SECURITYSTATEMENT NHG

Inleiding
NHG beschikt over veel, en vaak gevoelige (persoons)gegevens. Een schending van de beschikbaarheid, integriteit of vertrouwelijkheid van deze gegevens, bijvoorbeeld door fraude of een informatielek, kan verstrekkende gevolgen hebben. Met een adequate set maatregelen doen we er alles aan om financiële- of imagoschade bij NHG en haar stakeholders of een inbreuk op het fundamentele recht op privacy van onze klanten te voorkomen. In dit document is beschreven hoe NHG invulling geeft aan informatiebeveiliging.

Kaders
Kaders worden gevormd door relevante wet- en regelgeving. Hierbij is met name de Algemene Verordening Gegevensbescherming (AVG) van belang. In de Privacyverklaring van NHG is te lezen hoe NHG invulling geeft aan privacy. NHG heeft een procedure datalekken geïmplementeerd waarin is geborgd dat maatregelen worden getroffen om de schade voor betrokkenen zoveel mogelijk te beperken en tijdig en juist kan worden voldaan aan de meldplicht.

ISO/IEC 27001
NHG heeft ervoor gekozen om informatiebeveiliging in te richten in overeenstemming met ISO/IEC27001. Daartoe is een security strategie en een security beleid 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. In de uitvoering van de risicoanalyse worden het bestuur en het gehele management gekend.

Stakeholders
Bij het bepalen van maatregelen houdt NHG rekening met specifieke belangen van haar stakeholders. Vooral de belangen van de ketenpartners (geldverstekkers, hun servicers en intermediairs) worden hierin gekend. Maar uiteraard 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. 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. Hierbij 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 online diensten 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 processen en de beheersmaatregelen die zijn ondernomen 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.

Security by design
NHG past Security by Design toe door te zorgen dat al in de ontwerpfase de juiste beveiligingsstandaarden worden opgelegd en borgt dat deze tot en met de beheerfase worden ingevuld. Bij grote ontwikkeltrajecten wordt, om dit te borgen, een Quality Control proces ingericht. In het design wordt eveneens aandacht besteedt aan aspecten als lyfecycle management, secure coding (OWASP), patchmanagement, hardening en monitoring.

Verwerkers
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 Security Agreement opgesteld waarin de vereisten zijn beschreven waar de leverancier aan dient te voldoen. In de regel zijn de partijen die NHG inzet gerenommeerde bedrijven die, vanuit het belang van hun concurrentiepositie, 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 voornaamste partijen waar NHG haar data onderbrengt zijn ISO-gecertificeerd. Uiteraard is met alle IT-leveranciers een Service Level Agreement overeengekomen. Het proces rondom het beheer van deze afspraken met leveranciers maakt onderdeel uit van de ISAE 3402 controle.

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, IPSec, Certificaten en redundante componenten ziet NHG als vanzelfsprekend.

Continuïteit
NHG heeft een Uitwijkplan. In dit plan 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 de verschillende IT-voorzieningen is (vanzelfsprekend) voorzien in back-up procedures en zijn relevante beschikbaarheidsafspraken gemaakt. De toepassingen die worden gebruikt in de hypotheek-processen van onze ketenpartners nemen we af met een beschikbaarheidspercentage van 99,9% en een maximale oplostijd van 4 uur bij incidenten.