

Informatiebeveiligingsbeleid het Noord-Hollands Archief

maart 2018

Versie 0.98

Classificatie: Vertrouwelijk intern

# Documentbeheer

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Versie | Datum | Auteur | Review | Status |
| 0.1 | 1-11-2017 | Jeroen Wittink, Roomyla Choenni | Initiële versie | gereviewed |
| 0.2 | 8-11-2017 | Jeroen Wittink | Besproken met Roomyla Choenni, Ed Sewalt en Maarten Brock:   * Inhoudsopgave * Doelstellingen * Governance | gereviewed |
| 0.5 | 31-01- 2018 | Jeroen Wittink | Ingevuld informatiebeveiligingsbeleid.  Besproken met Roomyla Choenni, Ed Sewalt en Maarten Brock. | gereviewed |
| 0.8 | 12-02-2018 | Jeroen Wittink, Roomyla Choenni | * Normenkaders toegevoegd * Aanpassingen rollen | gereviewed |
| 0.9 | 28-02- 2018 | Roomyla Choenni | * ISMS verwerkt | gerewiewed |
|  | 6-03-2018 | Roomyla Choenni | * Verder aanvullen | gereviewed |
| 1.0 | 13-03-2018 |  | Vaststellen in het IM overleg |  |
|  |  |  |  |  |
|  |  |  |  |  |

Inhoudsopgave

[Documentbeheer 2](#_Toc508182722)

[1. Doelstelling 5](#_Toc508182723)

[1.1 Reikwijdte beleid 5](#_Toc508182724)

[1.2 Doelstelling beleid 6](#_Toc508182725)

[2. Beleidsprincipes informatiebeveiliging 7](#_Toc508182726)

[2.1 Beleidsuitgangspunten 7](#_Toc508182727)

[2.2 PDCA-cyclus informatiebeveiliging 8](#_Toc508182728)

[2.3 Classificatie 9](#_Toc508182729)

[3. Normenkaders 11](#_Toc508182730)

[3.1 Wettelijke voorschriften 11](#_Toc508182731)

[3.2 Overige richtlijnen en landelijke afspraken 11](#_Toc508182732)

[3.3 Normenkaders voor externe leveranciers 12](#_Toc508182733)

[4. Governance informatiebeveiligingsbeleid 13](#_Toc508182734)

[4.1 Integrale veiligheid 13](#_Toc508182735)

[4.2 Inpassing in de organisatiegovernance 13](#_Toc508182736)

[4.3 Controle, naleving en sancties 14](#_Toc508182737)

[4.4 Rollen informatiebeveiliging 15](#_Toc508182738)

[4.5 Overleg 16](#_Toc508182739)

[4.6 Bewustwording informatiebeveiliging 16](#_Toc508182740)

[5. Melding en afhandeling incidenten 17](#_Toc508182741)

[5.1 Incidentmanagement 17](#_Toc508182742)

[5.2 Melden datalekken 17](#_Toc508182743)

[Bijlagen Informatiebeveiligingsbeleid 18](#_Toc508182744)

[Bijlage 1: Register art. 30 AVG met verwerkingen persoonsgegevens 18](#_Toc508182745)

[Bijlage 2: Privacyverklaring 18](#_Toc508182746)

[Bijlage 3: Bewerkersovereenkomst 18](#_Toc508182747)

[Bijlage 1: Register art. 30 AVG met verwerkingen persoonsgegevens 19](#_Toc508182748)

[Bijlage 2: Privacyverklaring 22](#_Toc508182749)

[Bijlage 3: Bewerkersovereenkomst 25](#_Toc508182750)

# 1. Doelstelling

Het Noord-Hollands Archief kiest voor de volgende definitie van informatiebeveiliging:

het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten *beschikbaarheid*, *integriteit* en *vertrouwelijkheid* van de informatievoorziening te garanderen.

De verschillende kwaliteitsaspecten worden als volgt uitgelegd:

* *Beschikbaarheid*: de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor de juiste gebruikers;
* *Integriteit*: de mate waarin gegevens of functionaliteit juist gedefinieerd en ingevuld zijn;
* *Vertrouwelijkheid*: de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

Naast de drie bovengenoemde aspecten onderkent het Noord-Hollands Archief een vierde aspect:

* *Controleerbaarheid*: de mogelijkheid om met voldoende zekerheid vast te kunnen stellen of wordt voldaan aan de eisen ten aanzien van *beschikbaarheid*, *integriteit* en *vertrouwelijkheid*.

Informatiebeveiliging is een beleidsverantwoordelijkheid van het management van het Noord-Hollands Archief. De informatiemanager is verantwoordelijk voor het opstellen van het beleid met betrekking tot informatiebeveiliging. Zij adviseert het management op dit gebied.

Het Noord-Hollands archief heeft de ambitie om met het dit beleidsdocument informatiebeveiliging structureel naar een hoger niveau te brengen en daar op te houden. Dit wordt gedaan door de verschillende onderdelen van het beleid (*governance*, wet- en regelgeving, de organisatie van de beveiligingsfunctie en de uitgangspunten van het informatiebeveiligingsbeleid) duidelijk te beschrijven. De nadruk ligt ook op de onderliggende relatie tussen de verschillende aspecten.

Het beleid wordt vastgesteld door het management van het Noord-Hollands Archief. Het beleid dient als strategisch document bij het nemen van beslissingen op het gebied van informatiebeveiliging en privacy, of bij vraagstukken die een dergelijke component hebben.

## 1.1 Reikwijdte beleid

Het Noord-Hollands Archief kiest voor een brede interpretatie van informatiebeveiliging. Er wordt niet alleen gekeken naar informatietechnologie, maar ook naar aanpalende en gedeeltelijk overlappende beleidsterreinen zoals fysieke beveiliging, juridische zaken, *privacy*, *business continuity* en sociale veiligheid.

Het Noord-Hollands Archief kiest voor een integrale aanpak van informatieveiligheid. Op strategisch niveau pakt het Noord-Hollands Archief informatiebeveiliging planmatig op. Ook wordt er binnen de organisatie gezocht naar inhoudelijke afstemming met de verschillende raakvlakken.

Het informatiebeveiligingsbeleid binnen het Noord-Hollands Archief heeft betrekking op alle medewerkers, gasten, bezoekers en externe relaties (inhuur / outsourcing). Het beleid heeft betrekking op alle organisatieonderdelen. Tevens vallen onder het informatiebeveiligingsbeleid alle *devices* waarmee geautoriseerde toegang tot het organisatienetwerk kan worden verkregen.

Bij het informatiebeveiligingsbeleid ligt de nadruk op die toepassingen en collecties, die vallen onder de verantwoordelijkheid van het Noord-Hollands Archief. Dit heeft zowel betrekking op (1) gecontroleerde informatie, die door de organisatie zelf is gegenereerd en wordt beheerd, als ook op (2) niet-gecontroleerde informatie waarop het Noord-Hollands Archief kan worden aangesproken, zoals uitspraken van medewerkers in discussies en op persoonlijke pagina’s. Onder de reikwijdte van dit beleid vallen ook websites en andere uitingen die op enige manier verbonden zijn met het Noord-Hollands Archief, bijvoorbeeld op sociale media.

Het Noord-Hollands Archief heeft collecties in het beheer van externe partijen. In dat geval bepaalt de externe partij de eisen die gesteld worden aan het archief. Echter, ook deze collecties vallen onder de reikwijdte van dit beleid.

## 1.2 Doelstelling beleid

Het informatiebeveiligingsbeleid bij het Noord-Hollands Archief heeft een tweeledig doel, namelijk

1. Het waarborgen van de continuïteit van de bedrijfsvoering en het minimaliseren van schade door het voorkomen van beveiligingsincidenten
2. Het minimaliseren van eventuele gevolgen van beveiligingsincidenten.

Dit beleid draagt bij aan de realisering van de algehele doelstellingen die het Noord-Hollands Archief voor zichzelf heeft geformuleerd, namelijk:

1. Partner zijn voor overheden: borgen van de duurzame toegankelijkheid en betrouwbaarheid van hun archieven;
2. Beschikbaar zijn voor het publiek: informatiecentrum zijn voor de geschiedenis van Noord-Holland en gemeenten in Kennemerland en Amstel- en Meerlanden.

Vanzelfsprekend heeft het Noord-Hollands Archief als doel om te voldoen aan relevante wet- en regelgeving op het gebied van informatieveiligheid en privacy. Daarnaast kent het informatieveiligheidsbeleid van het Noord-Hollands Archief de volgende doelstellingen:

* Voldoen aan de wettelijke taken met betrekking tot archief
* Veiligheid klantgegevens garanderen;
* Veilige omgeving bieden voor bezoekers, klanten en medewerkers;
* Bijdragen aan veiligheid en privacy binnen de sector;
* Waarborgen van de continuïteit van de organisatie en het primaire proces;

# 2. Beleidsprincipes informatiebeveiliging

Het Noord-Hollands Archief werkt vanuit een aantal beleidsprincipes en uitgangspunten. Deze vormen de onderliggende basis voor de strategie die gevolgd wordt, om te voldoen aan de doelstellingen, zoals geformuleerd in hoofdstuk 2 van dit beleid.

## 2.1 Beleidsuitgangspunten

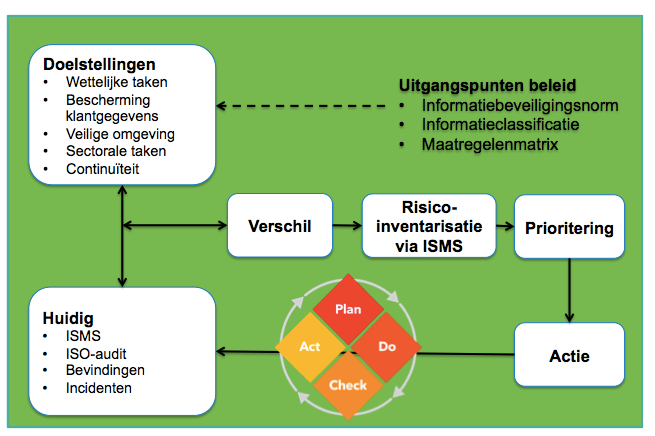
Het Noord-Hollands archief hanteert de volgende beleidsprincipes:

* De kern van het beleid is dat het Noord-Hollands Archief streeft naar **een balans** tussen veiligheid en werkbaarheid. De waarde van de informatie bepaalt de maatregelen die de organisatie neemt. In paragraaf 3.3 van dit document staat beschreven hoe de waarde van de informatie wordt bepaald.
* **Risicogebaseerde** aanpak van informatieveiligheid. Het Noord-Hollands Archief brengt op basis van het Information Security Monitoring System (ISMS) in kaart welke risico’s de organisatie loopt. Vervolgens wordt gekeken wat de kans is dat deze risico’s zich daadwerkelijk voordoen en wat de eventuele impact is. Op basis van deze risicoanalyse worden gericht maatregelen ingezet om de geïdentificeerde risico’s te mitigeren. Dit overzicht wordt gebruikt om vast te leggen op welk niveau de organisatie zich qua informatiebeveiliging zich bevindt en in hoeverre er voortgang te melden valt. Per kwartaal wordt er op basis van het ISMS een rapportage gemaakt met daarin een overzicht van gewogen risico’s.
* Informatiebeveiliging is **een lijnverantwoordelijkheid**: dat betekent dat de lijnmanagers (afdelingshoofden) in eerste instantie de verantwoordelijkheid dragen voor een goede informatiebeveiliging op hun afdeling. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan, in samenspraak met de informatiemanager en de security officer.
* Informatiebeveiliging is **ieders verantwoordelijkheid**. Naar medewerkers communiceert het Noord-Hollands dat een actieve bijdrage wordt verwacht aan de informatieveiligheid binnen het Noord-Hollands Archief. Dat gebeurt in de aanstellingsbrief, tijdens de gesprekscyclus tussen managers en medewerkers, met een organisatiebreed reglement, en met periodieke bewustwordingscampagnes.
* Informatiebeveiliging is **herkenbaar.** Het Noord-Hollands Archief brengt het abstracte onderwerp informatieveiligheid terug naar situaties en vraagstukken die herkenbaar zijn voor de gebruikers en medewerkers. Vervolgens worden concrete acties aangereikt die de gebruikers en medewerkers kunnen nemen om veiliger te werken.
* Informatiebeveiliging is een **continu proces**. Technologische, organisatorische en juridische ontwikkelingen maken het noodzakelijk om periodiek het gevoerde beleid te toetsen. Het doel is om te kijken of het Noord-Hollands Archief nog op de juiste wijze bezig is de beveiliging van de informatie waarborgt. De audits maken het mogelijk het beleid en de genomen maatregelen te controleren op efficiency **(controleerbaarheid).**
* **Eigendom van informatie:** het archief is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd, tenzij dit anders is overeengekomen. Daarnaast beheert de organisatie informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers dienen goed geïnformeerd te zijn over de regelgeving voor het (her)gebruik van deze informatie. Het Noord-Hollands Archief blijft verantwoordelijk voor de veiligheid van informatie, ook bij uitbesteding en *outsourcing*.
* **Waardering van informatie:** iedereen behoort de waarde van informatie te kennen en daarnaar te handelen. De waarde van de informatie wordt bepaald door de schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid (paragraaf 3.3). In de informatieclassificatie staat de waarde van de informatie op de verschillende kwaliteitsaspecten beschreven.
* **Afstemming maatregelen met waarde informatie** en het gewenste veiligheidsniveau. De waarde van de informatie bepaalt het veiligheidsniveau dat het Noord-Hollands Archief nastreeft, om deze waarde te garanderen. In de *maatregelenmatrix* is vastgelegd welke aanvullende maatregelen genomen worden bij informatie in hogere veiligheidscategorieën. Het pakket aan standaard veiligheidsmaatregelen is de *baseline* veiligheidsmaatregelen.
* Bij projecten en changes, zoals infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt **vanaf de start rekening gehouden** met informatiebeveiliging. Het Noord-Hollands Archief uitgangspunten *privacy by Design* (bij het onderwerp en in alle andere fases rekening houden met de privacy van de gebruik)en *privacy by Default* (standaard is de privacy van de gebruiker gegarandeerd, en hoeft niet geschonden te worden om gebruik te maken van de geleverde diensten).
* Geen concurrentie, maar **samenwerking** met andere archieven op het gebied van informatieveiligheid.
* Een **Integrale aanpak** van informatieveiligheid (Cultuur, ICT, proces, juridisch, fysiek, gedrag, bewustzijn etc.).
* Het datasubject blijft **eigenaar**van de eigen informatie, en heeft rechten op deze data conform de Wet bescherming persoonsgegevens en de Algemene verordening gegevensbescherming.
* Het Noord-Hollands Archief hanteert een **PDCA-cyclus** met betrekking tot informatieveiligheid. Deze staat beschreven in paragraaf 3.2. De PDCA-cyclus wordt mede onderbouwd door het gebruik van een ISMS.

## 2.2 PDCA-cyclus informatiebeveiliging

Informatiebeveiliging wordt als proces ingericht. Dat houdt in dat de jaarlijkse planning en controlecyclus gebaseerd is op de ISO 27001 (Plan, Do, Check, Act). Hierin worden jaarplannen opgesteld en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplannen.

Informatiebeveiliging is een continu proces. Het onderstaande figuur is een weergave van dit proces binnen het Noord-Hollands Archief:



Het Noord-Hollands Archief heeft een ISMS ingericht, op basis van de ISO 27001. In dit ISMS worden de risico’s van de organisaties bijgehouden en gewogen. De hoofdstukken in het ISMS komen overeen met de hoofdstukken uit de ISO 27001. In het ISMS wordt bijgehouden in hoeverre de organisatie voldoet aan een bepaalde maatregel/ voorschrift en in welke mate dit een risico is voor de organisatie. Ook de onderbouwing voor een bepaalde classificatie wordt toegevoegd aan het ISMS

Op basis van het ingevulde ISMS wordt een totaaloverzicht gegenereerd voor de gehele organisatie. De security officer rapporteert per kwartaal de stand van zaken op het gebied van informatieveiligheid. Dit gebeurt via stoplichten per onderdeel.

De security officer stelt samen met de informatiemanager jaarplannen op. Deze jaarplannen worden voorgelegd aan het MT ter goedkeuring. Ook de doelstellingen worden vastgelegd in het ISMS.

## 2.3 Classificatie

Bij het Noord-Hollands Archief zijn alle gegevens geclassificeerd, waarop dit informatiebeveiligingsbeleid van toepassing is. Het niveau van de beveiligingsmaatregelen is afhankelijk van de klasse waarin de informatie valt. De classificatie van informatie is afhankelijk van risico analyses. Daarbij zijn de volgende aspecten van belang:

* + Beschikbaarheid
  + Integriteit
  + Vertrouwelijkheid

Ten aanzien van de beschikbaarheidseisen worden de volgende klassen onderscheiden:

* **Laag:** algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van de organisatie, haar medewerkers of haar klanten;
* **Midden:** algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 24 uur brengt merkbare schade toe aan de belangen van de organisatie, haar medewerkers of haar klanten;
* **Hoog:** algeheel verlies of niet beschikbaar zijn van deze informatie brengt direct merkbare schade toe aan de belangen van de organisatie, haar medewerkers of haar klanten.

Voor vertrouwelijkheid en integriteit wordt de volgende indeling gevolgd.

|  |  |
| --- | --- |
| **Klasse** | **Basisprincipes** |
| **Openbaar** | * Iedereen, zowel binnen als buiten de organisatie, mag de gegevens inzien * Een specifieke groep mag deze gegevens wijzigen |
| **Laag** | * Iedereen die aan de organisatie is verbonden als medewerker mag deze gegevens inzien; toegang kan zowel binnen als buiten de organisatie worden verleend * Een specifieke groep mag deze gegevens wijzigen |
| **Midden** | * Iedereen die onderdeel is van een (gebruikers)groep mag deze gegevens inzien; toegang kan zowel binnen als buiten de organisatie worden verleend * Een specifieke groep mag deze gegevens wijzigen |
| **Hoog** | * Er is expliciet aangegeven wie welke rechten heeft t.a.v. de raadpleging en de verwerking van deze gegevens. |

Welk beveiligingsniveau geschikt is voor een bepaald informatiesysteem, hangt af van de classificatie van de informatie die het systeem verwerkt. De eigenaar bepaalt, in samenspraak met de informatie manager en functionaris gegevensbescherming, de classificatie. De vertrouwelijkheid van informatie is gebaseerd op privacywetgeving (Wbp, AVG) en op eigen beleid.

De classificatie van informatie binnen het Noord-Hollands Archief staat beschreven in de informatieclassificatie. Aan de verschillende niveaus zijn veiligheidsmaatregelen gekoppeld. Deze maatregelen kunnen betrekking hebben op cultuur, ICT, proces, juridisch, fysiek, gedrag, bewustzijn en andere aspecten. Voor informatie in de categorieën midden en hoog worden aanvullende veiligheidsmaatregelen genomen. De relatie tussen te nemen maatregelen en de waarde van informatie is vastgelegd in een maatregelenmatrix. Hierin staan per informatieklasse de noodzakelijke veiligheidsmaatregelen.

# 3. Normenkaders

## 3.1 Wettelijke voorschriften

Bij het Noord-Hollands Archief wordt op de volgende wijze omgegaan met relevante wet- en regelgeving.

**Wet Bescherming Persoonsgegevens (Wbp)**

Het Noord-Hollands Archief heeft de wettelijke vereisten (juistheid en nauwkeurigheid van gegevens en passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking) geïmplementeerd via beschermingsmaatregelen. Naleving van de beveiligingsmaatregelen leidt tot voldoen aan de wet. Het Noord-Hollands Archief volgt het Richtsnoer *beveiliging van persoonsgegevens* van de Autoriteit Persoonsgegevens.

**Archiefwet**

Het Noord-Hollands Archief houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d. Dit is onderdeel van de jaarlijkse externe accountantscontrole.

**Wet Computercriminaliteit**

De Wet Computercriminaliteit richt zich op de strafrechtelijke probleemgebieden in relatie tot het computergebruik. Naleving van dit informatiebeveiligingsbeleid en implementatie van de basis maatregelen bij het Noord-Hollands Archief moet leiden tot een niveau van beveiliging dat als voldoende mag worden gezien in het kader van de Wet Computercriminaliteit.

**Algemene verordening gegevensbescherming**

Deze Europese privacywetgeving vervangt de Wet bescherming persoonsgegevens (Wbp) en wordt vanaf 25 mei 2018 gehandhaafd. Het Noord-Hollands Archief neemt passende technische en organisatorische maatregelen om de adequate en veilige verwerking van persoonsgegevens te garanderen. Ook heeft het Noord-Hollands archief in het kader van de AVG een verwerkingsregister opgesteld.

**Wet algemene bepalingen Burgerservicenummer**

Een BSN mag alleen verwerkt worden als dit bij wet of algemene maatregel van bestuur (amvb) is bepaald. Een BSN mag verder alleen gebruikt worden als passende waarborgen zijn getroffen voor de bescherming van de rechten en vrijheden van de betrokkenen. De uitvoeringswet vult deze bepaling aan door te bepalen dat nationale identificatienummers die zijn voorgeschreven bij wet, zoals het BSN, slechts mogen worden gebruikt ter uitvoering van de betreffende wet of voor de doelen die bij wet zijn bepaald. Voor overheidsorganisaties is deze wettelijke basis neergelegd in de Wet algemene bepalingen Burgerservicenummer (Wabb)

## 3.2 Overige richtlijnen en landelijke afspraken

Het informatiebeveiligingsbeleid bij het Noord-Hollands archief is op hoofdlijnen gebaseerd op ISO 27001. Op basis van deze norm is een ISMS ingeregeld.

Aanvullende standaarden die binnen de archiefsector worden gebruikt, zijn NEN-ISO 15489-1(2016), NEN-ISO 23081-1 (2017) en NEN 2082(2008). In de bestaande archiefwet- en regelgeving wordt regelmatig naar deze standaarden verwezen.

## 3.3 Normenkaders voor externe leveranciers

Bij uitbesteding van de bewerking van persoonsgegevens door een externe partij, moeten minimaal de volgende zaken geregeld zijn:

* Bewerkersovereenkomst;
* Toetsing aan het informatiebeveiligingsbeleid;
* Service Level Agreement;
* Andere voorwaarden (bv. vanuit inkoop).

Het doel is om afspraken vast te leggen, zodat

1. De organisatie de veiligheid en privacy van de datasubjecten beschermt;
2. de organisatie goed onderbouwde beslissingen kan nemen over bewerking *door* externe partijen;
3. de organisatie goed onderbouwde beslissingen kan nemen over bewerking *voor* externe partijen;
4. Het Noord-Hollands Archief de bescherming van de data kan garanderen conform de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming;

# 4. Governance informatiebeveiligingsbeleid

In dit gedeelte wordt beschreven hoe informatieveiligheid ingebed is binnen het Noord-Hollands Archief.

## 4.1 Integrale veiligheid

Bij het Noord-Hollands Archief wordt op strategisch niveau aandacht geschonken aan informatiebeveiliging, fysieke beveiliging, ARBO-veiligheid, privacy en bedrijfscontinuïteit. De samenwerking tussen deze disciplines is een noodzakelijke voorwaarde voor een goede *governance*. Het doel is om aan alle soorten risico’s en hun onderlinge verwevenheid passende aandacht te schenken. Dit is ook vormgegeven door de (budgettaire) planningscyclus voor deze aspecten parallel te laten verlopen. Dat biedt handvatten om onderlinge interferentie op te merken en te behandelen.

## 4.2 Inpassing in de organisatiegovernance

In deze paragraaf wordt beschreven hoe *governance* van informatieveiligheid binnen Noord-Hollands archief is georganiseerd. Van belang daarbij is om onderscheid te maken naar richtinggevend of strategisch, sturend of tactisch en uitvoerend niveau.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Niveau** | **Taak** | **Rol** | **Overleg** | **Document** |
| **Besluiten**  **(strategie)** | Strategie IB   * Bepalen IB-strategie * Organisatie t.b.v. IB inrichten * IB-planning en control vaststellen * Business continuity management | * MT NHA * Portefeuillehouder IB (hoofd bedrijfsvoering), o.b.v. advies de security officer en informatiemanager | * MT NHA, eventueel aangevuld met specialisten | * Meerjarenbeleidsplan 2017-2020 * Informatiebeveiligingsbeleid * Beleidsnotities informatiebeveiliging en integrale veiligheid * Informatiebeleidsplan * Baseline informatiebeveiliging gemeenten (BIG) * Privacystatement * Informatieclassificatie en maatregelenmatrix |
| **Sturen**  **(Tactiek)** | Planning en Control IB:   * Voorbereiden normen en wijze van toetsen * Uitwerken standaarden * Evalueren beleid en maatregelen * Begeleiden en uitvoeren audits * Uitvoeren risicoanalyses | * Informatiemanager * Security officer * Functionaris gegevensbescherming (FG) * Hoofd bedrijfsvoering | * Informatie-management-overleg | * Kwartaalrapportage uit ISMS * Audits, assessments (o.a. ISO 27001), * privacy Impact Assessments * Jaarplan informatieveiligheid en privacy, op basis van ISMS * Voortgangsrapportage informatieveiligheid * Service Level Agreements * Bewerkersovereenkomsten * Risico top 8 |
| **Uitvoeren**  **(Operatie)** | Implementeren IB-maatregelen   * Registreren en evalueren incidenten * Communicatie eindgebruikers | * Functioneel beheerder(s) * Security officer * Functionaris gegevensbescherming (FG) * Proces- en informatie-eigenaren * Communicatieadviseur | * Operationeel overleg in de lijn * Presentatie voor hele organisatie | * Incidentregistratie incl. evaluatie * Richtlijnen veilig (digitaal) werken * Bewerkersovereenkomst * Procedures * Register verwerkingen |

N.b. in de matrix staan rollen beschreven, die hoeven niet één op één overeen te komen met medewerkers. Ook kan een rol bij verschillende medewerkers worden belegd.

## 4.3 Controle, naleving en sancties

De externe controle wordt uitgevoerd door onafhankelijke accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale *Planning & Control*-cyclus. Bij schending van vooraf overeengekomen gedragsregels omtrent informatiebeveiliging volgt een gesprek met de CISO. Hier wordt een passend vervolg besproken. Sancties zijn in overeenstemming met de aard van de overtreding.

## 4.4 Rollen informatiebeveiliging

Het Noord-Hollands Archief heeft een aantal rollen, om informatiebeveiliging gestructureerd en gecoördineerd op te pakken. Het Noord-Hollands Archief volgt zoveel mogelijk de rollen op het gebied van privacy en informatieveiligheid, zoals beschreven door het PVIB.

**Bestuur**

Het bestuur is eindverantwoordelijk voor de informatiebeveiliging binnen het Noord-Hollands Archief. Het bestuur stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging vast. De inhoudelijke verantwoordelijkheid voor informatiebeveiliging is gemandateerd aan de directeur van het Noord-Hollands Archief. Deze heeft de opdracht om voor de informatiebeveiliging voor de gehele instelling zorg te dragen. Het bestuur is hoofdelijk aansprakelijk voor het informatiebeveiligingsbeleid binnen het Noord-Hollands Archief.

**Portefeuillehouder informatiebeveiliging**

De portefeuillehouder informatiebeveiliging is het MT-lid dat veiligheid in portefeuille heeft. Hij is eindverantwoordelijk voor informatiebeveiliging binnen het Noord-Hollands Archief.

**Functionaris informatiebeveiliging (Information Security Officer)**

De functionaris informatiebeveiliging is een rol op strategisch (en tactisch) niveau. De informatiemanager vervult deze rol binnen het Noord-Hollands Archief. De functionaris informatiebeveiliging bewaakt de uniformiteit binnen de instelling. Zij is verantwoordelijk voor het opstellen van beleid met betrekking tot informatiebeveiliging en de jaarplannen op het gebied van informatieveiligheid. Zij adviseert vanuit haar rol het MT over vraagstukken op het gebied van informatieveiligheid.

**Functionaris gegevensbescherming**

De functionaris voor de gegevensbescherming (FG) houdt binnen het Noord-Hollands Archief toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens en de Algemene verordening gegevensbescherming. De FG adviseert vanuit haar rol het MT over vraagstukken op het gebied van privacy. De wettelijke taken en bevoegdheden van de FG, zoals beschreven in de Avg, geven deze functionaris een onafhankelijke positie in de organisatie. De FG fungeert ook als interne toezichthouder namens de Autoriteit Persoonsgegevens.

**ICT Security Officer**

De ICT Security Officer is verantwoordelijk voor veiligheid van de ICT-omgeving. Hij voert risicoanalyses uit op het gebied van ICT-gerelateerde zaken. De ICT Security Officer beheert het ISMS van de organisatieen vult de verschillende onderdelen in. Hij rapporteert op basis van het ISMS per kwartaal aan het MT. Hij maakt ook een jaarplan op basis van het ISMS, incidenten en andere bevindingen.

**Proceseigenaar**

Een proceseigenaar is (gedelegeerd) verantwoordelijk voor de correcte uitvoering van een proces.

**Informatie-eigenaar**

Een informatie-eigenaar is verantwoordelijk voor de beschikbaarheid, integriteit en vertrouwelijkheid van de data.

**Leidinggevende**

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

* periodiek het onderwerp informatiebeveiliging en veilig (digitaal) werken onder de aandacht te brengen in werkoverleggen;
* er voor te zorgen dat zijn medewerkers op de hoogte zijn van de regels rond veiligheid, waaronder informatiebeveiliging;
* toe te zien op de naleving van het beveiligingsbeleid door zijn medewerkers;
* aanspreekpunt r te zijn voor alle personeel gerelateerde informatiebeveiligingszaken.

De leidinggevende kan hierin ondersteund worden door de *functionaris informatiebeveiliging* en de *ICT security officer*.

## 4.5 Overleg

Binnen het Noord-Hollands Archief wordt gestructureerd overleg gevoerd over informatieveiligheid, om te voldoen aan de doelstellingen, zoals geformuleerd in hoofdstuk 2 van dit beleidsstuk.

Op **strategisch niveau** worden besluiten genomen over strategie, doelen, scope en ambitie op het gebied van informatiebeveiliging. Dit gebeurt binnen het MT, aangevuld met deinformatiemanager en de ICT security officer. Tijdens dit overleg wordt ook de richting bepaald die het Noord-Hollands Archief volgt op het gebied van informatieveiligheid en privacy. Dit gebeurt mede op basis van de kwartaalrapportages uit het ISMS en een classificering van risico’s.

Op **tactisch niveau** wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden en acties. Deze plannen en instrumenten zijn sturend voor de uitvoering. Dit tactisch overleg is onderdeel van het informatiemanagementoverleg.

Op **operationeel niveau** worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Binnen het Noord-Hollands Archief gebeurt dit binnen de verschillende afdelingen.

## 4.6 Bewustwording informatiebeveiliging

Het Noord-Hollands Archief start met een presentatie rondom de implicaties van de AVG

voor manier van werken. Dit is de aftrap voor bredere bewustwording omtrent informatiebeveiliging. Er wordt een digitale brochure opgesteld met do’s en don’ts.

De meldingen in het incidentenregister, plus de reactie hierop worden gedeeld in de afdelingsoverleggen. Daarnaast wordt tweejaarlijks een bewustwordingssessie gehouden met praktijkvoorbeelden. Hier wordt ook de voortgang rondom het ISMS gedeeld.

Het Noord-Hollands Archief houdt bij welke acties zijn ondernomen op het gebied van bewustwording rond veilig (digitaal) werken.

# 5. Melding en afhandeling incidenten

## 5.1 Incidentmanagement

Incidentbeheer en –registratie hebben betrekking op de wijze waarop geconstateerde dan wel vermoede inbreuken op de informatiebeveiliging door de medewerkers en bezoekers gemeld worden en de wijze waarop deze worden afgehandeld.

Elke eenheid is zelf verantwoordelijk voor het signaleren en melden van incidenten en inbreuken op informatiebeveiliging.

De incidenten worden geregistreerd volgens een standaard indeling, waardoor een objectieve vergelijking met incidenten bij andere instellingen mogelijk wordt. De incidenten worden afgehandeld en dienen als input voor de incidentrapportages, waarover in het operationeel overleg wordt gesproken. Bij constatering van bepaalde trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen of een bewustwordingscampagne.

De afhandeling van informatiebeveiligingsincidenten vindt plaats volgens het Noord-Hollands Archief crisismanagementplan. De *informatiemanager* en de *ICT security officer* nemen eventueel zitting in het crisisteam bij incidenten die de informatieveiligheid raken. Bij datalekken wordt de *functionaris gegevensbescherming* ingeschakeld.

## 5.2 Melden datalekken

Het Noord-Hollands Archief heeft een proces voor het melden en afhandelen van datalekken binnen de organisatie. De functionaris gegevensbescherming is de eigenaar van dit proces.

Gebruikers kunnen een datalek melden bij de *security officer* of functionaris gegevensbescherming.

De functionaris gegevensbescherming bepaalt of een datalek gemeld moet worden, eventueel in samenspraak met de directie en portefeuillehouder informatiebeveiliging.

Een datalek met een grote impact wordt opgeschaald naar het crisisteam. Het bestuur heeft de leiding bij een datalek met een grote impact. De *security officer* wordt ingezet om onderzoek te doen naar de oorzaak wanneer er sprake is van een digitaal datalek.

# Bijlagen Informatiebeveiligingsbeleid

### Bijlage 1: Register art. 30 AVG met verwerkingen persoonsgegevens

Dit document omschrijft welke persoonsgegevens er verzameld worden binnen het NHA en met welke reden, dit document is een levend document en valt onder het beheer van de FG.

### Bijlage 2: Privacyverklaring

Dit document is bedoeld voor burgers. Het omschrijft hoe het NHA omgaat met persoonsgegevens en wordt op de website geplaatst zodra Tanja in dienst is en akkoord met haar rol als FG

### Bijlage 3: Bewerkersovereenkomst

Dit document omvat de afspraken over persoonsgegevensbescherming tussen het NHA en leveranciers die te maken hebben met persoonsgegevens die het NHA verzamelt en/of beheert.

# Bijlage 1: Register art. 30 AVG met verwerkingen persoonsgegevens

**Noord-Hollands Archief**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **I.** | **a.** | **b.** | **c.** | **d.** | **e.** | **f.** | **g.** | **h.** | **i.** | **j.** | **k.** |
|  | **Werkproces** | **Welke persoons-gegevens worden verwerkt** | **Welke bijzondere persoons-gegevens worden verwerkt** | **Herkomst gegevens** | **Doel van de verwerking** | **Wettelijke grondslag** | **Verantwoordelijke** | **bewerker** | **(bewerkers)-overeenkomst** | **betrokkene** | **ontvangers** |
| **1** | Studiezaal | Naam, adres, woonplaats, doe bezoek | geen | bezoeker | Aanpassen dienstverlening | Bestemd voor statistische doeleinden | Klaartje Pompe | De Ree | Mais-Flexis | Marianne Hamersma, Marianne Voulon, Susan ‘t Hoenderdal | nvt |
| **2** | Nieuwsbrief | Naam, organisatie | geen | aanmelder | Informatie verstrekken | Op aanvraag van aanmelder | Maarten Brock | De Ree | Mais-Flexis | Annabelle Arntz | nvt |
| **3** | Personeelsadministratie | Naam, adres, geslacht, rekeningnummer | bsn | medewerker | Salaris | Noodzakelijk uitvoeren arbeidsovereenkomst | Lieuwe Zoodsma | Centric | PMIS | Simone Beemsterboer | nvt |
| **4** | Bestellingen | Naam. Adres, Geslacht | Rekening nummer | Eigen input klant | Dienstverlening | Noodzakelijk voor uitvoeren dienstverleningsovereenkomst | Oskar Brandenburg, Klaartje Pompe. Maarten Brock | DECOS | DECOS-JOIN | Medewerkers afdeling AC | nvt |
| **5** | HR | Naam, functie | ziekmelding | werknemer | Registratie ziekte | Noodzakelijk uitvoeren arbeidsovereenkomst | Klaartje Pompe/Maarten Brock/Oskar Brandenburg | Centric | PMIS | Simone Beemsterboer | nvt |
| **6** | HR | Naam, adres | Verklaring omtrent gedrag | sollicitant | Beoordelen geschiktheid | Noodzakelijk uitvoeren arbeidsovereenkomst | Lieuwe Zoodsma | Centric | PMIS | Simone Beemsterboer | nvt |
| **7** | Contact onderhouden | Naam, adres, organisatie | geen | Eigen input contact | Contact onderhouden met bv. ‘vrienden van het Noord-Hollands Archief’ of bestuursleden | Op aanvraag van contact | Lieuwe Zoodsma | DECOS | DECOS-JOIN | Paula van Someren | nvt |

|  |  |  |  |
| --- | --- | --- | --- |
| **Legenda:** |  |  |  |
| **opgesteld door** | **Roomyla Choenni** |  |  |
| **getoetst door** | **Ed Sewalt** |  |  |
| **vastgesteld door** | **Maarten Brock** |  |  |
| **verantwoordelijke** | **Maarten Brock** |  |  |
| **Functionaris Gegevens-bescherming** | **Tanja Holt** |  |  |
| **Gegevensregister wordt jaarlijks geactualiseerd door** | **Ed Sewalt** |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **II.** | **l.** | **m.** | **n.** | **o.** | **p.** |  |
|  | **Verwerking vindt plaats in applicatie / systeem** | **Bewaartermijn gegevens** | **Verstrekking aan derde land of internationale organisatie** | **Algemene beschrijving van de beveiligingsmaatregelen.** | **Bewerkers-overeenkomst** | **Privacy Impact Assessment** |
| **1** | Bezoekersadministratie | 7 jaar | nvt | registratie in MAIS-Flexis | Per Feb 2018 | laag |
| **2** | DECOS | 7 jaar | nvt | Beveiligde afgeschermde omgeving op afstand, achter inlog | Per Feb 2018 | laag |
| **3** | PIMS | 7 jaar | nvt | Beveiligde afgeschermde omgeving op afstand, achter inlog | Per Feb 2018 | hoog |
| **4** | DECOS | 7 jaar | nvt | Beveiligde afgeschermde omgeving op afstand, achter inlog | Per Feb 2018 | hoog |
| **5** | PIMS | 7 jaar | nvt | Beveiligde afgeschermde omgeving op afstand, achter inlog | Per Feb 2018 | hoog |
| **6** | PIMS | 7 jaar | nvt | Beveiligde afgeschermde omgeving op afstand, achter inlog | Per Feb 2018 | hoog |
| **7** | DECOS | 7 jaar | nvt | Beveiligde afgeschermde omgeving op afstand, achter inlog | Per Feb 2018 | laag |

|  |  |  |
| --- | --- | --- |
| **Begrippen** | | |
| **a.** | **werkproces** | In welk werkproces vindt de verwerking van de persoonsgegevens plaats? |
| **b.** | **Persoonsgegeven** | Elke gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon |
| **c.** | **Bijzonder persoonsgegeven** | Persoonsgegevens betreffende iemands (limitatief): godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven. Ook het BSN is een bijzonder persoonsgegeven, omdat het uniek is en tot een persoon herleidbaar is. |
| **d.** | **Herkomst gegevens** | Hoe komen de gegevens bij de afdeling/in het werkproces? |
| **e.** | **Doel van de verwerking** | Wat is het doel van de verwerking van de persoonsgegevens |
| **f.** | **Wettelijke grondslag** | Wat is de wettelijke grondslag van de verwerking. Op basis van welke wet/wetgeving/regelgeving? |
| **g.** | **Verantwoordelijke** | Natuurlijke persoon, rechtspersoon, bestuursorgaan of ieder ander die alleen of te met anderen het doel en de middelen voor de verwerking van de persoonsgegevens vaststelt. |
| **h.** | **bewerker** | Degene die voor de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. |
| **i.** | **(bewerkers)overeenkomst** | Een overeenkomst met een derde partij/externe op basis waarvan de verwerking/uitwisseling van de persoonsgegevens geregeld is. |
| **j.** | **betrokkene** | Op wie de persoonsgegevens betrekking heeft. |
| **k.** | **ontvangers** | Aan wie de persoonsgegevens wordt verstrekt. Hierbij wordt een uitzondering gemaakt voor wetenschapsdoeleinden[[1]](#footnote-1). |
| **l.** | **Verwerking vindt plaats in applicatie/systeem** | In welke applicaties of systemen worden de persoonsgegevens verwerkt/uitgewisseld of vastgelegd? |
| **m.** | **Bewaartermijn gegevens** | Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan vastgelegd is voor de verwerking van de doeleinden waarvoor zij worden verzameld of verwerkt. |
| **n.** | **Verstrekking aan derde land of internationale organisatie** | Worden de persoonsgegevens uitgewisseld met een derde land binnen of buiten de EU of een internationale organisatie? |
| **o.** | **Algemene beschrijving van de beveiligingsmaatregelen.** | Welke maatregelen zijn er getroffen om de persoonsgegevens te beveiligen? Bijvoorbeeld: autorisatiebeheer, hoe is dat geregeld? Beveiligd beheer en opslag van zowel digitale als hardcopy verwerkingen. |
| **p.** | **Privacy impact Assessment** | Is er een Privacy Impact Assessment uitgevoerd? Wat waren de resultaten? Waar staan de resultaten? |

# Bijlage 2: Privacyverklaring

Privacyverklaring Noord-Hollands Archief

Het Noord-Hollands Archief respecteert uw privacy en gaat volgens de eisen van de wet bescherming persoonsgegevens (WBP) en vanaf mei 2018 de algemene verordening gegevensbescherming (AVG) om met uw persoonsgegevens. In deze privacyverklaring informeert het Noord-Hollands Archief u over de wijze waarop het Noord-Hollands Archief met uw persoonsgegevens omgaat en wat uw rechten zijn.

Het Noord-Hollands Archief is aan te merken als de verantwoordelijke voor het verwerken van uw persoonsgegevens in de zin van de WBP en AVG.

De functionaris voor de gegevensbescherming (FG) van het Noord-Hollands Archief  is aangemeld bij de autoriteit persoonsgegevens (AP) en ziet erop toe dat de verwerking van persoonsgegevens door het Noord-Hollands Archief in overeenstemming is met de privacywetgeving WBP en AVG.

Doeleinden

Wij gebruiken persoonsgegevens voor de volgende doeleinden:

Afhandeling van door u aangevraagde (studie-)informatie of publicaties

Ter uitvoering en verbetering van onze dienstverlening

Nadere informatievoorziening over actuele ontwikkelingen, tentoonstellingen, het historisch café, congressen, seminars etc.

Werving en selectie

Samenstellen gebruikersstatistieken

Beveiliging en verbetering van onze website

Uw gegevens worden alleen voor de hierboven genoemde doeleinden gebruikt en voor andere doeleinden wordt expliciet uw toestemming gevraagd.

Rechten van betrokkene

Als eigenaar van uw persoonsgegevens (betrokkene) heeft u volgens de privacywetgeving bepaalde rechten. Verzoeken hiertoe kunt u richten aan de functionaris gegevensbescherming van het Noord-Hollands Archief :

[Tanja.Holt@noord-hollandsarchief.nl](mailto:Simone.Beemsterboer@noord-hollandsarchief.nl)

Uw rechten zijn:

A.       Recht op inzage: u kunt een verzoek aan de FG richten om een opgave te krijgen van de persoonsgegevens die wij van u gebruiken en beheren.

B.      Recht op correctie: indien wij uw persoonsgegevens foutief gebruiken, kunt vragen om correctie, waarbij het Noord-Hollands Archief wel gehouden is aan de registratie van persoonsgegevens volgens de AP

C.       Recht om 'vergeten te worden': u kunt een verzoek doen om uw gegevens te verwijderen uit de bestanden van het Noord-Hollands Archief. Uiteraard is dit niet van toepassing indien u nog een betalingsverplichting aan het Noord-Hollands Archief open heeft staan.

D.      Recht op dataportabiliteit: u kunt een verzoek doen om uw gegevens over te dragen aan een door u aangegeven instantie.

Verstrekking aan derden

Voor de verwerking van uw persoonsgegevens kan het Noord-Hollands Archief gebruik maken van dienstverleners, die als bewerker (ook verwerker genoemd) uitsluitend in opdracht en te behoeve van het Noord-Hollands Archief zullen optreden. Bewerkers werken op grond van een daartoe afgesloten verwerkersovereenkomst. Daarbuiten worden uw gegevens niet aan derden verstrekt, tenzij het Noord-Hollands Archief daartoe verplicht is op grond van de wet.

Het Noord-Hollands Archief draagt - samen met eventuele bewerkers - zorg voor een passende organisatorische en technische beveiliging van persoonsgegevens. Op deze wijze stellen wij zeker dat deze gegevens alleen toegankelijk zijn voor personen die daar uit hoofde van hun functie of taak toe bevoegd zijn en dat de gegevens alleen worden gebruikt voor de doeleinden waarvoor ze zijn verkregen.

Datalekken

Indien u van mening bent dat er persoonsgegevens van stagiairs of interne/externe medewerkers van het Noord-Hollands Archief voor onbevoegden toegankelijk zijn of u hiervan een vermoeden heeft vragen wij u dit direct te melden via het algemene nummer van het Noord-Hollands Archief of het servicepunt van de locatie.

De procedure voor het analyseren, oplossen en eventueel melden bij de AP van het data-incident treedt dan in werking.

Cameratoezicht

Het Noord-Hollands Archief beschermt uw veiligheid en eigendommen onder andere via cameratoezicht in de gebouwen. De beelden van deze camera's worden automatisch vernietigd na een maand.

Cookies

Via onze websites kunnen wij gebruik maken van cookies, eenvoudige kleine bestandjes die door uw browser worden opgeslagen op uw computer. U kunt uw browser zo instellen dat u tijdens uw bezoek aan onze websites geen cookies ontvangt. In dat geval kan het echter gebeuren dat u geen gebruik kunt maken van alle mogelijkheden van onze websites.

Hyperlinks

Onze websites bevatten hyperlinks naar websites van derden. Het Noord-Hollands Archief is niet verantwoordelijk voor de inhoud van deze websites en is evenmin verantwoordelijk voor het privacybeleid en het gebruik van cookies op deze websites.

Wijzigingen

Het Noord-Hollands Archief behoudt zich het recht voor om wijzigingen aan te brengen in de privacyverklaring. Wij adviseren u daarom regelmatig de privacyverklaring na te lezen op eventuele wijzigingen. Meer informatie is te vinden op het Noord-Hollands Archief onder het kopje 'organisatie’ en de website van de autoriteit persoonsgegevens (AP).

Contactgegevens

Het Noord-Hollands Archief stelt uw vragen en opmerkingen met betrekking tot deze privacyverklaring op prijs. Als u van mening bent dat deze privacyverklaring niet wordt nageleefd of een klacht heeft over het gebruik van uw persoonsgegevens door het Noord-Hollands Archief of een verzoek in wilt dienen om gebruik te maken van uw rechten als betrokkene, kunt u dit rechtstreeks laten weten aan: [Tanja.Holt@noord-hollandsarchief.nl](mailto:Tanja.Holt@noord-hollandsarchief.nl)

Privacyverklaring het Noord-Hollands Archief

Per 7-03-2018

# Bijlage 3: Bewerkersovereenkomst

**Bewerkersovereenkomst**

**Noord Hollands-Archief**

Partijen:

1. Noord-Hollands Archief, een semi-overheidsinstelling statutair gevestigd te Haarlem, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 57581665 (**"Verantwoordelijke"**);

en

1. [**NAAM BEWERKER**], een [besloten vennootschap / naamloze vennootschap / stichting / vereniging] statutair gevestigd te [PLAATS], ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer [NUMMER] (**"Bewerker"**);

Verantwoordelijke en Bewerker worden gezamenlijk ook aangeduid als “**Partijen**” en elk afzonderlijk tevens een "**Partij**"

**OVERWEGINGEN**

1. Gezien het feit dat het Noord-Hollands archief gehouden is aan de Algemene Verordening Gegevensbescherming dient er een overeenkomst afgesloten te worden rondom het gebruik van persoonsgegevens.
2. DEFINITIES

In deze Bewerkersovereenkomst worden de hierna volgende termen in de navolgende betekenis gebruikt, tenzij uitdrukkelijk anders is aangegeven.

**"Overeenkomst**" betekent de [NAAM OVEREENKOMST], inclusief wijzigingen en aanvullende overeenkomsten, overeengekomen tussen de Verantwoordelijke en de Bewerker, die naar deze Bewerkersovereenkomst verwijst.

**"Bewerkersovereenkomst"** betekent deze bewerkersovereenkomst, inclusief eventuele bijlagen;

**"Security Breach"** betekent iedere inbreuk op de beveiliging van Persoonsgegevens die leidt of kan leiden tot ongeautoriseerde toegang, verlies, verandering of openbaarmaking van Persoonsgegevens.

**"Persoonsgegevens"** betekent elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon dat Verwerkt wordt door de Bewerker onder de Overeenkomst, zoals beschreven onder Annex 1;

"**Sub Bewerker**" betekent een bewerker, zoals gedefinieerd in de Wbp, die in opdracht van de Bewerker Persoonsgegevens zal Verwerken ten behoeve van de Verantwoordelijke;

"**Technische en Organisatorische** betekent de technische en organisatorische

**Maatregelen”** beveiligingsmaatregelen die Persoonsgegevens beveiligen tegen verlies of onrechtmatige verwerking en die, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen gelet op de risico’s van de Verwerking van Persoonsgegevens;

"**Toepasselijke Wetgeving** " betekent alle wetgeving, inclusief de Wet bescherming persoonsgegevens, betreffende de bescherming van persoonsgegevens die van toepassing is op de Verwerking van Persoonsgegevens in verband met de activiteiten die uitgevoerd worden op grond van de Overeenkomst;

**"Verwerken" of "Verwerking"** betekent elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;

1. VERPLICHTINGEN VAN DE BEWERKER
   1. De Bewerker zal:
2. Persoonsgegevens verwerken conform de instructies van de Verantwoordelijke en op de wijze zoals omschreven onder Annex 1;
3. Persoonsgegevens alleen bewaren zolang de Verantwoordelijke dat verlangt en de Persoonsgegevens wijzigen, anonimiseren, blokken of verwijderen zodra de Verantwoordelijke daartoe instructies geeft; en
4. ervoor zorgen dat alleen (i) haar werknemers; en (ii) Sub Bewerkers toegang krijgen tot Persoonsgegevens en slechts zolang dit noodzakelijk is in het kader van de uitvoering van de verplichtingen van de Bewerker onder de Overeenkomst.
5. Technische en Organisatorische Maatregelen
   1. De Bewerker zal Technische en Organisatorische Maatregelen, zoals beschreven in Annex 2, treffen, in stand houden en zo nodig aanpassen om de Persoonsgegevens te beveiligen.
6. DOORGIFTE VAN PERSOONSGEGEVENS
   1. Verantwoordelijke geeft de Bewerker hierbij instructie om Persoonsgegevens door te geven en te Verwerken in een land buiten de Europese Economische Ruimte (EER), mits:
      1. dat land een passend beschermingsniveau waarborgt en welke formeel zo is erkend door plaatsing op de 'witte lijst' van de Europese Commissie; of
      2. gebruik wordt gemaakt van een modelcontract als bedoeld in artikel 26, vierde lid, van richtlijn nr. 95/46/EG tussen de Verantwoordelijke en de Bewerker of een Sub Bewerker.
   2. Indien Persoonsgegevens worden doorgestuurd naar een Sub Bewerker in een land buiten de EER, geeft de Verantwoordelijke hierbij instructie en een volmacht aan de Bewerker om, op naam van de Verantwoordelijke, de Sub Bewerker instructies te geven en de onder artikel 4.1.b genoemde overeenkomsten te sluiten.
7. SUB BEWERKERS
   1. Het is Bewerker toegestaan Persoonsgegevens te doen Verwerken door Sub Bewerkers mits Bewerker met de desbetreffende Sub Bewerker een schriftelijke overeenkomst heeft gesloten waarin deze Sub Bewerker verplichtingen overeenkomstig aan deze Bewerkersovereenkomst oplegt.
8. GEHEIMHOUDING  
   1. Bewerker zal de Persoonsgegevens geheimhouden en zal haar werknemers, Sub Bewerkers en werknemers van Sub Bewerkers, voordat zij toegang verkrijgen tot de Persoonsgegevens, contractueel verplichten tot geheimhouding van de Persoonsgegevens waarvan zij met betrekking tot de uitvoering van de Overeenkomst kennis kunnen nemen.
   2. De geheimhoudingsplicht van Persoonsgegevens door Bewerker of Sub Bewerker kan alleen worden doorbroken wanneer een wettelijk voorschrift verplicht om Persoonsgegevens te verstrekken of de Verantwoordelijke hiertoe instructie geeft.
9. MELDPLICHT
   1. Bewerker zal Verantwoordelijke zo spoedig mogelijk informeren over iedere Security Breach en zal maatregelen treffen die redelijkerwijs van haar kunnen worden verwacht om de nadelige gevolgen van de Security Breach te herstellen dan wel zoveel mogelijk te beperken.

* 1. Verantwoordelijke is uit hoofde van de Toepasselijke Wetgeving zelf verantwoordelijk voor het doen van meldingen aangaande de Security Breach aan de desbetreffende toezichthouder(s) en/ of betrokkene(n).

1. Duur en beëindiging Bewerkersovereenkomst
   1. Deze Bewerkersovereenkomst wordt gesloten op het moment dat Partijen deze hebben ondertekend en loopt door tot beëindiging van de Overeenkomst.
   2. Bewerker zal de hiervoor bedoelde Persoonsgegevens onverwijld na beëindiging van de Overeenkomst, of zoveel eerder als dat mogelijk is, overdragen aan Verantwoordelijke.
   3. Na overdracht, schriftelijke afwijzing van overdracht door Verantwoordelijke, of indien de Verantwoordelijke niet reageert binnen één maand na het aanbod tot overdracht, zal de Bewerker de Persoonsgegevens onverwijld vernietigen. Op eerste verzoek van Verantwoordelijke zal Bewerker schriftelijk bevestigen dat dit daadwerkelijk gebeurd is.
2. OVERIGE BEPALINGEN
   1. Op deze Bewerkersovereenkomst is Nederlands recht van toepassing.
   2. Wijzigingen en aanvullingen van deze Bewerkersovereenkomst kunnen slechts schriftelijk, bij akte ondertekend door beide partijen, worden overeengekomen.

**Verantwoordelijke**

Datum: ……………………………………..

Naam: ……………………………………..

Handtekening: ..……….………………….

**Bewerker**

Datum: ……………………………………..

Naam: …………………………………….

Handtekening:……….…………………..

#### ANNEX 1

#### BESCHRIJVING VERWERKING PERSOONSGEGEVENS

**Categorieën persoonsgegevens**

De categorieën persoonsgegevens die door Bewerker worden verwerkt zijn:

* [bijv. naam en adres klant of ip-adressen]

**Verwerking persoonsgegevens**

#### De Persoonsgegevens zullen door Bewerker als volgt worden verwerkt:

* [beschrijving proces]

**Verantwoordelijke**

Datum: ………………………………

Naam: ………………………………

Handtekening:........ ………………

**Bewerker**

Datum: ………………………………

Naam: ………………………………

Handtekening:........ ………………

#### ANNEX 2

#### BESCHRIJVING TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

Deze Annex beschrijft de technische en organisatorische maatregelen en procedures die Bewerker zal nemen om de verwerking van Persoonsgegevens adequaat te beveiligen.

[TECHNISCHE EN ORGANISATORISCHE MAATREGELEN DIE DOOR BEWERKER WORDEN GENOMEN]

**Verantwoordelijke**

Datum: ………………………………

Naam: ………………………………

Handtekening:........ ………………

**Bewerker**

Datum: ………………………………

Naam: ………………………………

Handtekening:........ ……............

1. Algemene Verordening Persoonsgegevens, Artikel 23:

   *Het verbod om bijzondere persoonsgegevens te verwerken ten behoeve van wetenschappelijk onderzoek of statistiek is niet van toepassing voor zover:*

   1. *Het onderzoek een algemeen belang dient,*
   2. *De verwerking voor het betreffende onderzoek of de betreffende statistiek noodzakelijk is,*
   3. *Het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kosten en*
   4. *Bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.*

   Algemene Verordening Persoonsgegevens, Artikel 24:

   *a. een zwaarwegend geneeskundig belang prevaleert; of*

   *b. de verwerking noodzakelijk is ten behoeve van wetenschappelijk onderzoek*

   *of statistiek en de betrokkene uitdrukkelijke toestemming heeft gegeven.*

   Algemene Verordening Persoonsgegevens, Artikel 27:

   *Het verbod om bijzondere persoonsgegevens te verwerken, is niet van toepassing voor zover dit noodzakelijk is met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden als bedoeld in artikel 9, tweede lid, onderdeel j, van de verordening, voor zover:*

   *a. de verwerking een algemeen belang dient;*

   *b. het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een*

   *onevenredige inspanning kost; en*

   *c. bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke*

   *levenssfeer van de betrokkene niet onevenredig wordt geschaad.*

   Algemene Verordening Persoonsgegevens, Overweging 160:

   *"Wanneer persoonsgegevens met het oog op historisch onderzoek worden verwerkt, dient deze verordening ook voor verwerking met dat doel te gelden. Dit dient ook historisch onderzoek en onderzoek voor genealogische doeleinden te omvatten, met dien verstande dat deze verordening niet van toepassing mag zijn op overleden personen."* [↑](#footnote-ref-1)