligingsbeleid waarin de belangrijkste beveiligingsprocessen zijn vastgelegd. Dit beleid omvat onder meer toegangsbeheer, het gebruik van multi-factor-authenticatie waar passend, patch- en updatebeheer, incidentmanagement, back-up en herstel, leveranciersbeheer en periodieke evaluatie van beveiligingsmaatregelen. Het beleid wordt minimaal jaarlijks beoordeeld en waar nodig aangepast op basis van risico's, wijzigingen in de dienstverlening, incidenten, audits of nieuwe wettelijke en normatieve eisen.

Het ISMS van Beeldbank wordt jaarlijks intern geaudit en extern door Brand Compliance. Dit rapport beschrijft hoe Beeldbank de maatregelen uit ISO 27001:2022 heeft ingericht en welke verbeterpunten uit de laatste audit worden opgevolgd.

NIS2-richtlijn

Dit rapport stelt niet vast dat Beeldbank of iedere klant rechtstreeks onder de NIS2-verplichtingen valt. NIS2 wordt hier gebruikt als relevant referentiekader voor weerbaarheid, risicobeheersing, continuïteit en leveranciersbeveiliging. Ook wanneer Beeldbank of een specifieke klant niet rechtstreeks onder alle NIS2-verplichtingen valt, zijn de uitgangspunten bruikbaar voor het versterken van beveiliging en continuïteit.

- beveiliging van netwerk- en informatiesystemen;
- incidentdetectie en incidentrespons;
- continuïteit van dienstverlening;
- back-up en herstel;
- leveranciersbeheer;
- beveiliging van cloud- en hostingdiensten;
- periodieke beoordeling van risico's.

Verwerkersovereenkomst

De verwerkersovereenkomst is een belangrijk juridisch kader voor alle verwerkingen die Beeldbank namens klanten uitvoert. Hierin staan afspraken over de rolverdeling, doeleinden, beveiligingsmaatregelen, subverwerkers, datalekken, bewaartermijnen, verwerking buiten de EER en beëindiging.

De verwerkersovereenkomst bepaalt dat Beeldbank persoonsgegevens uitsluitend verwerkt in opdracht van de klant en volgens schriftelijke instructies, tenzij een wettelijke verplichting anders voorschrijft.

Beheerovereenkomst en serviceafspraken

De beheerovereenkomst is relevant voor beheer, onderhoud, ondersteuning, monitoring, responstijden, vertrouwelijkheid, beveiligingsmaatregelen, exit en datalekken. Hierin is onder meer opgenomen dat Beeldbank beheer- en supportdiensten levert, meldingen vastlegt in Jira, monitoring uitvoert en remote support biedt.

Algemene voorwaarden en gebruiksvoorwaarden

De algemene voorwaarden bevatten aanvullende verplichtingen voor veilig en rechtmatig gebruik van de dienst. Gebruikers mogen de dienst onder meer niet gebruiken voor onrechtmatige content, malware, ongeautoriseerde toegang, verstoring van systemen of verwerking van persoonsgegevens zonder geldige grondslag. Ook moeten klanten beveiligingsincidenten, kwetsbaarheden of vermoedens van misbruik onverwijld melden aan Beeldbank.



1.3 Scope en doelgroep

Dit rapport heeft betrekking op de Beeldbank-dienst en de processen, systemen, leveranciers en beveiligingsmaatregelen die nodig zijn voor het leveren, beheren, beveiligen en ondersteunen van deze dienst.

Binnen de scope van dit rapport vallen in ieder geval:

- de Beeldbank SaaS-applicatie;
- het opslaan, beheren, zoeken, delen, downloaden en publiceren van beeld- en mediabestanden;
- gebruikersbeheer, rollen, rechten en autorisaties binnen de applicatie;
- metadata, toestemmingsinformatie en overige gegevens die door of namens de licentienemer in Beeldbank worden vastgelegd;
- optionele functionaliteiten zoals AI-tagging, gezichtsdetectie en naamsuggesties;
- hosting, opslag, back-ups, monitoring en technisch beheer;
- logging, beveiligingsmonitoring en incidentafhandeling;
- support-, beheer- en onderhoudsprocessen;
- leveranciers en subverwerkers die betrokken zijn bij de levering van de Beeldbank-dienst;
- bewaartermijnen, verwijdering, export en exit van klantdata;
- beveiligingsmaatregelen rond ontwikkeling, test, acceptatie en productie;
- risicobeheersing en verbetermaatregelen binnen het gecertificeerde ISMS.

De scope sluit aan op de dienstverlening van Beeldbank: het aanbieden van een veilige online omgeving voor het beheren, beschermen en delen van beeld- en mediabestanden. Daarbij richt dit rapport zich op de maatregelen die Beeldbank zelf toepast of contractueel beheerst via haar leveranciers en subverwerkers.

Niet binnen de scope van dit rapport vallen de interne processen, systemen en besluiten van de licentienemer. De licentienemer blijft zelf verantwoordelijk voor onder meer:

- de rechtmatigheid van het uploaden, opslaan, delen en publiceren van beeldmateriaal;
- het beschikken over de benodigde toestemmingen, licenties, gebruiksrechten en grondslagen;
- het bepalen van interne bewaartermijnen voor eigen content;
- het toekennen en intrekken van gebruikersrechten binnen de eigen organisatie;
- de juistheid en volledigheid van ingevoerde metadata;
- het beoordelen van publicatie- en portretrechtelijke belangen;
- het beantwoorden van verzoeken van betrokkenen, voor zover deze verantwoordelijkheid bij de licentienemer ligt;
- het eigen interne informatiebeveiligingsbeleid en apparaatbeheer van gebruikers.

Beeldbank ondersteunt de licentienemer met technische en organisatorische maatregelen, contractuele afspraken en functionaliteiten binnen de applicatie. De verantwoordelijkheid voor de inhoud, het gebruik en de rechtmatigheid van de door de licentienemer geplaatste gegevens blijft echter bij de licentienemer, tenzij schriftelijk anders is overeengekomen.



2. Over Beeldbank

2.1 Context en functionaliteit van Beeldbank

Beeldbank is een Software-as-a-Service-oplossing waarmee organisaties beeld- en mediabestanden veilig kunnen opslaan, beheren, zoeken, delen en publiceren. De dienst is bedoeld voor organisaties die veel werken met foto's, video's, huisstijlmateriaal, communicatiemiddelen en andere digitale mediabestanden.

Beeldbank ondersteunt klanten onder meer met:

- centrale opslag van beeld- en mediabestanden;
- zoeken en filteren op metadata, tags en andere kenmerken;
- beheer van gebruikers, rollen en rechten;
- vastlegging en beheer van toestemmingen en publicatierechten;
- delen van bestanden met interne en externe partijen;
- optionele AI-functionaliteiten, zoals automatische tagsuggesties, gezichtsdetectie en naamsuggesties;
- back-up, monitoring, technisch beheer en ondersteuning.

Beeldbank levert de applicatie als online dienst en verzorgt daarbij ook de technische hosting, het beheer en de beveiliging van de omgeving. Hierdoor hoeven klanten zelf geen eigen infrastructuur voor de Beeldbank-dienst te beheren.

De dienst is ontwikkeld voor teams die beeldmateriaal op een gestructureerde en veilige manier willen beheren, zoals marketing-, communicatie-, HR-, archief-, voorlichtings- en contentteams. Daarbij ondersteunt Beeldbank klanten met functionaliteiten die helpen om zorgvuldig om te gaan met persoonsgegevens, toestemmingen, publicatierechten en het veilig delen van bestanden.

De klant, in de overeenkomst aangeduid als licentienemer of verwerkingsverantwoordelijke, blijft verantwoordelijk voor de inhoud die in Beeldbank wordt geplaatst en voor de rechtmatigheid van het gebruik daarvan. Beeldbank is verantwoordelijk voor het leveren, beveiligen en beheren van de dienst conform de contractuele afspraken.

2.2 Gegevens die worden verwerkt en doeleinden

Beeldbank verwerkt gegevens die nodig zijn voor het leveren, beveiligen, beheren en ondersteunen van de Beeldbank-dienst. De verwerking vindt plaats in overeenstemming met de verwerkersovereenkomst, de AVG en de instructies van de klant.

Binnen Beeldbank kunnen onder meer de volgende categorieën gegevens worden verwerkt:

Beeld- en mediabestanden

Dit zijn de bestanden die door of namens de klant worden geüpload en beheerd, zoals foto's, video's, documenten, logo's en ander digitaal beeldmateriaal. Deze bestanden kunnen persoonsgegevens bevatten wanneer personen herkenbaar in beeld zijn of wanneer de bestanden aan personen gekoppelde informatie bevatten.



Metadata en tags

Bij beeld- en mediabestanden kunnen metadata, tags, categorieën, beschrijvingen, rechteninformatie, publicatie-informatie en andere kenmerken worden vastgelegd. Deze gegevens worden gebruikt om bestanden vindbaar, beheerbaar en bruikbaar te maken.

Persoonsgegevens van afgebeelde personen

Afhankelijk van het gebruik door de klant kunnen persoonsgegevens van afgebeelde personen worden verwerkt, zoals:

- naam;
- e-mailadres;
- telefoonnummer;
- adresgegevens;
- toestemmingsinformatie;
- publicatievoorkeuren;
- gekoppelde beelden of mediabestanden;
- eventuele opmerkingen of context die de klant zelf toevoegt.

De klant bepaalt welke gegevens van afgebeelde personen worden vastgelegd en is verantwoordelijk voor de rechtmatigheid daarvan.

Gebruikersgegevens

Voor toegang tot de applicatie verwerkt Beeldbank gegevens van gebruikers, zoals naam, e-mailadres, rol, rechten, organisatie en eventueel loggegevens over gebruik van de applicatie. Deze gegevens zijn nodig voor authenticatie, autorisatie, support, beveiliging en auditdoeleinden.

Technische gegevens en loggegevens

Beeldbank verwerkt technische gegevens die nodig zijn voor beveiliging, monitoring, foutopsporing, beschikbaarheid en ondersteuning. Denk aan systeemlogs, foutmeldingen, performancegegevens, sessiegegevens en beveiligingsmeldingen. Deze gegevens worden gebruikt om de dienst stabiel, veilig en betrouwbaar te houden.

Gegevens bij optionele AI-functionaliteiten

Wanneer de klant optionele functionaliteiten zoals automatische tagsuggesties, gezichtsdetectie of naamsuggesties inschakelt, kunnen aanvullende technische gegevens worden verwerkt. Dit kan bijvoorbeeld gaan om automatisch gegenereerde tags, gezichtsuitsneden en technische gezichtskenmerken.

Bij gezichtsdetectie wordt eerst met behulp van Google Vision AI vastgesteld of er een gezicht in een afbeelding aanwezig is en waar dit gezicht zich in de afbeelding bevindt. Google Vision AI koppelt hierbij zelf geen naam of identiteit aan het gezicht.

Wanneer de functionaliteit voor naamsuggesties is ingeschakeld, kan het gedetecteerde gezicht vervolgens worden verwerkt door een door Beeldbank beheerde, self-hosted en stateless microservice. Deze microservice zet het gezicht om naar een technische vector, ook wel embedding genoemd. Deze vector is een wiskundige representatie van kenmerken van het gezicht en wordt gebruikt om gezichten binnen dezelfde Beeldbank-omgeving met elkaar te vergelijken.

De vector wordt opgeslagen in de database van de betreffende klantomgeving en kan worden vergeleken met andere vectoren die al aan een persoon zijn gekoppeld. Op basis van deze





vergelijking en clusteranalyse kan Beeldbank een naamsuggestie tonen. Deze suggestie wordt niet automatisch definitief toegepast, maar vereist beoordeling of bevestiging door een gebruiker.

Omdat deze vectoren kunnen worden gebruikt om personen binnen de klantomgeving te herkennen of te koppelen, behandelt Beeldbank deze gegevens als gevoelige persoonsgegevens en past daarop passende beveiligings- en privacymaatregelen toe.

Doeleinden van de verwerking

Beeldbank verwerkt deze gegevens voor de volgende doeleinden:

- het leveren van de Beeldbank-dienst;
- het opslaan, beheren, zoeken, delen en publiceren van beeld- en mediabestanden;
- het beheren van gebruikers, rollen en autorisaties;
- het ondersteunen van rechtenbeheer, toestemmingen en publicatie-informatie;
- het ondersteunen van zoekfunctionaliteiten, tagging en filtering;
- het leveren van optionele AI-functionaliteiten, voor zover door de klant ingeschakeld;
- het uitvoeren van technisch beheer, support en onderhoud;
- het beveiligen van de applicatie en klantdata;
- het maken en beheren van back-ups;
- het monitoren van beschikbaarheid, capaciteit en prestaties;
- het afhandelen van incidenten, fouten en beveiligingsmeldingen;
- het voldoen aan contractuele en wettelijke verplichtingen.

Beeldbank verwerkt persoonsgegevens niet voor eigen commerciële doeleinden en verwerkt klantdata niet buiten de afgesproken doelen van de dienstverlening, tenzij daarvoor een afzonderlijke grondslag of toestemming bestaat.

2.3 Samenwerking met subverwerkers

Beeldbank maakt gebruik van zorgvuldig geselecteerde subverwerkers en leveranciers om de Beeldbank-dienst veilig, betrouwbaar en schaalbaar te kunnen leveren. Deze partijen ondersteunen onder meer bij hosting, opslag, back-ups, monitoring, technische ondersteuning, beveiliging en optionele beeldanalyse.

Subverwerkers worden alleen ingezet wanneer dit noodzakelijk is voor de uitvoering van de dienstverlening en wanneer passende contractuele, technische en organisatorische maatregelen zijn getroffen. Beeldbank blijft verantwoordelijk voor een zorgvuldige selectie, beoordeling en beheersing van deze partijen.

De belangrijkste subverwerkers, hun rol binnen de dienstverlening, de verwerkingslocaties en de wijze waarop Beeldbank deze leveranciers beoordeelt en beheerst, worden toegelicht in hoofdstuk 7.

2.4 Waarborging van beveiliging en privacy

Beeldbank neemt passende technische en organisatorische maatregelen om klantdata, persoonsgegevens en de beschikbaarheid van de dienst te beschermen. Deze maatregelen zijn afgestemd op de aard van de gegevens, de risico's van de verwerking, de afspraken met klanten en de uitgangspunten van ISO 27001:2022.





Beeldbank richt haar dienstverlening zo in dat persoonsgegevens en klantdata zoveel mogelijk binnen Nederland en de Europese Economische Ruimte worden verwerkt. Verwerking buiten de Europese Economische Ruimte vindt alleen plaats wanneer dit volgens de AVG is toegestaan én, voor zover vereist op grond van de verwerkersovereenkomst, na uitdrukkelijke schriftelijke toestemming van de verwerkingsverantwoordelijke. Voor leveranciers en subverwerkers worden afspraken gemaakt over de locatie van verwerking, beveiligingsmaatregelen, geheimhouding, incidentmelding, continuïteit en verwijdering van gegevens na beëindiging van de dienstverlening.

De beveiliging van Beeldbank is gebaseerd op meerdere lagen. Daarbij kan worden gedacht aan toegangsbeheer, rollen en rechten, versleuteling van gegevens tijdens transport en opslag, monitoring, logging, back-ups, patch- en updatebeheer, leveranciersbeheer en procedures voor incidenten en datalekken.

Beeldbank werkt volgens de principes van privacy by design en security by design. Dit betekent dat privacy en beveiliging worden meegenomen bij ontwerp, ontwikkeling, beheer en doorontwikkeling van de dienst. Nieuwe of gewijzigde functionaliteiten worden beoordeeld op privacy- en beveiligingsrisico's voordat zij worden toegepast.

Het ISMS van Beeldbank is ISO 27001:2022 gecertificeerd. Maatregelen worden periodiek beoordeeld en waar nodig verbeterd op basis van risico's, incidenten, interne en externe audits, technische ontwikkelingen, klantvragen en wijzigingen in wet- en regelgeving.





3. Beveiligingsmaatregelen

Beeldbank neemt passende technische en organisatorische maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van de Beeldbank-dienst en klantdata te beschermen. Deze maatregelen zijn afgestemd op de aard van de dienstverlening, de gevoeligheid van de gegevens, de risico's van de verwerking, de afspraken met klanten en de uitgangspunten van ISO 27001:2022.

De beveiliging van Beeldbank is opgebouwd uit meerdere lagen. Daarbij wordt niet vertrouwd op één enkele maatregel, maar op een combinatie van toegangsbeheer, versleuteling, monitoring, logging, back-ups, veilige softwareontwikkeling, leveranciersbeheer, incidentafhandeling en continue verbetering.

3.1 Technische beveiliging

Beeldbank past technische beveiligingsmaatregelen toe om ongeautoriseerde toegang, verlies, wijziging of misbruik van klantdata te voorkomen. Deze maatregelen hebben betrekking op de applicatie, infrastructuur, opslag, netwerkverbindingen, beheeromgevingen en ondersteunende systemen.

Toegangsbeheer en autorisatie

Toegang tot Beeldbank en de onderliggende systemen wordt beperkt tot bevoegde gebruikers, medewerkers en leveranciers die deze toegang nodig hebben voor hun rol. Hierbij wordt gewerkt volgens het least privilege-principe: gebruikers en beheerders krijgen alleen toegang tot de gegevens en functionaliteiten die noodzakelijk zijn voor hun werkzaamheden.

Binnen de Beeldbank-applicatie kunnen klanten zelf gebruikers, rollen en rechten beheren. Hierdoor kan de licentienemer bepalen welke gebruikers toegang hebben tot welke bestanden, mappen, collecties, metadata, downloadopties, publicatiemogelijkheden en beheerfuncties.

Voor toegang tot persoonsgegevens en beheersystemen gelden aanvullende beperkingen. Toegang wordt waar nodig gelogd, periodiek beoordeeld en aangepast wanneer rollen wijzigen of toegang niet langer noodzakelijk is.

Authenticatie en veilige toegang

Beeldbank ondersteunt veilige toegang tot de applicatie via persoonlijke gebruikersaccounts. Afhankelijk van de inrichting van de klantomgeving kunnen aanvullende authenticatiemaatregelen worden toegepast, zoals tweefactorauthenticatie of Single Sign-On.

Gebruikers zijn zelf verantwoordelijk voor zorgvuldig gebruik van hun account, wachtwoord en eventuele authenticatiemiddelen. Beeldbank treft passende maatregelen om authenticatie veilig in te richten en verwacht van licentienemers dat zij gebruikersaccounts en toegangsrechten binnen de eigen organisatie zorgvuldig beheren.

Versleuteling

Beeldbank past versleuteling toe om gegevens te beschermen tijdens transport en, waar passend, bij opslag. Gegevens die tussen gebruikers, de applicatie en onderliggende systemen worden uitgewisseld, worden via beveiligde verbindingen verwerkt.





Voor opslag en infrastructuur maakt Beeldbank gebruik van beveiligingsmaatregelen van professionele cloud- en hostingproviders, waaronder encryptie, toegangsbeperking en infrastructuurbeveiliging. Waar lokale apparatuur of werkplekken worden gebruikt, gelden aanvullende maatregelen zoals beveiligde toegang tot apparaten en het gebruik van standaard beveiligingsvoorzieningen van het besturingssysteem.

Logging en monitoring

Beeldbank gebruikt logging en monitoring om de werking, beschikbaarheid, capaciteit en beveiliging van de dienst te bewaken. Loggegevens en gebruiksinformatie kunnen worden verwerkt voor beveiliging, monitoring, capaciteitsbeheer, foutanalyse en optimalisatie van de dienst.

Monitoring wordt onder meer gebruikt om storingen, capaciteitsproblemen, foutmeldingen en mogelijke beveiligingssignalen tijdig te signaleren. Verdachte activiteiten of afwijkingen worden beoordeeld en, wanneer nodig, opgevolgd volgens het incidentmanagementproces.

Capaciteitsbeheer

Beeldbank bewaakt de capaciteit van de dienst om beschikbaarheid en continuïteit te ondersteunen. Daarbij wordt onder meer gekeken naar processorbelasting, geheugen, schijfruimte, beschikbaarheid en andere technische indicatoren.

Bij overschrijding van ingestelde drempelwaarden kunnen meldingen worden gegenereerd, zodat tijdig kan worden beoordeeld of aanvullende capaciteit, technisch onderzoek of een verbetermaatregel nodig is. Capaciteitsbeheer helpt om verstoringen te voorkomen en ondersteunt de betrouwbare werking van de dienst.

Patch- en updatebeheer

Beeldbank beoordeelt en verwerkt beveiligingsupdates en software-updates op basis van risico en impact. Updates voor systemen, frameworks, afhankelijkheden en infrastructuur worden toegepast om bekende kwetsbaarheden te verhelpen en de stabiliteit van de dienst te verbeteren.

Kritieke kwetsbaarheden krijgen prioriteit en worden binnen 72 uur verholpen. Waar nodig worden tijdelijke mitigerende maatregelen genomen totdat een structurele oplossing is doorgevoerd.

Kwetsbaarhedenbeheer

Beeldbank volgt kwetsbaarheden in gebruikte software, libraries, frameworks en infrastructuurcomponenten. Afhankelijkheden worden periodiek gecontroleerd en waar nodig bijgewerkt. Beveiligingsadviezen, dependency scanning en meldingen van leveranciers worden gebruikt om risico's tijdig te signaleren.

Wanneer een kwetsbaarheid relevant is voor Beeldbank, wordt beoordeeld wat de mogelijke impact is op klantdata, beschikbaarheid en beveiliging. Op basis daarvan worden passende maatregelen getroffen.

3.2 Veilige softwareontwikkeling en wijzigingsbeheer

Beeldbank hanteert het principe van security by design en privacy by design. Dit betekent dat beveiliging en privacy vanaf het ontwerp worden meegenomen bij nieuwe functionaliteiten, wijzigingen en technische verbeteringen.





Ontwikkelproces

Bij de ontwikkeling van software worden beveiligingsprincipes toegepast, waaronder:

- validatie van invoer;
- voorkomen van kwetsbaarheden zoals injection en ongeautoriseerde toegang;
- gebruik van actuele en onderhouden libraries en frameworks;
- geen opslag van wachtwoorden, API-sleutels of andere secrets in broncode;
- beoordeling van wijzigingen voordat deze naar productie gaan.

OTAP-structuur

Beeldbank werkt met een gescheiden ontwikkel-, test-, acceptatie- en productieproces. Wijzigingen worden eerst getest in een niet-productieomgeving voordat zij in productie worden doorgevoerd. Dit verkleint het risico dat fouten, kwetsbaarheden of ongewenste wijzigingen direct impact hebben op de live-omgeving.

Broncodebeheer

De broncode van Beeldbank wordt beheerd in een afgeschermd Git-repository via Bitbucket Cloud. De repositories zijn niet openbaar toegankelijk en toegang is beperkt tot bevoegde ontwikkelaars die aan de dienst werken.

Voor broncodebeheer geldt dat toegangsbeperking en versiebeheer zijn ingericht. Toegang tot de repositories is beveiligd met multi-factor-authenticatie. MFA is contractueel verplicht voor beheertoegang en broncoderepositories (artikel 7.2 van de overeenkomst met de ontwikkelpartner). In de repositories staat geen klantdata.

3.3 Organisatorische beveiliging

Naast technische maatregelen neemt Beeldbank organisatorische maatregelen om veilig en zorgvuldig met informatie om te gaan.

Beleid en verantwoordelijkheden

Beeldbank hanteert informatiebeveiligingsbeleid waarin de belangrijkste beveiligingsprocessen zijn vastgelegd. Dit beleid omvat onder meer toegangsbeheer, het risico gebaseerd toepassen van multi-factor-authenticatie, patch- en updatebeheer, incidentmanagement, back-up en herstel, leveranciersbeheer en periodieke evaluatie van beveiligingsmaatregelen.

Binnen Beeldbank zijn verantwoordelijkheden belegd voor informatiebeveiliging, privacy, leveranciersbeheer, incidentafhandeling en opvolging van verbetermaatregelen. De directie van Beeldbank vervult de rol van Security Officer en is het eerste aanspreekpunt voor informatiebeveiliging en privacy, bereikbaar via privacy@beeldbank.nl. Het beleid wordt minimaal jaarlijks beoordeeld en waar nodig aangepast op basis van risico's, incidenten, klantvragen, technische ontwikkelingen of wijzigingen in wet- en regelgeving.

Vertrouwelijkheid

Personen die toegang hebben tot vertrouwelijke informatie, klantdata of persoonsgegevens zijn gehouden aan geheimhouding. Dit geldt voor medewerkers en, waar van toepassing, voor leveranciers of andere partijen die in opdracht van Beeldbank werkzaamheden uitvoeren.

Toegang tot klantdata wordt alleen verleend wanneer dit noodzakelijk is voor beheer, support, beveiliging, foutoplossing of uitvoering van de dienstverlening.



Leveranciersbeheer

Beeldbank maakt gebruik van leveranciers en subverwerkers voor onder meer hosting, opslag, monitoring, ondersteuning en aanvullende functionaliteiten. Leveranciers worden beoordeeld op hun rol, beveiligingsmaatregelen, verwerkingslocatie, contractuele afspraken, certificeringen, continuïteit en eventuele verwerking van persoonsgegevens.

Wanneer een leverancier persoonsgegevens verwerkt namens Beeldbank, worden passende verwerkersafspraken gemaakt. Leveranciers die geen klantpersoonsgegevens verwerken maar wel relevant zijn voor beveiliging, ontwikkeling of continuïteit, worden meegenomen in het leveranciersbeheer.

Bewustwording en veilig werken

Beeldbank stimuleert veilig werken door duidelijke afspraken over toegang, gebruik van systemen, omgang met klantdata, beveiligingsincidenten en vertrouwelijke informatie. Medewerkers en betrokken leveranciers worden geacht zorgvuldig om te gaan met systemen, accounts, apparaten en gegevens.

Bij locatie-onafhankelijk werken worden aanvullende maatregelen toegepast, zoals veilige toegang tot systemen, beveiligde apparaten en beperking van toegang tot informatie op basis van noodzaak.

3.4 Back-up en herstel

Beeldbank maakt back-ups om herstel mogelijk te maken bij technische fouten, incidenten, verstoringen of calamiteiten. Back-ups zijn bedoeld voor continuïteit en herstel van de dienstverlening en vormen geen vervanging voor de eigen bewaarplicht of exportverantwoordelijkheid van de licentienemer.

Databaseback-ups worden dagelijks gemaakt en opgeslagen in object storage binnen de AMS3-regio. Deze back-ups blijven gedurende 30 dagen beschikbaar. Waar mogelijk kunnen back-ups per klantomgeving worden teruggezet.

Back-ups worden uitsluitend gebruikt voor hersteldoeleinden. Toegang tot back-ups is beperkt tot bevoegde personen en systemen. Verwijderde gegevens kunnen nog tijdelijk aanwezig zijn in back-ups totdat de back-upcyclus is doorlopen. Dit sluit aan op het verwijder- en bewaarbeleid dat verder wordt toegelicht in hoofdstuk 4.

Beeldbank beoordeelt haar back-up- en herstelmaatregelen periodiek. Het terugzetten van een back-up wordt jaarlijks in de praktijk getest. De laatste praktijktest was op 15 juni 2026: de volledige database van een klantomgeving is vanaf de nachtelijke back-up teruggezet in ongeveer vijf minuten. Het continuïteitsplan is op 4 augustus 2026 getest met een ransomwarescenario en op basis daarvan aangepast.

3.5 Bescherming tegen dreigingen

Beeldbank neemt maatregelen om de dienst te beschermen tegen technische dreigingen, misbruik, ongeautoriseerde toegang, malware, kwetsbaarheden en verstoringen.

Deze maatregelen omvatten onder meer:

- beveiligde verbindingen;





- toegangsbeperking op basis van rollen en noodzaak;
- monitoring van beschikbaarheid en afwijkend gedrag;
- patch- en updatebeheer;
- controle op kwetsbaarheden in afhankelijkheden;
- veilige ontwikkelprincipes;
- scheiding tussen ontwikkel-, test-, acceptatie- en productieomgevingen;
- logging en opvolging van incidenten;
- leveranciersbeoordeling;
- back-ups en herstelmogelijkheden.

Beeldbank kan niet garanderen dat de dienst altijd volledig foutloos, zonder onderbreking of volledig vrij van risico's functioneert. Wel treft Beeldbank passende maatregelen om risico's te beperken, incidenten tijdig te signaleren en de impact van verstoringen zoveel mogelijk te beperken.

3.6 Incidentmanagement en opvolging

Beeldbank hanteert een proces voor het signaleren, beoordelen, registreren en opvolgen van beveiligingsincidenten. Incidenten en vermoedens van incidenten worden gemeld via privacy@beeldbank.nl en beoordeeld door de Security Officer. Incidenten worden beoordeeld op aard, oorzaak, impact, getroffen gegevens, betrokken systemen en benodigde maatregelen.

Wanneer een incident mogelijk leidt tot een datalek, wordt beoordeeld of persoonsgegevens betrokken zijn en of de klant moet worden geïnformeerd. Beeldbank informeert klanten zonder onnodige vertraging en ondersteunt hen waar nodig bij het beoordelen van meldplicht richting toezichthouder of betrokkenen.

Na afhandeling van een incident wordt beoordeeld of aanvullende structurele maatregelen nodig zijn. Denk aan technische aanpassingen, procesverbeteringen, extra monitoring, aanpassing van documentatie of aanvullende bewustwording.

3.7 Continue verbetering binnen het ISO 27001-gecertificeerde ISMS

Beeldbank beoordeelt de maatregelen in dit hoofdstuk periodiek en scherpt ze aan op basis van risicoanalyses, incidenten, interne en externe audits, klantvragen, technische ontwikkelingen en wijzigingen in wet- en regelgeving. Het verbeterregister in het ISMS legt vast welke punten open staan en wanneer ze zijn afgerond.

De verbeterpunten voor de komende periode komen uit de certificeringsaudit van augustus 2026:

- een unieke identifier per risico, voor de traceerbaarheid in het ISMS;
- hersteltijd en aanvaardbaar dataverlies opnemen in de overeenkomsten met klanten;
- in het beleid vastleggen hoe de controle op toegangsrechten, rollen en autorisaties wordt uitgevoerd.

Met deze aanpak werkt Beeldbank aantoonbaar aan continue verbetering van beveiliging, privacybescherming en betrouwbaarheid van de dienstverlening.





4. Privacy en verwerking van persoonsgegevens

Beeldbank verwerkt persoonsgegevens zorgvuldig en in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG, de verwerkersovereenkomst en de afspraken met de licentienemer. Binnen de dienstverlening treedt de licentienemer in de meeste gevallen op als verwerkingsverantwoordelijke en Beeldbank als verwerker. Dit betekent dat de licentienemer bepaalt voor welke doelen persoonsgegevens worden verwerkt en dat Beeldbank deze gegevens verwerkt volgens de instructies van de licentienemer.

Beeldbank verwerkt persoonsgegevens uitsluitend voor zover dit nodig is voor het leveren, beveiligen, beheren en ondersteunen van de Beeldbank-dienst. De dienstverlening omvat onder meer opslag, beheer, zoeken en delen van beeld- en mediabestanden, gebruikersbeheer, veilige hosting, back-ups, technische ondersteuning en, indien door de klant ingeschakeld, automatische analyse zoals AI-tagging, gezichtsdetectie en naamsuggesties met menselijke bevestiging.

4.1 Verwerkingsdoelen en categorieën betrokkenen

Beeldbank verwerkt persoonsgegevens om licentienemers en hun gebruikers te ondersteunen bij het veilig beheren van beeld- en mediabestanden. De verwerking vindt plaats voor de volgende doelen:

- het opslaan en beheren van beeld- en mediabestanden;
- het organiseren, zoeken, filteren en terugvinden van bestanden;
- het beheren van metadata, tags, toestemmingen en publicatierechten;
- het beheren van gebruikersaccounts, rollen en autorisaties;
- het delen van bestanden met interne en externe partijen;
- het leveren van technische ondersteuning en klantenservice;
- het beveiligen, monitoren en verbeteren van de dienst;
- het maken en beheren van back-ups;
- het aanbieden van optionele functionaliteiten zoals AI-tagging, gezichtsdetectie en naamsuggesties.

Binnen Beeldbank kunnen persoonsgegevens worden verwerkt van onder meer:

- afgebeelde personen;
- gebruikers van de Beeldbank-applicatie;
- contactpersonen van de licentienemer;
- externe ontvangers of personen met wie bestanden worden gedeeld;
- personen van wie gegevens voorkomen in metadata, toestemmingsformulieren of gekoppelde documentatie.

Afhankelijk van het gebruik door de licentienemer kunnen onder meer de volgende persoonsgegevens worden verwerkt:

- beeld- en mediabestanden waarop personen herkenbaar zijn;
- naam, adres, telefoonnummer en e-mailadres van afgebeelde personen;
- toestemmingsinformatie en publicatievoorkeuren;
- metadata, tags, beschrijvingen en rechteninformatie;
- naam en e-mailadres van gebruikers;



- rollen, rechten en accountgegevens;
- technische loggegevens en gebruiksinformatie;
- biometrische sjablonen of gezichts-embeddings, uitsluitend indien de betreffende functionaliteit is ingeschakeld.

De verwerkersovereenkomst noemt onder meer visuele gegevens, contactgegevens van afgebeelde personen, gebruikersgegevens en biometrische sjablonen in de vorm van pseudonieme vectorrepresentaties voor naamsuggesties met menselijke bevestiging.

4.2 Rolverdeling en verantwoordelijkheden

De licentienemer is verantwoordelijk voor de rechtmatigheid van de persoonsgegevens en content die binnen Beeldbank worden opgeslagen, beheerd, gedeeld of gepubliceerd. Dit betekent dat de licentienemer zelf moet beoordelen of er een geldige grondslag bestaat voor het verwerken van persoonsgegevens, of de juiste informatie aan betrokkenen is verstrekt en of benodigde toestemmingen, gebruiksrechten of publicatierechten aanwezig zijn.

Beeldbank is als verwerker verantwoordelijk voor het verwerken van persoonsgegevens volgens de instructies van de licentienemer en voor het treffen van passende technische en organisatorische beveiligingsmaatregelen. In de algemene voorwaarden is vastgelegd dat de licentienemer verantwoordelijk blijft voor de rechtmatigheid van de verwerking, de inhoud van opgeslagen gegevens, het informeren van betrokkenen en het beoordelen of het gebruik van de dienst geschikt is voor het beoogde doel.

Beeldbank ondersteunt de licentienemer door functionaliteiten aan te bieden voor onder meer gebruikersbeheer, rechtenbeheer, toestemmingsregistratie, veilig delen, logging, verwijdering en export. Deze functionaliteiten helpen de licentienemer om privacyverplichtingen praktisch uit te voeren, maar nemen de verantwoordelijkheid van de licentienemer niet over.

4.3 Toegangsbeheer en beveiliging van persoonsgegevens

Beeldbank beperkt toegang tot persoonsgegevens tot bevoegde personen en systemen die deze toegang nodig hebben voor de uitvoering van hun rol. Binnen de applicatie kunnen licentienemers zelf gebruikers, rollen en rechten beheren. Hierdoor kan per gebruiker worden bepaald welke bestanden, mappen, metadata, downloadopties, publicatiemogelijkheden en beheerfuncties beschikbaar zijn.

Beeldbank past passende technische en organisatorische maatregelen toe om persoonsgegevens en klantdata te beschermen. Deze maatregelen zijn afgestemd op de aard van de verwerking, de stand van de techniek en de risico's. Denk hierbij aan toegangscontrole, versleuteling, logging, monitoring, back-ups, leveranciersbeheer en procedures voor incidenten en datalekken. De algemene voorwaarden bepalen ook dat Beeldbank passende maatregelen treft voor back-up en herstel en dat loggegevens en gebruiksinformatie mogen worden verwerkt voor beveiliging, monitoring, capaciteitsbeheer, foutanalyse en optimalisatie van de dienst.

Persoonsgegevens worden niet breder toegankelijk gemaakt dan noodzakelijk. Wanneer leveranciers of subverwerkers worden ingezet, worden passende afspraken gemaakt over beveiliging, vertrouwelijkheid, verwerkingslocatie, incidentmelding en verwijdering.





4.4 Bewaartermijnen en verwijderingsbeleid

Beeldbank bewaart persoonsgegevens niet langer dan noodzakelijk voor de uitvoering van de dienstverlening, de afspraken met de licentienemer en de toepasselijke wettelijke verplichtingen. De licentienemer bepaalt in beginsel zelf welke bestanden, metadata en persoonsgegevens binnen de eigen Beeldbank-omgeving worden opgenomen en hoe lang deze nodig zijn voor het eigen doel.

Voor de verwerking binnen Beeldbank gelden de volgende uitgangspunten:

Gegevenscategorie	Bewaartermijn / verwijdering
Klantdata en inhoud binnen Beeldbank	Tijdens de looptijd van de overeenkomst. Na beëindiging van de overeenkomst worden gegevens binnen één maand verwijderd.
Beeld- en mediabestanden	Zolang de licentienemer deze binnen de omgeving bewaart of totdat de overeenkomst eindigt.
Metadata en toestemmingsinformatie	Zolang gekoppeld aan bestanden of personen binnen de klantomgeving, tenzij eerder verwijderd op verzoek van de licentienemer.
Gebruikersgegevens	Zolang het gebruikersaccount nodig is voor toegang tot de dienst of totdat de licentienemer het account verwijderd.
Ongekoppelde embeddings / “onbekende gezichten”	Blijven bestaan zolang de bijbehorende ongekoppelde gezichten in de klantomgeving staan. Worden de gezichten verwijderd, dan verdwijnen de embeddings via de back-upcyclus mee.
Gekoppelde embeddings	Zolang het bijbehorende beeld bestaat; direct verwijderen zodra het beeld wordt verwijderd.
Back-ups	Verwijderde embeddings verdwijnen uit back-ups binnen 30 dagen. Databaseback-ups blijven 30 dagen beschikbaar.
Logs	Circa 180 dagen, voor beveiliging, monitoring en foutanalyse. Alleen toegankelijk voor bevoegde beheerders.

Voor de leesbaarheid wordt onderscheid gemaakt tussen databaseback-ups en serverback-ups. Databaseback-ups worden dagelijks gemaakt en blijven maximaal 30 dagen beschikbaar. Productieserverback-ups worden uitsluitend gebruikt voor hersteldoeleinden en kennen een kortere technische bewaartermijn. Verwijderde gegevens kunnen tijdelijk nog in back-ups aanwezig zijn totdat de betreffende back-upcyclus is doorlopen.



De verwerkersovereenkomst noemt onder meer dat klantinhoud tot één maand na afloop van het contract wordt verwerkt, dat gekoppelde embeddings de bewaartermijn van het bijbehorende beeld volgen en dat verwijderde embeddings binnen 30 dagen uit back-ups verdwijnen.

4.5 Verwerking door subverwerkers

Beeldbank maakt gebruik van subverwerkers voor onderdelen van de dienstverlening, zoals hosting, opslag en optionele beeldanalyse. Subverwerkers worden alleen ingezet wanneer dit noodzakelijk is voor de dienstverlening en wanneer passende contractuele en beveiligingsafspraken zijn gemaakt.

De belangrijkste subverwerkers voor persoonsgegevens zijn:

Subverwerker	Soort verwerking	Locatie
Google Vision	Analyse, gezichtsdetectie en automatische labels/tagsuggesties; alleen actief indien de functie is ingeschakeld	EU-regio, uitsluitend EER
Google Cloud Storage	Opslag en beheer van visuele gegevens en persoonsgegevens	Nederland
DigitalOcean	Hosting en opslag van gegevens	Nederland

Beeldbank verwerkt klantdata en persoonsgegevens binnen Nederland en/of de Europese Economische Ruimte. De primaire hosting, opslag, back-upvoorzieningen en verwerking door de belangrijkste subverwerkers zijn ingericht binnen de EER.

Deze subverwerkers zijn opgenomen in de verwerkersovereenkomst. Daarin staat ook dat Google Vision alleen wordt gebruikt voor analyse, gezichtsdetectie en automatische labels wanneer de functie is ingeschakeld, dat Google Cloud Storage wordt gebruikt voor opslag en beheer van gegevens in Nederland en dat DigitalOcean wordt gebruikt voor hosting en opslag in Nederland.

4.6 Meldplicht datalekken en beveiligingsincidenten

Beeldbank hanteert een proces voor het signaleren, beoordelen, registreren en opvolgen van beveiligingsincidenten en mogelijke datalekken. Wanneer sprake is van een vermoedelijke of vastgestelde inbreuk in verband met persoonsgegevens, informeert Beeldbank de verwerkingsverantwoordelijke zonder onredelijke vertraging en uiterlijk binnen 24 uur na vaststelling van de inbreuk.

Voor zover bekend verstrekt Beeldbank daarbij informatie over de vermoedelijke oorzaak, de categorieën persoonsgegevens, de categorieën betrokkenen, het aantal betrokkenen en de genomen of voorgestelde maatregelen. De technisch beheerder van het platform is contractueel verplicht een incident binnen 12 uur aan Beeldbank te melden, zodat de termijn van 24 uur





richting de klant haalbaar blijft. Beeldbank neemt zonder onredelijke vertraging maatregelen om de inbreuk te herstellen, de gevolgen te beperken en verdere inbreuken te voorkomen.

De licentienemer beslist als verwerkingsverantwoordelijke of een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens en/of aan betrokkenen. Beeldbank ondersteunt de licentienemer waar nodig bij deze beoordeling en melding. Beeldbank houdt een logboek bij van inbreuken en de genomen maatregelen; de licentienemer kan dit inzien wanneer daarom wordt gevraagd.

4.7 Rechten van betrokkenen

Betrokkenen hebben op grond van de AVG verschillende rechten, waaronder het recht op inzage, rectificatie, verwijdering, beperking van verwerking, overdraagbaarheid, bezwaar en, waar verwerking is gebaseerd op toestemming, intrekking van toestemming.

Omdat de licentienemer meestal verwerkingsverantwoordelijke is voor persoonsgegevens binnen de eigen Beeldbank-omgeving, worden verzoeken van betrokkenen in beginsel door de licentienemer beoordeeld en beantwoord. Beeldbank ondersteunt de licentienemer bij het uitvoeren van deze verzoeken, voor zover dat binnen de dienstverlening en de technische mogelijkheden nodig is.

Wanneer een verzoek betrekking heeft op gegevens die Beeldbank zelf als verwerkingsverantwoordelijke verwerkt, bijvoorbeeld in het kader van eigen contactgegevens, administratie of communicatie, behandelt Beeldbank het verzoek zelf volgens de privacyverklaring en toepasselijke privacywetgeving.

4.8 Gezichtsdetectie, embeddings en naamsuggesties

Beeldbank biedt optionele functionaliteiten voor gezichtsdetectie en naamsuggesties. Deze functionaliteiten zijn alleen actief wanneer zij in de klantomgeving zijn ingeschakeld. Als de functionaliteit niet is ingeschakeld, worden er voor die klantomgeving geen gezichts-embeddings aangemaakt en geen naamsuggesties gedaan.

De werking bestaat uit de volgende stappen.

Stap 1: gezichtsdetectie met Google Vision AI

Eerst wordt met behulp van Google Vision AI vastgesteld of er een gezicht in een afbeelding aanwezig is en waar dit gezicht zich bevindt. Google Vision AI koppelt hierbij zelf geen naam of identiteit aan het gezicht. De functie wordt gebruikt voor detectie en analyse, niet voor het zelfstandig identificeren van personen.

Stap 2: omzetting naar een technische vector

Wanneer naamsuggesties zijn ingeschakeld, kan het gedetecteerde gezicht worden doorgestuurd naar een door Beeldbank beheerde, self-hosted en stateless microservice. Deze microservice zet het gezicht om naar een technische vector, ook wel embedding genoemd.

De microservice is stateless. Dit betekent dat de microservice het gezicht niet zelfstandig opslaat nadat de verwerking is uitgevoerd.

Stap 3: opslag binnen de klantomgeving





De gegenereerde vector wordt opgeslagen in de database van de betreffende klantomgeving. De vector wordt alleen gebruikt binnen die klantomgeving. Er vindt geen vergelijking plaats met gegevens van andere klanten.

Stap 4: vergelijking en clusteranalyse

De vector wordt vergeleken met andere vectoren in dezelfde klantomgeving die al aan een persoon zijn gekoppeld. Met behulp van vergelijking en clusteranalyse wordt bepaald welke persoon het beste bij het gedetecteerde gezicht lijkt te passen.

Stap 5: menselijke bevestiging

De uitkomst van de analyse wordt gebruikt om een mogelijke naamsuggestie te tonen. Deze suggestie wordt niet automatisch definitief toegepast. Een gebruiker moet de suggestie beoordelen of bevestigen. Daarmee blijft menselijke controle onderdeel van het proces.

Stap 6: opt-out en verwijdering

Op verzoek van de licentienemer of betrokkene kunnen gekoppelde embeddings worden verwijderd en kunnen toekomstige suggesties voor die persoon worden geblokkeerd. Wanneer de functionaliteit wordt uitgeschakeld, worden geen nieuwe embeddings aangemaakt. Bestaande embeddings kunnen op verzoek worden verwijderd. Na beëindiging van het contract worden alle data, inclusief embeddings, binnen één maand verwijderd en verdwijnen verwijderde embeddings binnen 30 dagen uit back-ups.

Belangrijke waarborgen

Voor gezichtsdetectie en naamsuggesties gelden de volgende waarborgen:

- de functionaliteit is optioneel per klantomgeving;
- Google Vision AI koppelt zelf geen naam of identiteit aan gezichten;
- naamsuggesties vereisen menselijke beoordeling of bevestiging;
- embeddings worden gebruikt binnen dezelfde klantomgeving;
- er vindt geen cross-tenant matching plaats;
- bij uitschakeling worden geen nieuwe embeddings aangemaakt;
- bestaande embeddings kunnen op verzoek worden verwijderd;
- klantdata, gezichten en embeddings worden niet gebruikt voor algemene AI-modeltraining, tenzij daarvoor vooraf uitdrukkelijke toestemming is gegeven.

De verwerkersovereenkomst bevestigt dat naamsuggesties optioneel zijn, dat bij uitschakeling geen nieuwe embeddings worden aangemaakt, dat bestaande embeddings op verzoek worden verwijderd en dat data en back-ups logisch gescheiden zijn per klantomgeving.

4.9 Back-ups en herstel

Beeldbank maakt back-ups om de continuïteit van de dienstverlening te ondersteunen en herstel mogelijk te maken bij technische fouten, incidenten of calamiteiten. Databaseback-ups worden dagelijks gemaakt en opgeslagen in object storage binnen de AMS3-regio. Deze back-ups blijven 30 dagen beschikbaar. Daarnaast worden er dagelijks back-ups gemaakt van de productieserver, die 7 dagen worden bewaard.





Het beeldmateriaal van klanten staat in Google Cloud Storage en valt buiten deze databaseback-up. Daar is bewust geen aparte back-up van: de bescherming bestaat uit de duurzaamheid van de dienst zelf, waarvoor Google 99,999999999 procent hanteert. Verwijderd beeldmateriaal wordt pas na 7 dagen definitief verwijderd en is binnen die termijn terug te halen. Beeldmateriaal dat niet is verwijderd blijft onbeperkt beschikbaar.

Back-ups worden uitsluitend gebruikt voor hersteldoeleinden. Toegang tot back-ups is beperkt tot bevoegde personen en systemen. Verwijderde gegevens kunnen nog tijdelijk aanwezig zijn in back-ups totdat de back-upcyclus is doorlopen. Voor verwijderde embeddings geldt dat deze binnen 30 dagen uit back-ups verdwijnen.

Wanneer een herstelactie nodig is, wordt beoordeeld welke klantomgeving, gegevenscategorie en herstelperiode relevant is. Herstel vindt plaats met inachtneming van vertrouwelijkheid, integriteit en tenant-isolatie.

4.10 Privacy by design en dataminimalisatie

Beeldbank werkt volgens de uitgangspunten van privacy by design en privacy by default. Dit betekent dat privacybescherming wordt meegenomen bij ontwerp, ontwikkeling, beheer en doorontwikkeling van de dienst.

- alleen gegevens verwerken die nodig zijn voor het doel;
- optionele functionaliteiten, zoals naamsuggesties, per klantomgeving inrichten;
- geen nieuwe embeddings aanmaken wanneer de functie is uitgeschakeld;
- klantomgevingen logisch scheiden;
- toegangsrechten beperken tot noodzakelijke rollen;
- passende beveiligingsmaatregelen toepassen;
- verwerkingen documenteren in de verwerkersovereenkomst;
- klanten ondersteunen bij DPIA's wanneer technische input nodig is.

De verwerkersovereenkomst vermeldt expliciet privacy by design & default, dataminimalisatie, optionele naamsuggesties, tenant-isolatie en ondersteuning bij klant-DPIA's als onderdeel van de privacy- en beveiligingsmaatregelen.

4.11 Samenvatting

Beeldbank verwerkt persoonsgegevens alleen voor zover dit nodig is voor de dienstverlening en volgens de afspraken met de licentienemer. De licentienemer blijft verantwoordelijk voor de rechtmatigheid van de gegevens en content binnen de eigen omgeving. Beeldbank zorgt voor passende technische en organisatorische beveiligingsmaatregelen, duidelijke afspraken met subverwerkers, ondersteuning bij rechten van betrokkenen, een datalekproces, bewaartermijnen, back-ups en privacywaarborgen rond optionele AI-functionaliteiten.

Met deze aanpak ondersteunt Beeldbank haar klanten bij een veilige, controleerbare en AVG-conforme inzet van de Beeldbank-dienst.





5. Digitale toegankelijkheid

Digitale toegankelijkheid betekent dat digitale diensten zo worden ontworpen en ingericht dat zij door zoveel mogelijk gebruikers goed te gebruiken zijn. Dit gaat niet alleen over mensen met een beperking, maar ook over duidelijke schermen, begrijpelijke navigatie, voorspelbare functies en het voorkomen van onnodige drempels bij het werken met informatie.

Voor Beeldbank is toegankelijkheid belangrijk omdat gebruikers veilig en zorgvuldig moeten kunnen omgaan met beeldmateriaal, persoonsgegevens, toestemmingen, publicatierechten en deelmogelijkheden. Een begrijpelijke en goed bruikbare applicatie verkleint de kans op fouten, zoals het onbedoeld delen van bestanden, het verkeerd toepassen van rechten of het missen van relevante toestemmingsinformatie.

5.1 Context en richtlijnen

Beeldbank is een gespecialiseerde SaaS-applicatie voor het beheren, zoeken, delen en publiceren van beeld- en mediabestanden. De applicatie wordt gebruikt door verschillende typen gebruikers, zoals communicatie-, marketing-, HR-, archief-, voorlichtings- en contentteams.

Bij het ontwerp en de doorontwikkeling van Beeldbank wordt rekening gehouden met gebruiksvriendelijkheid, begrijpelijke bediening en veilige standaardinstellingen. Waar passend worden algemeen aanvaarde toegankelijkheidsrichtlijnen, zoals de WCAG-richtlijnen, als inspiratie en toetsingskader gebruikt.

Beeldbank ondersteunt klanten bij het zorgvuldig beheren en delen van beeldmateriaal. Daarbij ligt de nadruk op:

- duidelijke navigatie;
- begrijpelijke schermen en acties;
- herkenbare knoppen en meldingen;
- duidelijke rechten- en toestemmingsinformatie;
- controle voordat bestanden worden gedeeld of gepubliceerd;
- veilige standaardinstellingen;
- het beperken van onbedoelde fouten door gebruikers.

Voor overheidsorganisaties of andere organisaties die zelf onder specifieke toegankelijkheidsverplichtingen vallen, blijft de klant verantwoordelijk voor de beoordeling hoe de eigen inzet van Beeldbank past binnen de voor haar geldende verplichtingen. Beeldbank kan daarbij ondersteunen met informatie over de werking en inrichting van de applicatie.

5.2 Gebruiksvriendelijkheid en toegankelijkheid binnen Beeldbank

Beeldbank streeft naar een applicatie die overzichtelijk, begrijpelijk en consistent werkt. Dit is belangrijk omdat gebruikers vaak werken met grote hoeveelheden bestanden, metadata, toestemmingen en publicatiekanalen.

Binnen de applicatie wordt onder meer aandacht besteed aan:

- logische opbouw van menu's en schermen;
- duidelijke zoek- en filtermogelijkheden;





- herkenbare acties voor uploaden, downloaden, delen en publiceren;
- waarschuwingen of signalen wanneer rechten of toestemmingen relevant zijn;
- inzichtelijke rollen en autorisaties;
- duidelijke weergave van metadata en publicatie-informatie;
- consistente vormgeving van knoppen, meldingen en formulieren;
- ondersteuning van efficiënt beheer van grote hoeveelheden beeldmateriaal.

Deze maatregelen dragen niet alleen bij aan toegankelijkheid, maar ook aan privacy en beveiliging. Wanneer gebruikers goed begrijpen welke acties zij uitvoeren, is de kans kleiner dat persoonsgegevens of beeldmateriaal onbedoeld verkeerd worden gedeeld of gepubliceerd.

5.3 Toegankelijkheid, privacy en veilige standaardinstellingen

Digitale toegankelijkheid hangt binnen Beeldbank samen met privacy by design en security by design. Een veilige applicatie moet niet alleen technisch goed zijn beveiligd, maar ook begrijpelijk zijn voor de gebruikers die ermee werken.

- inzicht in wie toegang heeft tot bestanden;
- duidelijke rechten- en toestemmingsinformatie bij beeldmateriaal;
- beheer van publicatierechten en vervaldata;
- controle over download- en deelmogelijkheden;
- waarschuwingen of beperkingen wanneer beeldmateriaal niet zomaar gebruikt mag worden;
- rollen en rechten waarmee toegang kan worden beperkt;
- duidelijke beheerfuncties voor het aanpassen of verwijderen van gegevens.

Deze aanpak helpt klanten om zorgvuldig om te gaan met persoonsgegevens, portretrechtelijke belangen en interne publicatieregels.

5.4 Beperkingen en afhankelijkheden

De toegankelijkheid en begrijpelijkheid van het gebruik kunnen mede afhankelijk zijn van:

- de inrichting van de klantomgeving;
- de gekozen rollen en rechten;
- de kwaliteit en volledigheid van metadata;
- de wijze waarop klanten toestemmingsinformatie vastleggen;
- de gebruikte bestandsnamen, omschrijvingen en tags;
- interne werkafspraken en instructies van de klant;
- het apparaat, de browser en de instellingen van de gebruiker.

5.5 Doorontwikkeling en verbetering

Beeldbank blijft de toegankelijkheid en gebruiksvriendelijkheid van de applicatie doorontwikkelen. Verbeteringen kunnen voortkomen uit klantvragen, gebruikerservaringen, supportmeldingen, technische ontwikkelingen, wijzigingen in wet- en regelgeving en interne beoordelingen.

Wanneer toegankelijkheids- of gebruiksvriendelijkheidsverbeteringen worden doorgevoerd, worden deze waar relevant meegenomen in het reguliere ontwikkel- en wijzigingsproces. Daarbij wordt ook gekeken naar mogelijke impact op privacy, beveiliging en beheerbaarheid.





Beeldbank ziet digitale toegankelijkheid daarom niet als een eenmalige toets, maar als onderdeel van continue verbetering van de dienstverlening.





6. Compliance en risico's

Beeldbank werkt aan een gestructureerde aanpak voor compliance, informatiebeveiliging en risicobeheersing. Daarbij worden wettelijke verplichtingen, contractuele afspraken met klanten en de uitgangspunten van ISO 27001:2022 samengebracht in beleid, processen, technische maatregelen en periodieke beoordeling.

Het doel hiervan is om risico's voor klantdata, persoonsgegevens, beschikbaarheid en continuïteit aantoonbaar te beheersen. Beeldbank gebruikt hierbij het principe van continue verbetering. Dat betekent dat risico's, maatregelen, incidenten, leveranciers en verbeterpunten periodiek worden beoordeeld en waar nodig worden aangepast.

6.1 Toetsing aan AVG, ISO 27001 en andere kaders

Beeldbank verwerkt persoonsgegevens in overeenstemming met de AVG, de Uitvoeringswet AVG, de verwerkersovereenkomst en de instructies van de licentienemer. De licentienemer is in de meeste gevallen verwerkingsverantwoordelijke en Beeldbank treedt op als verwerker.

Voor informatiebeveiliging gebruikt Beeldbank ISO 27001:2022 als belangrijkste normenkader. Beeldbank is ISO 27001:2022 gecertificeerd. Certificaatnummer NL 3108.1.1, afgegeven door Brand Compliance B.V., geaccrediteerd door de Raad voor Accreditatie. De certificeringsaudit vond plaats op 25 en 27 augustus 2026 en leverde geen afwijkingen op. Het certificaat is te valideren via IAF CertSearch (iafcertsearch.org). De volgende audit in de cyclus staat gepland voor augustus 2027.

De toetsing aan ISO 27001 richt zich onder meer op informatiebeveiligingsbeleid, risicobeoordeling, toegangsbeheer, leveranciersbeheer, logging en monitoring, incidentmanagement, back-up en herstel, continuïteit, veilige softwareontwikkeling, wijzigingsbeheer en periodieke evaluatie.

Naast ISO 27001 en AVG houdt Beeldbank rekening met relevante aanvullende kaders, zoals de NIS2-richtlijn, de EU AI Act voor optionele AI-functionaliteiten, contractuele verplichtingen, subverwerkersafspraken en, waar relevant, richtlijnen voor digitale toegankelijkheid.

Dit rapport is een toelichting op de maatregelen achter het certificaat en vervangt het certificaat niet. Het beschrijft hoe Beeldbank haar informatiebeveiliging en privacymaatregelen heeft ingericht en welke verbeterpunten uit de laatste audit worden opgevolgd.

6.2 Risicomanagement en BIV-classificatie

Beeldbank beoordeelt beveiligings- en privacyrisico's aan de hand van de mogelijke impact op beschikbaarheid, integriteit en vertrouwelijkheid. Deze drie aspecten worden ook wel de BIV-classificatie genoemd.

Risico's kunnen bijvoorbeeld ontstaan door technische kwetsbaarheden, menselijke fouten, onjuiste autorisaties, verstoringen bij leveranciers, datalekken, verlies van gegevens, foutieve publicatie van beeldmateriaal of onzorgvuldig gebruik van optionele AI-functionaliteiten.

Beeldbank beoordeelt risico's periodiek en neemt passende maatregelen om deze te beperken. Voorbeelden daarvan zijn toegangsbeheer, logging, monitoring, back-ups,





leveranciersbeoordelingen, beveiligingsupdates, incidentprocedures, scheiding van klantomgevingen en beperking van gegevensverwerking tot wat noodzakelijk is.

Alle risico's in het risicoregister van Beeldbank (44 risico's, stand september 2026) zijn gekoppeld aan beheersmaatregelen uit Annex A van ISO 27001:2022 en vastgelegd in de Verklaring van Toepasselijkheid.

6.3 Gegevensbeschermingseffectbeoordeling - DPIA

Een gegevensbeschermingseffectbeoordeling, ook wel DPIA genoemd, is een hulpmiddel om vooraf privacyrisico's van een verwerking te beoordelen. Een DPIA kan met name relevant zijn wanneer een klant Beeldbank gebruikt voor grootschalige verwerking van beeldmateriaal met herkenbare personen, gevoelige doelgroepen of optionele functionaliteiten zoals gezichtsdetectie en naamsuggesties.

De licentienemer is als verwerkingsverantwoordelijke verantwoordelijk voor de beoordeling of een DPIA nodig is en voor het uitvoeren daarvan. Beeldbank ondersteunt de licentienemer waar nodig met informatie over de werking van de dienst, de verwerkte gegevens, beveiligingsmaatregelen, subverwerkers, bewaartermijnen, back-ups en optionele AI-functionaliteiten.

Bij de beoordeling van gezichtsdetectie en naamsuggesties kan de licentienemer onder meer kijken naar het doel van de functionaliteit, de categorieën betrokkenen, het type beeldmateriaal, de grondslag voor verwerking, de proportionaliteit en noodzakelijkheid, de bewaartermijnen, de mogelijkheid tot opt-out of verwijdering, de technische werking van embeddings, de menselijke bevestiging bij naamsuggesties en de afwezigheid van cross-tenant matching.

Beeldbank adviseert klanten om optionele gezichtsfunctionaliteiten pas in te schakelen nadat intern is beoordeeld of het gebruik past binnen de eigen privacyverplichtingen, informatievoorziening aan betrokkenen en eventuele DPIA-verplichtingen.

6.4 Beheer van informatiebeveiligingsincidenten

Beeldbank hanteert een proces voor het signaleren, beoordelen, registreren en opvolgen van informatiebeveiligingsincidenten. Incidenten kunnen betrekking hebben op beschikbaarheid, integriteit of vertrouwelijkheid van de dienst of gegevens.

Bij een incident wordt beoordeeld wat er is gebeurd, welke systemen of gegevens betrokken zijn, of persoonsgegevens zijn geraakt, wat de mogelijke impact is voor klanten of betrokkenen en welke maatregelen nodig zijn om het incident te beheersen. Ook wordt beoordeeld of melding aan de klant noodzakelijk is en welke structurele verbeteringen nodig zijn om herhaling te voorkomen.

Beeldbank ondersteunt de licentienemer met de informatie die redelijkerwijs nodig is voor die beoordeling, zoals de aard van het incident, de categorieën gegevens, de mogelijke gevolgen en de genomen of voorgestelde maatregelen.

Na afhandeling van een incident beoordeelt Beeldbank of aanvullende verbetermaatregelen nodig zijn. Dit kan leiden tot technische aanpassingen, proceswijzigingen, extra monitoring, aanvullende instructies of aanpassing van beleid.





6.5 Continuïteitsplanning en beschikbaarheid

Beeldbank neemt maatregelen om de beschikbaarheid en continuïteit van de dienst te ondersteunen. Daarbij wordt onder meer gekeken naar hosting, monitoring, capaciteitsbeheer, back-ups, herstelmogelijkheden, leveranciersafhankelijkheden en incidentrespons.

De continuïteitsmaatregelen bestaan onder andere uit monitoring van beschikbaarheid en prestaties, capaciteitsbewaking, dagelijkse databaseback-ups, back-ups van de productieomgeving, herstelmogelijkheden per klantomgeving waar technisch mogelijk, leveranciersbeoordeling en opvolging van kritieke kwetsbaarheden.

In het continuïteitsplan van Beeldbank gelden de volgende interne normen:

- maximale onbeschikbaarheid van het platform bij een urgente storing: 8 uur tijdens kantooruren;
- maximale onbeschikbaarheid bij een calamiteit met herstel uit back-up: 24 uur;
- maximaal aanvaardbaar dataverlies: 24 uur.

Het continuïteitsplan wordt minimaal één keer per jaar getest aan de hand van een realistisch scenario. De laatste test was op 4 augustus 2026 (ransomwarescenario); het terugzetten van een back-up is op 15 juni 2026 in de praktijk getest. Beide tests zijn vastgelegd en hebben geleid tot aanpassingen in het plan. Daarmee is aantoonbaar dat herstelmaatregelen niet alleen bestaan, maar ook werken.

6.6 Exitstrategie en beëindiging van de dienstverlening

Een duidelijke exitprocedure is belangrijk om te zorgen dat klantdata na beëindiging van de dienstverlening zorgvuldig wordt teruggeleverd of verwijderd. Beeldbank neemt exit en gegevensverwijdering daarom mee in haar contractuele afspraken en interne beheerprocessen.

Na beëindiging van de overeenkomst kan de licentienemer gegevens exporteren of laten overdragen, voor zover dit binnen de dienstverlening en technische mogelijkheden is afgesproken. Na afloop van de overeengekomen termijn worden klantdata en persoonsgegevens verwijderd volgens de afspraken in de verwerkersovereenkomst.

In de praktijk betekent dit dat klantdata beschikbaar blijft gedurende de looptijd van de overeenkomst. Na beëindiging wordt een redelijke termijn geboden voor export of overdracht, indien dat is afgesproken. Daarna worden klantdata en persoonsgegevens verwijderd volgens de contractuele afspraken. Verwijderde gegevens kunnen nog tijdelijk aanwezig zijn in back-ups totdat de back-upcyclus is doorlopen. Back-ups worden niet gebruikt voor regulier gebruik, maar uitsluitend voor hersteldoeleinden.

6.7 Samenwerking met leveranciers en subverwerkers

Beeldbank maakt gebruik van leveranciers en subverwerkers voor onderdelen van de dienstverlening, zoals hosting, opslag, monitoring, support, broncodebeheer en optionele beeldanalyse. Deze partijen worden beoordeeld en beheerst binnen het leveranciersbeheer van Beeldbank.

Bij de beoordeling van leveranciers kijkt Beeldbank naar de aard van de dienstverlening, het soort gegevens dat wordt verwerkt, de locatie van verwerking, beveiligingsmaatregelen,





certificeringen en assurance-rapportages, contractuele afspraken, geheimhouding, doorgifte buiten de Europese Economische Ruimte, continuïteit, exitmogelijkheden en incidentmelding.

Subverwerkers die persoonsgegevens verwerken namens Beeldbank worden opgenomen in de verwerkersafspraken. Beeldbank informeert klanten over relevante subverwerkers en wijzigingen daarin volgens de afspraken in de verwerkersovereenkomst.

Leveranciers die geen klantpersoonsgegevens verwerken, maar wel relevant zijn voor beveiliging, ontwikkeling of continuïteit van de dienst, worden eveneens beoordeeld. Denk bijvoorbeeld aan leveranciers voor broncodebeheer, monitoring of projectmanagement.

6.8 AI-functionaliteiten en compliance

Beeldbank biedt optionele AI-functionaliteiten, zoals automatische tagsuggesties, gezichtsdetectie en naamsuggesties. Deze functionaliteiten worden alleen toegepast wanneer zij in de klantomgeving zijn ingeschakeld.

Bij het gebruik van AI-functionaliteiten houdt Beeldbank rekening met privacy, transparantie, dataminimalisatie, beveiliging en menselijke controle. Google Vision AI wordt gebruikt voor detectie en analyse, maar koppelt zelf geen namen of identiteit aan gezichten. Eventuele naamsuggesties worden binnen Beeldbank gegenereerd op basis van technische vectors of embeddings en vereisen menselijke beoordeling of bevestiging door een gebruiker.

Beeldbank gebruikt klantdata, gezichten en embeddings niet voor algemene AI-modeltraining, tenzij de klant daarvoor vooraf uitdrukkelijk toestemming heeft gegeven.

De licentienemer blijft verantwoordelijk voor de beoordeling of het gebruik van AI-functionaliteiten past binnen de eigen doelen, grondslag, informatieplicht en eventuele DPIA-verplichtingen. Beeldbank ondersteunt de licentienemer met technische en organisatorische informatie over de werking en beveiliging van deze functionaliteiten.

6.9 Audits, beoordelingen en verbetermaatregelen

Het ISMS van Beeldbank wordt jaarlijks intern geaudit (laatste interne audit 26 mei 2026, alle vijftien bevindingen verwerkt) en extern door Brand Compliance (certificeringsaudit 25 en 27 augustus 2026, geen afwijkingen). Daarbij worden maatregelen periodiek beoordeeld en waar nodig verbeterd.

Deze aanpak bestaat uit periodieke beoordeling van risico's, actualisatie van beleid en procedures, leveranciersbeoordelingen, opvolging van verbetermaatregelen, evaluatie van beveiligingsincidenten, beoordeling van back-up en herstel, toegangsreviews, actualisatie van subverwerkersinformatie en toetsing aan relevante ISO 27001-controls.

Verbeterpunten worden vastgelegd in het verbeterregister en opgevolgd. De verbeterpunten uit de certificeringsaudit van augustus 2026 zijn: een unieke identifier per risico, hersteltijd en aanvaardbaar dataverlies opnemen in de overeenkomsten met klanten, en in het beleid vastleggen hoe de controle op toegangsrechten, rollen en autorisaties wordt uitgevoerd.





6.10 Samenvatting

Beeldbank beheerst compliance- en beveiligingsrisico's door een combinatie van beleid, technische maatregelen, contractuele afspraken, leveranciersbeheer, incidentmanagement, back-ups, exitafspraken en continue verbetering.

De AVG vormt het belangrijkste juridische kader voor persoonsgegevens. ISO 27001:2022 vormt het belangrijkste normenkader voor informatiebeveiliging. Beeldbank is ISO 27001:2022 gecertificeerd en gebruikt het ISMS om maatregelen te structureren, aantoonbaar te maken en waar nodig te verbeteren.

Met deze aanpak ondersteunt Beeldbank klanten bij een veilige, controleerbare en privacybewuste inzet van de Beeldbank-dienst.





7. Gebruik van subverwerkers

Beeldbank maakt gebruik van subverwerkers en ondersteunende leveranciers om de Beeldbank-dienst veilig, betrouwbaar en schaalbaar te kunnen leveren. Deze partijen ondersteunen onder meer bij hosting, opslag, back-ups, monitoring, technische ondersteuning, beveiliging, softwareontwikkeling en optionele beeldanalyse.

Subverwerkers en leveranciers worden alleen ingezet wanneer dit noodzakelijk is voor de werking, beveiliging, ondersteuning of doorontwikkeling van de dienst. Beeldbank blijft verantwoordelijk voor een zorgvuldige selectie, beoordeling en beheersing van deze partijen. Daarbij kijkt Beeldbank niet alleen naar certificeringen, maar ook naar de aard van de dienstverlening, het soort gegevens dat wordt verwerkt, de locatie van verwerking, contractuele afspraken, beveiligingsmaatregelen, continuïteit, exitmogelijkheden en de mate waarin de leverancier past binnen de privacy- en beveiligingseisen van Beeldbank.

Voor leveranciers die namens Beeldbank persoonsgegevens verwerken, worden passende contractuele afspraken gemaakt. Daarin wordt onder meer vastgelegd voor welk doel gegevens mogen worden verwerkt, welke beveiligingsmaatregelen gelden, hoe wordt omgegaan met geheimhouding, waar gegevens worden verwerkt, hoe incidenten worden gemeld en wat er met gegevens gebeurt na beëindiging van de dienstverlening.

Beeldbank beoordeelt leveranciers en subverwerkers periodiek opnieuw. Daarbij wordt gekeken of de leverancier nog voldoet aan de gestelde beveiligings- en privacy-eisen en of wijzigingen in de dienstverlening, wetgeving of risico's aanleiding geven tot aanvullende maatregelen.

7.1 Leveranciersbeoordeling en beheersing

Beeldbank beoordeelt subverwerkers en relevante leveranciers voorafgaand aan inzet en gedurende de samenwerking. Deze beoordeling is onderdeel van het leveranciersbeheer en sluit aan op de uitgangspunten van AVG en ISO 27001:2022.

Bij deze beoordeling wordt gekeken naar de rol van de leverancier, de gegevens die worden verwerkt, de locatie waar gegevens worden verwerkt, de beveiligingsmaatregelen van de leverancier, de contractuele afspraken, de beschikbaarheid van certificeringen of assurance-rapportages en de gevolgen voor continuïteit, privacy en beveiliging.

Certificeringen en assurance-documentatie, zoals ISO 27001, SOC 2, SOC 3 of CSA STAR, worden door Beeldbank gebruikt als ondersteunend bewijs bij de leveranciersbeoordeling. Deze documentatie vervangt niet de eigen beoordeling door Beeldbank. Beeldbank blijft zelf beoordelen of de inzet van een leverancier passend is binnen de dienstverlening en de afspraken met klanten.

Waar nodig neemt Beeldbank aanvullende maatregelen. Dit kan bijvoorbeeld bestaan uit beperking van toegang, aanvullende contractuele afspraken, extra monitoring, versleuteling, logging, periodieke evaluatie of afspraken over exit en verwijdering.





7.2 DigitalOcean

DigitalOcean wordt gebruikt voor hosting en technische infrastructuur van onderdelen van de Beeldbank-dienst. De hosting vindt plaats binnen de Europese Economische Ruimte, op de AMS3-locatie in Amsterdam.

Binnen deze infrastructuur worden onder meer de applicatieserver, database, logbestanden en onderdelen van gedeelde bestanden verwerkt. Ook worden databaseback-ups opgeslagen in object storage binnen de AMS3-regio. Daarmee blijven deze onderdelen van de Beeldbank-dienst binnen Nederland en de Europese Economische Ruimte.

DigitalOcean beschikt over externe assurance en beveiligingsdocumentatie, waaronder SOC 2 Type II, SOC 3 en CSA STAR Level 1. Deze verklaringen geven aanvullende onderbouwing voor beveiligingsmaatregelen op het gebied van onder meer beveiliging, beschikbaarheid en vertrouwelijkheid.

Waar van toepassing betreft Beeldbank ook certificeringsdocumentatie van onderliggende datacenterfaciliteiten, zoals ISO/IEC 27001:2022-certificaten en Statements of Applicability, bij haar leveranciersbeoordeling. Deze documentatie ondersteunt de beoordeling van fysieke en facilitaire beveiligingsmaatregelen, zoals toegangscontrole, stroomvoorziening, netwerkbeschikbaarheid en omgevingsbeveiliging.

Beeldbank gebruikt de beschikbare certificeringen en assurance-documentatie als onderdeel van haar leveranciersbeoordeling. Daarnaast past Beeldbank eigen beheersmaatregelen toe, zoals toegangsbeperking, monitoring, beveiligingsupdates, back-ups, versleuteling en logisch gescheiden klantomgevingen.

7.3 Google Cloud Storage

Google Cloud Storage wordt gebruikt voor de opslag van door klanten geüploade beeld- en mediabestanden. Dit betreft de bestanden die klanten in Beeldbank plaatsen en beheren. Deze bestanden kunnen persoonsgegevens bevatten, bijvoorbeeld wanneer personen herkenbaar in beeld zijn of wanneer bestanden zijn gekoppeld aan metadata, toestemmingsinformatie of publicatierechten.

De opslag via Google Cloud Storage is ingericht binnen Nederland en Europa. In de verwerkersafspraken is Google Cloud Storage opgenomen voor opslag en beheer van gegevens in Nederland. Daarmee blijft de reguliere opslag van klantdata binnen de Europese Economische Ruimte.

Google Cloud Storage beschikt over uitgebreide beveiligingsmaatregelen, waaronder encryptie tijdens transport en opslag, toegangsbeheer, logging, monitoring en infrastructuurbeveiliging. Relevante certificeringen, zoals ISO 27001, ISO 27017 en ISO 27018, worden door Beeldbank gebruikt als aanvullende onderbouwing van de beveiligingsmaatregelen.

Beeldbank gebruikt Google Cloud Storage uitsluitend voor de werking van de Beeldbank-dienst: het veilig opslaan, beheren en beschikbaar maken van bestanden binnen de klantomgeving. Klantdata wordt niet gebruikt voor eigen commerciële doeleinden van Beeldbank of voor algemene AI-modeltraining, tenzij de klant daarvoor vooraf uitdrukkelijk toestemming heeft gegeven.





7.4 Google Vision API

Bij gezichtsdetectie wordt Google Vision API gebruikt om vast te stellen of er een gezicht in een afbeelding aanwezig is en waar dit gezicht zich bevindt. Google Vision API koppelt hierbij zelf geen naam of identiteit aan het gezicht en voert voor Beeldbank geen persoonsherkenning of matching met bekende personen uit.

Wanneer naamsuggesties zijn ingeschakeld, vindt de verdere verwerking binnen de Beeldbank-infrastructuur plaats. Het gedetecteerde gezicht kan dan worden verwerkt door een door Beeldbank beheerde, self-hosted en stateless microservice. Deze microservice zet het gezicht om naar een technische vector, ook wel embedding genoemd. Deze vector wordt binnen de klantomgeving gebruikt om gezichten te vergelijken met eerder gekoppelde gezichten en om een mogelijke naamsuggestie te doen.

7.5 Overige ondersteunende leveranciers

Naast hosting-, opslag- en AI-diensten maakt Beeldbank gebruik van ondersteunende leveranciers voor monitoring en foutopsporing (Sentry), meldingen (Slack), projectbeheer (Jira) en broncodebeheer (Bitbucket Cloud). Deze leveranciers verwerken geen klantpersoonsgegevens en krijgen alleen toegang tot gegevens voor zover dat noodzakelijk is voor hun rol. Broncode wordt beheerd in Bitbucket Cloud; hierin staat geen klantdata.

7.6 Verwerking binnen en buiten de Europese Economische Ruimte

Beeldbank verwerkt klantdata en persoonsgegevens binnen Nederland en/of de Europese Economische Ruimte. De primaire hosting, opslag, back-upvoorzieningen en verwerking door de belangrijkste subverwerkers zijn ingericht binnen de EER. Voor de belangrijkste verwerkingen binnen de Beeldbank-dienst worden Europese verwerkingslocaties gebruikt, waaronder Amsterdam/AMS3 voor DigitalOcean, Nederland voor Google Cloud Storage en de EU-regio voor Google Vision API.

Beeldbank verwerkt klantdata niet buiten de Europese Economische Ruimte. Indien dit in de toekomst wijzigt, gebeurt dit uitsluitend wanneer dit volgens de AVG is toegestaan én na uitdrukkelijke schriftelijke toestemming van de verwerkingsverantwoordelijke, voor zover die toestemming op grond van de verwerkersovereenkomst vereist is. In dat geval worden passende waarborgen getroffen, zoals een adequaatheidsbesluit, standaardcontractbepalingen en aanvullende technische en organisatorische maatregelen waar nodig.

7.7 Wijzigingen in subverwerkers

Beeldbank houdt bij welke subverwerkers worden ingezet voor de Beeldbank-dienst. Wanneer een nieuwe subverwerker wordt ingezet of een bestaande subverwerker wezenlijk wijzigt, informeert Beeldbank de licentienemer volgens de afspraken in de verwerkersovereenkomst.

Hierdoor houdt de licentienemer inzicht in de partijen die betrokken zijn bij de verwerking van persoonsgegevens. Eventuele bezwaren tegen een wijziging worden behandeld volgens de contractuele afspraken tussen Beeldbank en de licentienemer.



7.8 Exit en verwijdering bij subverwerkers

Bij beëindiging van de dienstverlening of bij het beëindigen van de inzet van een subverwerker wordt beoordeeld welke gegevens moeten worden teruggeleverd, verwijderd of veilig buiten gebruik gesteld. Beeldbank zorgt ervoor dat subverwerkers gegevens niet langer bewaren dan noodzakelijk voor het doel waarvoor zij zijn ingeschakeld, behoudens wettelijke verplichtingen of technische back-uptermijnen.

7.9 Samenvatting

Met leveranciers die persoonsgegevens verwerken namens Beeldbank worden passende afspraken gemaakt. Daarnaast beoordeelt Beeldbank leveranciers periodiek op beveiliging, privacy, continuïteit, verwerkingslocatie, contractuele afspraken en exitmogelijkheden.





8. Conclusie en aanbevelingen

Beeldbank heeft haar dienstverlening ingericht met aandacht voor privacy, informatiebeveiliging, continuïteit en zorgvuldig gebruik van beeld- en mediabestanden. De dienst ondersteunt organisaties bij het veilig opslaan, beheren, zoeken, delen en publiceren van beeldmateriaal, waarbij functionaliteiten zoals rollen en rechten, toestemmingsbeheer, metadata, back-ups en optionele AI-functionaliteiten helpen om grip te houden op persoonsgegevens en publicatierechten.

De belangrijkste uitgangspunten binnen Beeldbank zijn dat klantdata alleen wordt verwerkt voor de afgesproken dienstverlening, dat persoonsgegevens passend worden beveiligd, dat subverwerkers zorgvuldig worden beoordeeld en dat klanten ondersteuning krijgen bij hun eigen verantwoordelijkheden onder de AVG. Daarbij blijft de licentienemer verantwoordelijk voor de rechtmatigheid van de content en persoonsgegevens die binnen de eigen Beeldbank-omgeving worden geplaatst, terwijl Beeldbank verantwoordelijk is voor een veilige en betrouwbare verwerking volgens de gemaakte afspraken.

8.1 Samenvatting van maatregelen en compliance

Beeldbank past technische en organisatorische maatregelen toe om de vertrouwelijkheid, integriteit en beschikbaarheid van klantdata te beschermen. Deze maatregelen zijn afgestemd op de AVG, de verwerkersovereenkomst, contractuele afspraken met klanten en de uitgangspunten van ISO 27001:2022.

De beveiliging van de Beeldbank-dienst is opgebouwd uit meerdere lagen. Daarbij worden onder meer toegangsbeheer, rollen en rechten, versleuteling, monitoring, logging, back-ups, patch- en updatebeheer, leveranciersbeheer, incidentmanagement en veilige softwareontwikkeling toegepast. Ook wordt gewerkt met logische scheiding van klantomgevingen en met beveiligingsmaatregelen bij leveranciers en subverwerkers.

Voor privacybescherming werkt Beeldbank volgens de uitgangspunten van dataminimalisatie, privacy by design en privacy by default. Persoonsgegevens worden verwerkt voor duidelijke doelen en binnen de afspraken met de licentienemer. Optionele functionaliteiten zoals gezichtsdetectie, automatische tagsuggesties en naamsuggesties worden alleen toegepast wanneer zij in de klantomgeving zijn ingeschakeld. Bij naamsuggesties blijft menselijke beoordeling onderdeel van het proces.

Beeldbank is ISO 27001:2022 gecertificeerd (certificaat NL 3108.1.1, Brand Compliance B.V.). Dit rapport beschrijft de maatregelen achter dat certificaat en laat zien welke verbeterpunten uit de laatste audit worden opgevolgd.

8.2 Toekomstige verbeterpunten en planning

Beeldbank ziet informatiebeveiliging en privacybescherming als een continu proces. Wetgeving, technologie, klantbehoeften en dreigingen veranderen voortdurend. Daarom worden maatregelen periodiek beoordeeld en waar nodig verbeterd.

Het ISMS van Beeldbank wordt jaarlijks intern en extern geaudit. Verbeterpunten uit audits, incidenten en tests worden vastgelegd in het verbeterregister en opgevolgd.





Verbeterpunten voor de komende periode zijn:

- een unieke identifier per risico, voor de traceerbaarheid in het ISMS;
- hersteltijd en aanvaardbaar dataverlies opnemen in de overeenkomsten met klanten;
- in het beleid vastleggen hoe de controle op toegangsrechten, rollen en autorisaties wordt uitgevoerd;
- het periodiek evalueren van subverwerkers, verwerkingslocaties en certificeringsdocumentatie;
- het ondersteunen van klanten met informatie voor DPIA's bij gebruik van optionele AI-functionaliteiten;
- het blijven beoordelen van nieuwe wetgeving, zoals de EU AI Act en NIS2, voor zover relevant voor de dienstverlening.

Deze verbeterpunten laten zien dat Beeldbank informatiebeveiliging en privacy gestructureerd beheert en blijft verbeteren. Dit past bij de uitgangspunten van ISO 27001 en bij de verantwoordelijkheid die hoort bij het beheren van beeldmateriaal en persoonsgegevens voor klanten.

8.3 Eindconclusie

Op basis van de beschreven maatregelen biedt Beeldbank een veilige en controleerbare omgeving voor het beheren van beeld- en mediabestanden. De dienst ondersteunt klanten bij het zorgvuldig omgaan met persoonsgegevens, toestemmingen, publicatierechten en het veilig delen van bestanden.

Beeldbank heeft belangrijke privacy- en beveiligingsmaatregelen ingericht, waaronder toegangsbeheer, versleuteling, monitoring, back-ups, leveranciersbeheer, incidentmanagement, bewaartermijnen, exitafspraken en waarborgen rond optionele AI-functionaliteiten. Beeldbank houdt het ISMS aantoonbaar op orde via jaarlijkse interne en externe audits.

Daarmee biedt Beeldbank klanten niet alleen een praktisch platform voor beeldbeheer, maar ook een dienstverlening waarin privacy, beveiliging en continue verbetering structureel zijn verankerd.





9. Bijlagen en verwijzingen

Dit hoofdstuk bevat een overzicht van documenten en externe bronnen die kunnen worden gebruikt ter onderbouwing van de in dit rapport beschreven privacy- en beveiligingsmaatregelen. Het gaat om contractuele documenten van Beeldbank en openbare of opvraagbare documentatie van subverwerkers en leveranciers.

De genoemde documenten worden niet standaard integraal als bijlage toegevoegd. Waar mogelijk wordt verwezen naar de actuele online versie of naar een beveiligde link. Documenten die niet openbaar beschikbaar zijn, zoals bepaalde assurance-rapportages, kunnen op aanvraag of via het trustportaal van de betreffende leverancier beschikbaar zijn.

9.1 Contractuele documenten Beeldbank

De contractuele afspraken tussen Beeldbank en haar klanten vormen de basis voor de verwerking van persoonsgegevens, beveiliging, beheer, ondersteuning en beëindiging van de dienstverlening.

Tot deze documenten behoren onder meer de verwerkersovereenkomst, beheerovereenkomst, algemene voorwaarden en privacyverklaring van Beeldbank. In deze documenten zijn afspraken vastgelegd over de rolverdeling tussen licentienemer en Beeldbank, de doeleinden van verwerking, beveiligingsmaatregelen, subverwerkers, geheimhouding, rechten van betrokkenen, datalekken, bewaartermijnen, back-ups, exit en verwijdering van gegevens.

Deze documenten worden gebruikt als juridische en organisatorische onderbouwing van de maatregelen die in dit rapport zijn beschreven. Waar mogelijk worden de actuele versies als bijlage toegevoegd of via een beveiligde link beschikbaar gesteld.

Document	Relevantie	Beschikbaarheid
Verwerkersovereenkomst Beeldbank	Afspraken over verwerking, beveiliging, subverwerkers en bewaartermijnen.	Zie voorbeeld
Beheerovereenkomst Beeldbank	Afspraken over beheer, support, monitoring, exit en datalekken.	Zie voorbeeld
Algemene voorwaarden Beeldbank	Afspraken over gebruik, verantwoordelijkheid en aansprakelijkheid.	Publiek beschikbaar
Privacyverklaring Beeldbank	Informatie over eigen verwerkingen door Beeldbank.	Publiek beschikbaar



9.2 Subverwerkers en externe bewijsdocumentatie

Subverwerker / leverancier	Documentatie	Relevantie	Beschikbaarheid
Beeldbank B.V.	ISO/IEC 27001:2022-certificaat NL 3108.1.1 (Brand Compliance B.V., RvA-geaccrediteerd)	Certificering van het ISMS van Beeldbank.	Zie certificaat
DigitalOcean	SOC 2 Type II	Onafhankelijke assurance over onder meer beveiliging, beschikbaarheid en vertrouwelijkheid.	Trustportal / op aanvraag
DigitalOcean	SOC 3	Publieke assurance-rapportage over beheersmaatregelen van DigitalOcean.	Trustportal / op aanvraag
DigitalOcean	CSA STAR Level 1 / CAIQ	Cloud security self-assessment op basis van het Cloud Controls Matrix-raamwerk.	Publieke link
Equinix AMS (datacenter achter DigitalOcean AMS3)	ISO/IEC 27001 (AMS-sites), SOC 2 Type II	Onderbouwing van fysieke beveiliging, toegangscontrole, stroomvoorziening, koeling en continuïteit.	Via het klantportaal van Equinix / op aanvraag
Google Cloud	ISO/IEC 27001	Certificering voor informatiebeveiliging.	Publieke link
Google Cloud	ISO/IEC 27017	Normenkader en certificering voor cloud security.	Publieke link
Google Cloud	ISO/IEC 27018	Normenkader en certificering voor bescherming van persoonsgegevens in publieke cloudomgevingen.	Publieke link
Google Cloud	Google Cloud Data Processing and Security Terms	Contractuele voorwaarden over verwerking, beveiliging	Publieke link



Subverwerker / leverancier	Documentatie	Relevantie	Beschikbaarheid
		en gegevensbescherming.	
Google Cloud	Google Cloud Subprocessors	Overzicht van subprocessors die Google kan inzetten voor Google Cloud Platform-diensten.	Publieke link
Google Vision API	Cloud Vision API Data Usage-documentatie	Uitleg over gebruik van ingestuurde content, waaronder dat Google content niet gebruikt om Cloud Vision-modellen te trainen of te verbeteren.	Publieke link

9.3 Beschikbaarheid en actualisatie

Dit rapport wordt minimaal jaarlijks herzien, na elke externe audit en bij wezenlijke wijzigingen in de dienstverlening of de subverwerkers. De actuele versie is v8, september 2026. Eerdere versies worden vervangen; klanten die een oudere versie hebben ontvangen, kunnen de actuele versie opvragen via privacy@beeldbank.nl.

9.4 Samenvatting

De bijlagen en verwijzingen bij dit rapport bestaan uit contractuele documenten van Beeldbank en relevante externe bewijsdocumentatie van subverwerkers en leveranciers. Daarmee blijft het rapport overzichtelijk voor klanten, terwijl wel inzicht wordt gegeven in de belangrijkste juridische afspraken, beveiligingswaarborgen, certificeringen en assurance-documentatie.

Interne beleidsdocumenten, risicoanalyses, ISO 27001-control mappings en verbeterregisters maken onderdeel uit van het interne managementsysteem van Beeldbank en worden niet standaard als bijlage bij dit rapport gedeeld.