PRIVACY & SECURITYSTATEMENT NHG

Inleiding

NHG beschikt over veel, en vaak gevoelige (persoons)gegevens. Veel van die gegevens zijn afkomstig van onze ketenpartners: geldverstekkers en hun servicers. Een schending van de beschikbaarheid, integriteit of vertrouwelijkheid van die gegevens, bijvoorbeeld door fraude of een informatielek, kan verstrekkende gevolgen hebben.

Met een uitgebreide set maatregelen doen we er alles aan om financiële- of imagoschade bij NHG en haar stakeholders en een inbreuk op het fundamentele recht op privacy van onze klanten te voorkomen. Dit statement is met name bedoeld om ketenpartners een globaal inzicht te geven in de getroffen maatregelen en hen daarmee enige mate van zekerheid te bieden over de volledigheid en doeltreffendheid daarvan.

Hoofdstuk 1 geeft een generieke omschrijving. In hoofdstuk 2 worden de voornaamste concrete maatregelen opgesomd.

HOOFDSTUK 1: GENERIEKE OMSCHRIJVING

Kaders

Kaders worden gevormd door relevante wet- en regelgeving. Hierbij is met name de Algemene Verordening Gegevensbescherming (AVG) van belang. Voor de implementatie van de AVG maakt NHG gebruik van het 'Nymity Privacy Management Accountability Framework'. Dit framework onderkend 55 technische en organisatorische maatregelen die tezamen leiden tot een adequate implementatie van privacy.

ISO/IEC 27001

NHG richt security in volgens ISO/IEC27001. Daartoe is een securitystrategie en een securitybeleid opgesteld als ook een security architectuur die ziet op alle bedrijfsmiddelen, een risicoanalyse die periodiek wordt herijkt, een verbeterplan en een procedure beveiligingsincidenten. Daarnaast wordt intensief gewerkt aan awareness en kennis, kent NHG een gedegen screening-proces en worden periodiek zelfbeoordelingen en onafhankelijke beoordelingen uitgevoerd. Het bestuur en management worden actief gekend in het gevoerde risicomanagement. NHG streeft continu naar verbetering en volgt hierbij het door DNB opgestelde 'Toetsingskader Informatiebeveiliging'

Stakeholders

Bij het bepalen van maatregelen houdt NHG rekening met de belangen van haar stakeholders. Vooral de belangen van de ketenpartners worden hierin gekend. Daarnaast worden ook de belangen van de Raad van Commissarissen, het Ministerie van Financiën, het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en partijen als Vereniging Eigen Huis, de Autoriteit Financiële Markten en De Nederlandsche Bank meegewogen.

Proces

Informatiebeveiliging is ingericht als cyclisch proces (plan-do-check-act). Op basis van de uitkomst van evaluaties en controles of door nieuwe ontwikkelingen kan de noodzaak aanwezig

zijn om het informatiebeveiligingsbeleid aan te passen of om extra beveiligingsmaatregelen te treffen. Ook is het mogelijk dat nieuwe ontwikkelingen, zoals de introductie van nieuwe bedrijfsprocessen of informatiesystemen, aanleiding geven om het informatiebeveiligingsbeleid te heroverwegen. Bij het realiseren van het verbeterplan wordt een risico gebaseerde aanpak gevolgd.

Controles
NHG voert periodieke controles uit op de opzet, het bestaan en de werking van de getroffen maatregelen. Er worden regelmatig technische scans (pentesten) uitgevoerd op de verschillende diensten die NHG heeft uitbesteed. In deze tests wordt specifiek aandacht besteed aan de logische scheiding van gegevens van verschillende ketenpartners en de voornaamste dreigingen (OWASP). Bij cruciale leveranciers worden third party mededelingen of certificeringen opgevraagd en beoordeeld. Ook wordt gebruik gemaakt van verschillende onlinediensten om de security settings bij partijen waar we gegevens mee delen te controleren.

ISEA3402 rapportage
De stakeholders van NHG hebben behoefte aan inzicht in de processen en in de zekerheden die zij biedt. NHG geeft jaarlijks met het ISAE 3402 type II rapport transparante informatie over de inrichting van de beheersmaatregelen die zijn ingericht voor een optimaal verloop van deze processen. De uitvoering van de processen en de werking van de beheersmaatregelen worden uiteengezet in dit rapport en zijn getoetst door de onafhankelijke accountant. De ISAE-verklaring van NHG ziet met name op de risico's van financiële processen.

Privacy & Security by design
NHG past Privacy & Security by Design toe door te zorgen dat al in de ontwerpfase van nieuwe processen en producten de juiste maatregelen worden geïdentificeerd en borgt dat deze tot en met de beheerfase worden ingevuld.

Multi layered security
Alle toepassingen waarin klantgegevens staan of gegevens van onze medewerkers en toepassingen die bedoeld zijn voor financiële transacties zijn beschermd door meerdere beveiligingslagen. Zo wordt naast encryptie en credentials altijd MFA, IP Whitelist of een token toegepast. Voor webservices die wij aan onze ketenpartners aanbieden geldt hetzelfde. Daarop wordt naast encryptie en credentials altijd een 2-weg certificaat of IP whitelisting toegepast. Alleen als de ketenpartner dat zelf niet wil of kan wordt daarvan afgeweken.

Due dilligence
NHG is een regieorganisatie op het gebied van IT-voorzieningen: nagenoeg alle diensten zijn uitbesteed. Bij de selectie van leveranciers worden hoge eisen gesteld aan de leverende organisatie en de te leveren techniek op het gebied van informatiebeveiliging. NHG heeft hiertoe een Beveiligingsovereenkomst opgesteld waarin de vereisten zijn beschreven waaraan de leverancier en de dienst dienen te voldoen.

In de regel zijn de partijen die NHG inzet gerenommeerde en gecertificeerde bedrijven die informatiebeveiliging hoog in het vaandel dragen. Daarnaast is met alle partijen die persoonsgegevens verwerken een verwerkersovereenkomst gesloten waarin ook de Meldplicht

datalekken wordt geadresseerd. De datacenters die NHG gebruikt zijn ISO of SOC2 gecertificeerd of geven een ISAE-rapportage af. Uiteraard is met alle IT-leveranciers een Service Level Agreement overeengekomen. Het proces rondom het beheer van de afspraken met leveranciers maakt onderdeel uit van de ISAE 3402 controle van NHG.

Marktstandaarden & best practices
Bij het ontwerpen van beveiligingsrichtlijnen en maatregelen baseert NHG zich zoveel mogelijk op marktstandaarden en best practices. Daartoe worden richtlijnen gebruikt die beschikbaar worden gesteld door bijvoorbeeld de Autoriteit Persoonsgegevens en het Nationaal Cyber Security Centrum. Waar nodig huurt NHG externe expertise in om te adviseren over beveiligingsvraagstukken. NHG houdt haar IT-leveranciers aan marktconforme – 'bij de huidige stand van de techniek passende' - maatregelen. Zoals vermeld worden deze diensten daarop eveneens gecontroleerd en getest. De inzet van middelen als high-end firewalls, anti D-Dos, encryptie, IDS, IPS, en redundante componenten zijn vanzelfsprekend.

Continuïteit
NHG heeft een Bedrijfscontinuïteitsplan en een Uitwijkplan. Daarin zijn procedures en afspraken voor calamiteitensituaties beschreven en hoe het crisisteam is samengesteld. Er zijn scenario's beschikbaar voor de situatie waarbij de bedrijfslocatie niet beschikbaar is en voor de situatie waarbij de IT-voorzieningen (tijdelijk) niet beschikbaar zijn. Voor IT-voorzieningen is (vanzelfsprekend) voorzien in back-ups en zijn passende beschikbaarheidsafspraken gemaakt. Voor de toepassingen die worden gebruikt in de hypotheek-processen van onze ketenpartners, de NHG Toets en het NHG Portaal, is een hoge beschikbaarheid vereist. Met de leveranciers van deze diensten worden SLA's afgesloten om het vereiste beschikbaarheidspercentage van 99,9% en de maximale oplostijd van 4 uur bij incidenten te realiseren.

HOOFDSTUK 2: CONCRETE MAATREGELEN

In de volgende twee paragrafen is een overzicht opgenomen van de voornaamste door NHG getroffen maatregelen.

Security
- De werkplek van alle NHG medewerkers, inclusief tijdelijke krachten en ingehuurd personeel, wordt beschermd door een firewall, antivirus en malware software die continu updates ontvangt van nieuwe kwaadaardige signatures. Het besturingssysteem wordt geautomatiseerd elke maand geüpdatet en securitypatches worden binnen uiterlijk 3 werkdagen geïnstalleerd. Daarnaast is de harddrive versleuteld en wordt de werkplek vergrendeld met pin of facial recognition. Toegang met de devices tot het netwerk is aanvullend afgeschermd met MFA. Door middel van mobile device management worden devices centraal beheerd en kunnen alleen in de netwerkomgeving komen als ze voldoen aan de beveiligingsvereisten. Als op een device vermoedelijk een virus of malware is gedetecteerd wordt onmiddellijk de toegang tot het netwerk ontnomen. De devices kunnen op afstand gewhiped worden.
- De mobiele telefoons van medewerkers en inhuurkrachten worden gekoppeld aan een account ter verificatie. Daarnaast worden de telefoons voorzien van anti-virus software en verplichte vergrendeling met pin. De devices kunnen op afstand gewhiped worden.

- Voor beheeraccounts zijn strengere maatregelen getroffen zoals MFA bij elk gebruik, logging van handelingen en beperking van de ingelogde periode. Alle beheer accounts zijn op naam en handelingen zijn traceerbaar.
- Toegang tot informatie is op basis van functieprofielen waarbij de principes 'Need to know' en 'Least privilege' zijn toegepast. De toegekende rechten worden beheerd in een matrix en periodiek gecontroleerd door de eigenaar van de data. Op betalingen en besluiten over kwijtschelding en declaraties wordt functiescheiding toegepast. Afhankelijk van het bedrag is dat door middel van het vier of zes ogen principe.
- IT-voorzieningen worden ingekocht waarbij gebruik wordt gemaakt van high-end TIER 3+ datacenters waarin alle technische en procedurele industrie standaarden worden ingezet rondom bescherming van apparatuur en bekabeling, klimaatbeheersing, brand detectie- en blussystemen, noodstroomvoorziening, fysieke barrières en stringente procedures voor toegang, bediening en wijziging. Systemen worden gemonitord en er zijn procedures actief voor het behandelen van incidenten en afwijkingen.
- NHG heeft geen legacy systemen en life cycle management, hardening en patching worden actief toegepast.
- Https-verbindingen zijn TLS1.2+ en scoren een A-niveau bij Qualys SSL Labs;
- E-mail wordt te allen tijde versleuteld verzonden en SPF, DKIM en DMARC zijn ingericht. Alle berichten en bijlagen die via e-mail worden ontvangen worden gescand op kwaadaardige signatures.
- De diensten die wij aanbieden aan onze ketenpartners worden minimaal eenmaal per jaar onderworpen aan een pentest en het ontwikkelplatform wordt gecontroleerd op secure coding;
- Bij de werving van nieuwe medewerkers is een Verklaring omtrent Gedrag verplicht, wordt minimaal 1 referentie gecontroleerd en wordt het relevante diploma geverifieerd. Nieuwe medewerkers en inhuurkrachten ondertekenen een gedragscode en worden gehouden de richtlijnen omtrent privacy en security na te leven;
- NHG stuurt actief op kennis en awareness door trainingen, workshops, simulaties en regelmatige berichtgeving over actuele dreigingen en hoe daarop te handelen;
- NHG heeft een vastgestelde procedure beveiligingsincidenten waarin is beschreven welke stappen moeten worden doorlopen om adequate opvolging te geven aan het incident. Afdichten, schade beperken, analyseren en leren voorkomen zijn hierin de leidende onderwerpen;
- Risico's op het gebied van security worden elke kwartaal besproken in het risk committee waarin een afgevaardigde van het management en het volledige bestuur van NHG zitting heeft.

Privacy
- De wettelijke grondslagen voor de verwerkingsactiviteiten zijn vastgelegd in het privacybeleid;
- Het privacybeleid is vertaald naar praktische richtlijnen voor medewerkers;
- Klanten worden geïnformeerd over de verwerking van persoonsgegevens in de privacyverklaring van NHG op www.nhg.nl/privacy. Daarnaast wordt de klant op alle logische plekken waarop persoonsgegevens worden gedeeld gewezen op die informatie. Nieuwe klanten ontvangen een welkomstbrief waarin wordt verwezen naar de

privacyverklaring. Ook in het bindend aanbod van de geldverstrekker wordt de klant gewezen op die verklaring;
- Sollicitanten en medewerkers worden geïnformeerd over de verwerkingsactiviteiten in respectievelijk de Privacyverklaring - solliciteren bij NHG en de Privacyverklaring – werken bij NHG.
- In bovengenoemde privacyverklaringen wordt de betrokkene geïnformeerd over de te volgen procedure voor het uitoefenen van diens rechten.
- NHG heeft een Beleid bewaar- en verwijdertermijnen waarin is vastgelegd hoe lang gegevens worden bewaard en na welke termijn gegevens worden verwijderd.
- Bij nieuwe processen en producten of wijzigingen daarin wordt een privacy impact analyse uitgevoerd;
- Alle verwerkingsactiviteiten zijn vastgelegd in het register verwerkingsactiviteiten;
- NHG heeft een vastgestelde procedure meldplicht datalekken waarin is beschreven welke stappen moeten worden doorlopen om adequate opvolging te geven aan het datalek en om tijdig aan de meldplicht te kunnen voldoen;
- Datalekken worden geadministreerd in een logboek waarin ook wordt vastgelegd wat de oorzaak van het incident is, welke maatregelen zijn getroffen ter afdichting en voorkoming, wat de aard van de persoonsgegevens is, de vermoedelijke gevolgen voor de verwerking en of sprake is van een melding aan de AP of de betrokkene;
- Er is een functionaris voor gegevensbescherming aangewezen die onafhankelijk toeziet op de naleving van de AVG;
- Gegevens worden opgeslagen binnen de Europese Unie. Alleen indien het onvermijdelijk is, bijvoorbeeld om incidenten te verhelpen, kan het zijn dat gegevens worden ingezien van buiten de EU. Voor die gevallen zijn overeenkomsten afgesloten waarin waarborgen zijn getroffen om te voldoen aan de AVG;
- Er is een procedure actief waarin is beschreven hoe gehandeld moet worden als een betrokkene diens recht op inzage, correctie, wissing, bezwaar of beperking uitoefent;
- Er wordt actief gewerkt aan datakwaliteit door maatregelen als invoervalidaties, beperking van rechten, beperking van handmatige invoer, ICT Architectuur, controles bij externe bronnen, rapportages en correcties;
- Met alle derden die persoonsgegevens verwerken is een verwerkersovereenkomst afgesloten;
- Bij uitwisseling van persoonsgegevens met derden die ook Verwerkingsverantwoordelijke zijn, zijn overeenkomsten afgesloten waarin soortgelijke waarborgen zijn opgenomen;
- Verdere verwerking voor andere doeleinden dan waarvoor de gegevens zijn verzameld wordt getoetst aan de vereisten van verenigbaarheid.
- Risico’s op het gebied van privacy worden elke kwartaal besproken in het risk committee waarin een afgevaardigde van het management en het volledige bestuur zitting heeft.
- Er wordt uitgebreide documentatie aangehouden om compliance met de AVG aan te tonen;