Oplevering werkzaamheden PRP20170524002 1

Titel: Oplevering werkzaamheden PRP20170524002

Datum: 1 maart 2018

Van: Jeroen Wittink, Factor50 Informatieveiligheid

Aan: Roomyla Choenni, Maarten Brock, Ed Sewalt

Status: Vertrouwelijk

Inleiding

Het Noord-Hollands Archief heeft de afgelopen maanden verschillende stappen

gezet om (1) informatieveiligheid naar een hoger niveau te brengen en te

houden en (2) compliant te worden aan de nieuwe Europese privacywetgeving,

de Algemene verordening gegevensbescherming (Avg).

De opdracht aan Factor50 was om het Noord-Hollands archief te begeleiden bij

het opstellen van informatiebeveiligingsbeleid en het inrichten van een

*Information Security Management System* (ISMS), om risico’s voor de organisatie

in kaart te brengen en bij te houden.

Het Noord-Hollands archief heeft onder begeleiding van Factor50 verschillende

producten opgeleverd. In samenhang vormen ze de strategie van het Noord-

Hollands archief op het gebied van informatieveiligheid en privacy. Het gaat om

de volgende producten: informatiebeveiligingsbeleid, privacy statement, Avgregister,

verwerkersovereenkomst, ISMS.

In de bijlage van deze memo hebben we een overzicht gemaakt van een top 8 van

concrete risico’s voor het Noord-Hollands Archief, op basis van de gesprekken en

het ingevulde ISMS.

Opgeleverde producten

Hieronder beschrijven we de opgeleverde documenten. De afgelopen maanden

zijn ze opgesteld en ingevuld, op basis van de situatie bij het Noord-Hollands

Archief. De documenten worden ter goedkeuring aangeboden aan de directie.

Werken aan informatieveiligheid en privacy is een continu proces. Daarom moet

het blijvende aandachtspunten blijven binnen de bedrijfsvoering. Het ISMS is

hierbij een belangrijk hulpmiddel.

Informatiebeveiligingsbeleid

In het informatiebeveiligingsbeleid staat beschreven wat de overkoepelende

strategie is van het Noord-Hollands Archief om informatieveiligheid binnen de

organisatie op het gewenste niveau te krijgen en te behouden. Het

informatiebeveiligingsbeleid is *intern* gericht. In het beleid staat beschreven wat

de doelstellingen zijn op het gebied van informatieveiligheid en privacy,

uitgangspunten, PDCA-cyclus (waaronder het gebruik van het ISMS), en hoe

informatieveiligheid en privacy is georganiseerd (overlegstructuur, rollen,

documenten, processen).

Oplevering werkzaamheden PRP20170524002 2

Avg verwerkingsregister

Een register van verwerkingen is een wettelijke verplichting onder de Avg

(artikel 30). In een dergelijk register moet een organisatie o.a. aangeven welke

persoonsgegevens worden verwerkt, met welk doel en op basis van welke

grondslag, en wie de verwerkers, betrokkenen en ontvangers zijn. Factor50 heeft

een template aangeleverd voor een register en aangegeven hoe een dergelijk

register moet worden ingevuld. Roomyla Choenni heeft dit gedaan voor het

Noord-Hollands Archief.

Privacy Statement

In een privacy statement staat beschreven hoe een organisatie omgaat met

privacygevoelige data van haar klanten. Een privacy statement (of

privacyverklaring) is *extern* gericht, en moet bijvoorbeeld gepubliceerd worden

op de website en eventueel op andere uitingen. Factor50 heeft een template

aangeleverd van een privacy statement en aangegeven welke elementen

opgenomen moeten worden, waaronder de rechten van de bezoekers en een

adres voor vragen, opmerkingen en verzoeken. Het Noord-Hollands Archief heeft

het statement aangepast aan de eigen situatie.

Verwerkersovereenkomst

Het Noord-Hollands Archief blijft verantwoordelijk voor de veiligheid van de

data die verzameld wordt, ook als deze door een andere partij wordt verwerkt.

In dat geval moet een verwerkersovereenkomst worden aangegaan. Factor50

heeft een template aangeleverd van een verwerkersovereenkomst. Roomyla

Choenni heeft de verwerkersovereenkomst aangepast en naar de externe

verwerkers verstuurd. In de verwerkersoverkomst staat naast de algemene

bepalingen beschreven welke verwerkingen door de externe partij worden

uitgevoerd. Deze verwerkingen staan beschreven in het Avg-register. Hierin

staat ook vermeld dat er een externe verwerker is. Het Noord-Hollands Archief

voldoet met het afsluiten van verwerkersovereenkomsten aan een wettelijke

verplichting onder de Avg.

Information Security Management System (ISMS)

In het ISMS staat beschreven wat de stand van zaken is op het gebied van

informatieveiligheid binnen het Noord-Hollands Archief. Dit is beschreven aan

de hand van de verschillende onderdelen van de ISO 27001. In het ISMS is de

GAP-analyse verwerkt die het Noord-Hollands Archief heeft laten uitvoeren.

Factor50 heeft een template voor een ISMS aangeleverd.

Ed Sewalt heeft samen met Ko Groen het ISMS ingevuld. Het ISMS geeft een

risicobeeld voor het Noord-Hollands Archief in de vorm van stoplichten, op de

verschillende terreinen. Per onderdeel zijn de specifieke risico’s ingevuld door

Ed Sewalt. Dit leidt tot een risicobeeld, waarbij rekening wordt gehouden met de

stand van zaken op een bepaald aandachtsgebied, maar ook met de importantie

van het gebied voor het Noord-Hollands archief. Per kwartaal wordt op via het

ISMS gerapporteerd aan het MT.

Oplevering werkzaamheden PRP20170524002 3

Bijlage: Risico top 10

Factor50 heeft op basis van het ISMS en verschillende gesprekken met

belanghebbenden een top 10 opgesteld van risico’s. Op basis van het ISMS,

rapportage Q1, ziet het risicoprofiel globaal er als volgt uit:

In het ISMS is per onderdeel een onderbouwing gegeven van de classificatie van

de risico’s, op basis van concrete voorbeelden.

Aandachtspunten

Op basis van de gesprekken en het ISMS, zien we de volgende concrete risico’s

voor het Noord-Hollands Archief. Dit zijn risico’s op het gebied van

informatieveiligheid. Er zijn ook andere risico’s op het gebied van de

bedrijfsvoering en de uitvoering van de wettelijke taak, in samenwerking met

andere instellingen waaronder het nationaal archief. Ed Sewalt heeft hiervoor

een aantal risico’s in kaart gebracht.

Risico top 8 informatieveiligheid

Hieronder de opzet van een top 8 risico’s op het gebied van informatieveiligheid

en privacy. De inschatting is gemaakt op basis van het ISMS en de gesprekken.

Een nadere uitwerking door het Noord-Hollands Archief is aan te bevelen.

1. Datalek door verkeerd mailen

a. Automatisch aanvullen mailadressen

b. Fouten en slordigheden met mail

c. Ontvangen van privacygevoelige informatie

Oplevering werkzaamheden PRP20170524002 4

2. Onvoldoende compliant aan Avg

a. Avg-registers onvoldoende en/ of onvolledig ingevuld;

b. Niet kunnen voldoen aan het recht op vergeten worden uit het

archief (zie uitspraak Raad van State);

c. Privacy by design en default niet genoeg geïncorporeerd bij

changes en projecten;

d. Niet toepassen van dataminimalisatie;

3. Verkeerde afhandeling datalekken

a. Ontbreken standaardcommunicatie;

b. Incidentregistratie en protocol afhandeling incident onvoldoende;

4. Incidenten door fysieke oorzaken

a. (Uitleen)laptops raken kwijt, mogelijk met ingevulde credentials

en/ of geen wachtwoord;

b. niet locken computers, met name in publiektoegankelijke ruimten;

c. Afvoer van (privacy-)gevoelige informatie op papier

5. Geen privacy impact assessments gehouden op systemen met informatie

in de hoogste categorie vertrouwelijkheid

6. Uitvallen dienstverlening

7. Cybercriminaliteit

a. Infrastructuur misbruikt voor crypto-mining

b. Identiteitsfraude

8. IT-leveranciers (beheerders) kunnen bij te veel informatie

Oplevering werkzaamheden PRP20170524002 5

Colofon

Organisatie

Factor50

Factor50 Informatieveiligheid B.V.

Kamer van Koophandel 64896722

Bankrelatie NL90INGB0007168446

Btw-indentificatienummer NL855892274B01

E-mail: contact@factor50.eu

Telefoon: +31 (0)85 8000 245

Adres: Zijlweg 148b

2015 BJ, Haarlem

Nederland

Handelsmerken en geheimhouding

Verstrekking van informatie ten behoeve van deze memo:

Noord-Hollands Arcief en Factor50 Informatieveiligheid B.V. verplichten zich als

partijen de aan elkaar gedeelde informatie geheim te zullen houden, noch te

doen verspreiden. Factor50 heeft de benodigde informatie uitsluitend gebruikt

ten behoeve van deze memo en beperkt tot deze memo.

Alle informatie, handelsmerken, namen, logo’s, beeltenissen, tabellen of andere

zaken waar eigendomsrechten op van toepassing zijn, gebruikt in dit document

zijn eigendom van de desbetreffende rechtmatige eigenaar.

Factor50 informatieveiligheid B.V. Kamer van Koophandel 64896722.

© 2018 Factor50. Alle rechten voorbehouden.