COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

AAN Digi-d v.o.f.
T.a.v.

DATUM 21 juli 2015
ONS KENMERK z2014-00185
CONTACTPERSOON

UW BRIEF VAN -
UW KENMERK -

ONDERWERP Handhavingsverzoek Digi-d

Geachte ,

Bij brief van 5 maart 2014 heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties aan het College bescherming persoonsgegevens (hierna: het CBP) verzocht om een onderzoek in te stellen naar de handelswijze van uw reclamebureau Digi-d bij het opslaan en verspreiden van persoonsgegevens van burgers en heeft het Ministerie verzocht om daartegen handhavend op te treden.

Bij brief van 9 maart 2015 heeft u een brief van het CBP ontvangen met daarin de tussentijdse resultaten van dit onderzoek. Middels de onderhavige brief informeert het CBP u over de definitieve resultaten van het onderzoek en haar conclusie. Volledigheidshalve zal hierna eerst de inhoud van het handhavingsverzoek en het verloop van het onderzoek worden weergegeven.

Inhoud verzoek en verloop onderzoek
In zijn verzoek heeft het Ministerie gesteld dat het volgens Digi-d veelvuldig voorkomt dat burgers abusievelijk inloggen op de site van Digi-d in de veronderstelling dat zij van doen hebben met de overheidsvoorziening voor authenticatie DigiD (hierna: DigiD). Daarbij zouden zij hun inloggegevens (gebruikersnaam en wachtwoord) op de site van Digi-d achterlaten. Uw reclamebureau zou deze gegevens vervolgens opslaan en de vertrouwelijkheid van deze gegevens zou niet gewaarborgd zijn, aldus het Ministerie. Daarnaast zouden er signalen zijn dat Digi-d persoonsgegevens ook breder heeft verspreid. Aangezien het Ministerie het niet verantwoord achtte om een en ander verder te laten voortduren, heeft het zich tot het CBP gewend. Het verzoek is niet onderbouwd met voorbeelden dan wel bewijsstukken.

Actieve DigiD-gebruikersnamen in combinatie met -wachtwoorden zijn persoonsgegevens als bedoeld in artikel 1, sub a van de Wet bescherming persoonsgegevens (hierna: Wbp) omdat deze direct herleidbaar zijn tot een individuele persoon.

Op 26 juni 2014 heeft het CBP tijdens een onderzoek ter plaatse van het kantoor van Digi-d aan de te de beschikking gekregen over een bestand met 38.621 inloggegevens dat zich heeft opgebouwd sinds Digi-d die gegevens klaarblijkelijk ging opslaan.

BIJLAGEN

Ten einde vast te kunnen stellen of zich in dit door Digi-d ter beschikking gestelde bestand actieve DigiD-gebruikersnamen en -wachtwoorden bevinden, heeft het CBP in zijn brief van 25 september 2014 aan Digi-d aangekondigd Logius te zullen inschakelen. Daarbij heeft het CBP aangegeven dat de inzet van Logius noodzakelijk is aangezien het CBP zelf niet in staat is om na te gaan wat DigiD-inloggegevens zijn. Tevens heeft het CBP in deze brief aangegeven de noodzakelijke beveiligingsmaatregelen te zullen treffen teneinde de vertrouwelijkheid van de voor Digi-d bestemde gegevens bij de bestandsvergelijking te garanderen.

Per fax van 26 september 2014 heeft Digi-d aangegeven bezwaar te hebben tegen het verstrekken van het bestand aan Logius.

Per brief van 9 oktober 2014 heeft het CBP nogmaals toegelicht dat, kort gezegd, het CBP op basis van eigen onderzoek zal moeten vaststellen of zich DigiD- inloggegevens in het bestand bevinden. Een verdere reactie van Digi-d op deze brief is uitgebleven.

In oktober 2014 heeft Logius op verzoek van het CBP een bestandsvergelijking uitgevoerd. Uit die vergelijking is gebleken dat er sprake is van **23.482** uniek herkenbare gebruikersnamen. Van de 23.482 unieke gebruikersnamen is van **12.746** vastgesteld dat het gaat om actieve DigiD-gebruikersnamen. Van deze 12.746 actieve DigiD gebruikersnamen was van **6.757** accounts tevens het DigiD-wachtwoord beschikbaar.

Ten aanzien van die actieve DigiD-inloggegevens heeft Logius per 14 januari 2015 de accounts geblokkeerd en betrokkenen daarover bij brief geïnformeerd, waardoor het veiligheidsrisico ten aanzien van deze gegevens is weggenomen. In dit door Digi-d ter beschikking gestelde bestand bevinden zich geen actieve DigiD-gebruikersnamen en -wachtwoorden meer.

Bij brief van 9 maart 2015 heeft het CBP aan Digi-d bericht dat door het loggen van de combinatie van DigiD-gebruikersnamen en -wachtwoorden door Digi-d geen sprake is van een passend beveiligingsniveau als bedoeld in artikel 13 Wbp en is Digi-d verzocht maatregelen te treffen. Daarbij is Digi-d in de gelegenheid gesteld zijn zienswijze kenbaar te maken.

Digi-d heeft bij brief van 20 maart 2015 zijn zienswijze aan het CBP gestuurd. Daarin heeft Digi-d, samengevat weergegeven, omschreven op welke wijze DigiD-gebruikersnamen en -wachtwoorden bij haar binnenkomen en heeft zij maatregelen omschreven die zij heeft getroffen dan wel wil gaan treffen om te voorkomen dat zij in overtreding is van artikel 13 Wbp.

Op 23 juni jl. heeft het CBP tijdens een tweede onderzoek ter plaatse bij het kantoor van Digi-d geconstateerd dat Digi-d vanaf 18 juni 2015 niet langer de wachtwoorden logt van de inlogpogingen die op haar website plaatsvinden. Verder heeft het CBP daarbij de beschikking gekregen over een kopie van het bestand met inloggegevens met als doel te constateren of en in hoeverre sinds de datum van haar eerste onderzoek ter plaatse (26 juni 2014) opnieuw inlogpogingen zijn gedaan met DigiD-inloggegevens.

Logius heeft ten aanzien van dit bestand dezelfde bestandsvergelijking uitgevoerd als zij deed ten aanzien van het eerste bestand. Uit die bestandsvergelijking is gebleken dat in de periode tot en met 17 juni 2015 van **1.764** DigiD-accounts zowel de gebruikersnamen als wachtwoorden aanwezig waren. Vervolgens heeft Logius op dezelfde wijze als bij het eerste bestand deze DigiD-accounts geblokkeerd en betrokkenen daarover geïnformeerd.

Conclusie
Het CBP heeft zich in haar onderzoek gericht op de vraag of in de bestaande en toekomstige bedrijfsvoering van Digi-d veiligheidsrisico's voor betrokkenen (DigiD-gebruikers) zijn weggenomen en afdoende worden voorkomen.

Concluderend stelt het CBP dat ten aanzien van de kopieën van bestanden waarover zij in het kader van haar onderzoek de beschikking heeft gekregen het veiligheidsrisico is weggenomen doordat Logius de DigiD-accounts, waarvan zowel gebruikersnamen als -wachtwoorden in het bestand aanwezig waren, heeft geblokkeerd. Dit heeft betrekking op de periode tot en met 17 juni 2015. Digi-d is verder, door sinds 18 juni 2015 geen wachtwoorden meer te loggen, niet langer in overtreding van artikel 13 van de Wbp.

Ten aanzien van mogelijk andere overtredingen van de Wbp waarop het Ministerie in zijn verzoek heeft gewezen, merkt het CBP het volgende op. Inactieve DigiD-inloggegevens - inloggegevens waarvan de accounts zijn geblokkeerd - zijn niet te kwalificeren als persoonsgegevens in de zin van artikel 1, onder a, van de Wbp. Het bewaren van het bestaande bestand met inactieve (DigiD-) inloggegevens door Digi-d vormt daarom geen overtreding van de Wbp. Van de door het Ministerie gestelde, maar niet nader onderbouwde, verspreiding van DigiD-inloggegevens door Digi-d is het CBP niet gebleken.

Dat Digi-d inloggegevens van burgers binnen blijft krijgen die in de veronderstelling zijn met de overheidsvoorziening DigiD van doen te hebben - en dit ook op andere manieren dan via inlogpogingen op haar website gebeurt, zoals bijvoorbeeld via het statistiekenprogramma en het e-mailadres - kan niet voorkomen worden zo lang de naamsverwarring tussen Digi-d en DigiD blijft bestaan. Daarbij is ook van belang dat Digi-d in het merendeel van de gevallen niet kan vaststellen of die gegevens voor haar bedoeld zijn of DigiD-inloggegevens bevatten. In zoverre kunnen dus ook geen andere of aanvullende maatregelen aan Digi-d worden opgelegd die erop neer zouden komen dat Digi-d bepaalde gegevens moet verwijderen.

De oplossing voor de feitelijke situatie waarin de naamsverwarring centraal staat, ligt bij partijen.

Gelijktijdig met deze brief stuurt het CBP een - bijna gelijkluidende - brief aan het Ministerie inzake de afhandeling van het handhavingsverzoek, waarvan een afschrift is bijgevoegd. Zoals eerder aan u meegedeeld in de brief van 9 maart 2015 heeft het CBP het voornemen deze brief - en de brief gericht aan het Ministerie - openbaar te maken. U heeft in uw reactie van 20 maart 2015 aangegeven daartegen geen bezwaar te hebben indien uw standpunten hierin zijn weergegeven. Volledigheidshalve stel ik u daarom tot 6 augustus in de gelegenheid om aan te

geven of u zich in openbaarmaking van deze brief kunt vinden. Het CBP beslist vervolgens met inachtneming van uw zienswijze of de brief openbaar wordt gemaakt. Hiervan ontvangt u schriftelijk bericht.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Namens het College bescherming persoonsgegevens,

Mr. A.B. Commandeur
Hoofd afdeling Toezicht sector Publiek