Autoriteit Persoonsgegevens
Postbus 93374, 2509 AJ Den Haag
T 070 8888 500
autoriteitpersoonsgegevens.nl

Vertrouwelijk/Aangetekend
Stichting Hogeschool van Arnhem en Nijmegen
T.a.v. het college van bestuur
Ruitenberglaan 31
6826 CC ARNHEM

## Datum
15 december 2025

## Ons kenmerk
2024-024797

## Contactpersoon
[VERTROUWELIJK]
070 8888 500

## Onderwerp
Besluit tot oplegging van een bestuurlijke boete

Geacht college van bestuur,

De Autoriteit Persoonsgegevens (hierna: AP) heeft onderzoek gedaan naar de door de Stichting Hogeschool van Arnhem en Nijmegen (hierna: de HAN) getroffen technische en organisatorische maatregelen ter beveiliging van de door de HAN verwerkte persoonsgegevens. De AP stelt op basis van dat onderzoek vast dat de HAN onvoldoende technische en organisatorische maatregelen heeft getroffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Daarmee heeft de HAN niet voldaan aan de voorwaarden van artikel 32 van de Algemene verordening gegevensbescherming (hierna: AVG).

De AP besluit om handhavend op te treden tegen de HAN, omdat de HAN met de geconstateerde overtreding het risico heeft genomen dat een inbreuk zou plaatsvinden op de persoonsgegevens van studenten, medewerkers en derden. Dit risico is niet slechts theoretisch gebleken, maar heeft zich ook daadwerkelijk voorgedaan. De AP vindt dit ernstig en acht het daarom noodzakelijk en passend om de HAN een bestuurlijke boete op te leggen van € 175.000,00.

In dit besluit worden de overtreding en de bestuurlijke boete toegelicht. Allereerst wordt ingegaan op de aanleiding en omvang van het onderzoek (paragraaf 1). Daarna wordt toegelicht welke overtreding de AP heeft geconstateerd (paragraaf 2) en wordt ingegaan op de reactie van de HAN (paragraaf 3). Vervolgens wordt de boetehoogte toegelicht (paragraaf 4) en volgt het dictum (paragraaf 5). Tot slot is vermeld wat een belanghebbende kan doen indien deze zich niet kan vinden in dit besluit.

Datum
15 december 2025

Ons kenmerk
2024-024797

## 1. Aanleiding en omvang van het onderzoek

Op 1 september 2021 heeft de HAN bij de AP melding gedaan van een datalek. Een hacker heeft contact opgenomen met de voorzitter van het college van bestuur van de HAN, omdat hij onrechtmatig in het bezit is gekomen van persoonsgegevens. De hacker heeft losgeld geëist voor een discrete afhandeling (vier Bitcoin, die op dat moment een waarde van in totaal circa € 165.000 vertegenwoordigden) in plaats van de persoonsgegevens te verspreiden en de pers te informeren.

De HAN heeft op diezelfde dag contact opgenomen met een adviesbureau voor digitale forensische expertise. Dit adviesbureau heeft onderzoek gedaan naar de inbreuk en heeft de bevindingen vastgelegd. Uit de bevindingen volgt dat de hacker gebruik heeft gemaakt van zogenoemde SQL-injectie via een webformulier.[1] De HAN heeft in vier aanvullingen op de datalekmelding bij de AP verklaard dat de gelekte gegevens afkomstig zijn van een databaseserver die meerdere databases omvat. Het aantal gegevensrecords is gaandeweg bijgesteld naar enkele honderdduizenden records.[2] Uit een door de HAN opgesteld overzicht van de persoonsgegevens op de databaseserver, blijkt onder meer het volgende:

- 95% van de records betrof algemene persoonsgegevens (NAW, en in ongeveer 1% van de gevallen binnen deze groep, ook een pasfoto);
- 2% van de records betrof gevoelige gegevens (NAW in combinatie met een wachtwoord, CV of andere bijlage);
- 1% van de records betrof bijzondere persoonsgegevens (veelal medische gegevens met betrekking tot studievoorzieningen en/of -voortgang, maar ook de gegevens van een enquête waarbij om politieke voorkeur werd gevraagd);
- de databaseserver bevatte tot slot 407 burgerservicenummers en 183 documentnummers van legitimatiebewijzen.

De HAN is niet ingegaan op de losgeldeis. De hacker is uiteindelijk bij vonnis van de rechtbank Amsterdam van 3 november 2023 veroordeeld voor – onder meer– het verwerven en voorhanden hebben van de ontvreemde persoonsgegevens.[3]

Een datalek valt zelfs met de beste beveiliging nooit volledig uit te sluiten en vormt op zichzelf dan ook geen overtreding van de AVG. In dit geval heeft de AP in het incident en de bevindingen van het forensisch rapport dat de HAN heeft laten opstellen, aanleiding gezien om een onderzoek te starten naar de beveiligingsmaatregelen die de HAN voorafgaand aan het incident heeft getroffen. Op grond van artikel 32 van de AVG is de verwerkingsverantwoordelijke die persoonsgegevens verwerkt, namelijk verplicht om (samengevat) alle beveiligingsmaatregelen te treffen die in redelijkheid kunnen worden gevergd. De AP heeft dus geen onderzoek gedaan naar het datalek zelf, maar naar de vraag of de HAN de verwerking van

[1] SQL-injectie is een aanvalstechniek waarbij een aanvaller kwaadaardige SQL-code invoegt in formuliervelden of URL-parameters, zodat de database onbedoelde opdrachten uitvoert.
[2] Het aantal gegevensrecords (rijen informatie) moet worden onderscheiden van het aantal betrokkenen (personen). Van betrokkenen bestaan in de regel meerdere gegevensrecords.
[3] Uitspraak van de rechtbank Amsterdam van 3 november 2023 (ECLI:NL:RBAMS:2023:6967).

persoonsgegevens op de web- en databaseserver adequaat heeft beveiligd. De bevindingen zijn neergelegd in een onderzoeksrapport van 20 augustus 2024. Daaruit blijkt het volgende.

## 2. Geconstateerde overtreding

De HAN is op grond van artikel 32 van de AVG gehouden om, rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, passende technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Uit deze verplichting volgt dat de volgende stappen moeten worden doorlopen:

1) de aan de verwerking inherente risico's voor de rechten en vrijheden van personen moeten worden geïnventariseerd;

2) de risico's moeten worden beoordeeld op de waarschijnlijkheid van het optreden ervan en de ernst van de nadelige gevolgen voor de betrokken personen;

3) er moeten maatregelen worden getroffen waarmee deze risico's kunnen worden beperkt, zodat er een op het risico afgestemd beveiligingsniveau ontstaat;

4) het hiervoor bedoelde beveiligingsniveau moet worden gewaarborgd.

Uit onderzoek van de AP volgt dat de HAN in de periode voorafgaand aan 2021 beschikte over informatiebeveiligingsbeleid. Ten aanzien van de door de AP onderzochte webserver en databaseserver is evenwel komen vast te staan dat de HAN niet alle hiervoor vermelde stappen heeft doorlopen en daardoor niet een op het risico afgestemd beveiligingsniveau heeft gewaarborgd. Daardoor heeft de HAN artikel 32 van de AVG overtreden. Daarbij neemt de AP het volgende in aanmerking.

### 1. Onvoldoende maatregelen tegen SQL-injectie

De HAN is zich ten aanzien van het voorkomen en gaandeweg bestrijden van SQL-injectie bewust geweest van het risico van SQL-injectie (stap 1). De HAN heeft ten tijde van belang echter de ernst van het risico niet voldoende beoordeeld (stap 2) en heeft daardoor onvoldoende maatregelen getroffen om dat risico te beperken (stap 3). Daardoor is evenmin een op het risico afgestemd beveiligingsniveau gewaarborgd (stap 4). Dat volgt, samengevat weergegeven, uit het volgende.

Uit de onderzochte programmacode van de bij het datalek betrokken applicatie blijkt dat er ten tijde van belang weliswaar *enige* aandacht was voor SQL-injectie, maar dat dit niet consequent het geval was. De HAN heeft vervolgens desgevraagd aan de AP verklaard dat haar programmeurs zich bewust waren van het risico van SQL-injectie en dat daarover een zogenoemd *best practices* beleid bestond. De HAN kan echter niet reproduceren of bij het maken van het specifieke formulier dat de hacker heeft gebruikt voor het

datalek een risicoanalyse is gemaakt en of het *best practices* beleid toen is toegepast. De HAN heeft het beleid ook niet overgelegd aan de AP.

De AP concludeert verder dat de logging en monitoring op databaseserver Robin te beperkt was. Uitsluitend queries die aan bepaalde criteria voldeden, werden door de server gelogd. Bijvoorbeeld als een query lang duurt, of een groot aantal rijen bevraagt. Door deze beperkte logging, maar óók door een beperkte monitoring van de gegevens die wél werden gelogd, is door de HAN niet gedetecteerd dat sprake was van SQL-injectie, laat staan welke gegevens gestolen zijn. Een toezichthouder van de AP heeft kunnen vaststellen dat er twee keer eerder sprake was van SQL-injectie, terwijl de HAN dat zelf níet heeft opgemerkt.

2. Het niet beperken van toegangsrechten van database-gebruiker

De HAN heeft het risico op onbevoegde toegang door niet-noodzakelijke toegangsrechten geïnventariseerd en beoordeeld (stappen 1 en 2). De HAN had echter geen maatregelen getroffen om dit risico in de praktijk te beperken (stap 3) en had daarmee evenmin een op het risico afgestemd beveiligingsniveau gewaarborgd (stap 4). Dat blijkt uit het volgende.

Het beveiligingsbeleid van de HAN bevatte ten tijde van belang het zogenaamde *least privilege*-beginsel, dat voorschrijft dat de toegang tot informatie en/of faciliteiten wordt beperkt tot het strikt noodzakelijke. Dit minimaliseert het aanvalsoppervlak van kwaadwillenden, beperkt potentiële schade door fouten of malafide acties, en verkleint de kans op datalekken.

Het *least privilege*-beginsel is in de praktijk echter niet toegepast op de databaseserver: de gebruiker “dbroxen” had alle toegangsrechten voor de gehele databaseserver Robin, terwijl daarvoor geen rechtvaardiging bestond. Daardoor kon een kwetsbaarheid in één applicatie leiden tot toegang tot alle databases (282 databases, waarvan er 94 persoonsgegevens bevatten).

3. Het onnodig bewaren van persoonsgegevens van uitgefaseerde applicaties

De HAN was zich bewust van het risico op het onnodig bewaren van persoonsgegevens (stap 1) en heeft de risico’s daarvan geïnventariseerd (stap 2). Er waren echter onvoldoende maatregelen getroffen om de risico’s te beperken (stap 3) waardoor geen op het risico afgestemd beveiligingsniveau is gewaarborgd (stap 4). Dat volgt uit het volgende.

De HAN beschikte over een verwijderingsbeleid, waaruit kan worden opgemaakt dat het risico op het onnodig bewaren van persoonsgegevens is onderkend. Het opstellen van verwijderbeleid is een eerste maatregel om dat risico te adresseren, maar vergt wel dat het beleid ook daadwerkelijk wordt geïmplementeerd en periodiek wordt uitgevoerd. Dat is ten aanzien van de gegevens op databaseserver Robin niet het geval gebleken. Door het ontbreken van een adequaat proces voor gegevensverwijdering is het verwijderingsbeleid niet uitgevoerd en is onnodig het risico ontstaan dat zich een inbreuk op deze gegevens zou voordoen. De HAN was er ook niet mee bekend dat zich persoonsgegevens op deze databaseserver bevonden van applicaties die al lange tijd waren uitgefaseerd (een zogenaamde *data graveyard*).

4. Het niet en niet-toereikend hashen van wachtwoorden

Op databaseserver Robin waren 4.381 wachtwoorden opgeslagen in platte tekst, zonder enige versleuteling. Daarnaast waren er 5.194 wachtwoorden opgeslagen die zijn gehasht met de MD5- en SHA1-algoritmen. Deze worden sinds 2004 (MD5) en 2017 (SHA1) als onveilig beschouwd door bewezen botsingen die de cryptografische betrouwbaarheid van de algoritmen ondermijnen. De wachtwoorden waren afkomstig uit uitgefaseerde applicaties waarvan bij de HAN niet bekend was dat de gegevens nog werden bewaard, zodat dit punt samenhangt met het voorgaande punt (het onnodig bewaren van persoonsgegevens van uitgefaseerde applicaties).

Inmiddels gebruikt de HAN een SSO-proces (Single Sign-On; centrale opslag van accountgegevens) om gebruikers in te loggen op verschillende platforms. Hierdoor bevatten databases van applicaties dus geen inloggegevens meer. De HAN heeft in dat kader gesteld dat de MD5- en SHA1-algoritmen ten tijde van de ontwikkeling van de uitgefaseerde applicaties nog wél voldeden. De AP kan de juistheid van die stelling niet meer controleren. Ook als de stelling juist zou zijn, geldt evenwel dat de HAN – of zij nu wel of geen wetenschap had van de voortdurende verwerking van de gegevens – verplicht was om de risico-inventarisatie door de tijd heen te actualiseren.

Gelet op het voorgaande heeft de HAN in het verleden in ieder geval onvoldoende maatregelen getroffen om de wachtwoorden voldoende te blijven beveiligen (stap 3), zodat ook op dit punt geen op het risico afgestemd beveiligingsniveau was gewaarborgd (stap 4).

### Tot slot

De bevindingen van de AP tonen aan dat adequate beveiliging geen kwestie is van op zichzelf staande risico's en maatregelen. In dit geval heeft juist de samenhang van de vermelde problemen bijgedragen aan de substantiële omvang van het incident. Als een van de genoemde risico's zich niet had verwezenlijkt doordat afdoende maatregelen waren getroffen, dan hadden de daaropvolgende risico's zich ook niet kunnen verwezenlijken.

## 3. Reactie van de HAN op de geconstateerde overtreding

De HAN heeft tegenover de AP erkend dat zij in haar hoedanigheid van verwerkingsverantwoordelijke verantwoordelijk is voor het waarborgen van een op het risico afgestemd beveiligingsniveau, en dat zij daarin tekort is geschoten gelet op de conclusies in het onderzoeksrapport, zoals hierboven weergegeven. De HAN heeft verder verklaard dat de overtreding van artikel 32 van de AVG haar kan worden toegerekend en verweten. Tijdens en na het onderzoek heeft de HAN ten aanzien van de hierboven geconstateerde tekortkomingen, aan de AP toegelicht welke herstelacties zij heeft uitgevoerd om de geconstateerde tekortkomingen te verhelpen en de overtreding aldus te beëindigen.

## 4. Bestuurlijke boete

De AP ziet aanleiding om gebruik te maken van haar bevoegdheid tot het opleggen van een bestuurlijke boete. Bij de uitoefening van deze bevoegdheid hanteert de AP ten aanzien van overheden de Boetebeleidsregels Autoriteit Persoonsgegevens 2019 (hierna: Boetebeleidsregels 2019).[4] De HAN is een bekostigde instelling voor hoger onderwijs en geldt uit dien hoofde voor de toepassing van het beleid als overheidsinstantie.

### 4.1. Boetecategorie en basisboete

In het onderzoeksrapport is een overtreding geconstateerd van artikel 32 van de AVG. In bijlage I bij de Boetebeleidsregels 2019 is dat aangemerkt als een overtreding van categorie II. Op grond van artikel 2.3 van de Boetebeleidsregels 2019 loopt de bandbreedte voor die categorie van € 120.000 tot € 500.000 en bedraagt de basisboete € 310.000. Vervolgens moet worden beoordeeld of er aanleiding bestaat om de boete hoger of lager vast te stellen dan de basisboete.

### 4.2. Relevante omstandigheden

Volgens de systematiek van de Boetebeleidsregels 2019 wordt de boete, binnen de van toepassing zijnde bandbreedte, hoger of lager vastgesteld dan de basisboete voor zover de factoren vermeld in artikel 83, tweede lid, van de AVG daartoe aanleiding geven. De onderdelen van artikel 83, tweede lid, van de AVG die in het hierna volgende niet worden besproken, missen in dit geval toepassing.

Factor c) de door de verwerkingsverantwoordelijke of de verwerker genomen maatregelen om de door betrokkenen geleden schade te beperken

Zoals vermeld in paragraaf 1 van dit besluit, dienen het datalek en de tekortkomingen in de beveiliging van elkaar te worden onderscheiden. Ook indien zich geen datalek had voorgedaan, zijn de in paragraaf 2 beschreven tekortkomingen een overtreding van artikel 32 van de AVG. Het datalek is echter wel een gevolg van de overtreding, zodat het datalek voor de beoordeling van deze factor in feitelijk opzicht wél relevant is.

De AP neemt allereerst in aanmerking dat de HAN op het moment dat zij bekend raakte met het datalek, de betrokken databaseserver direct heeft losgekoppeld en interne en externe expertise heeft ingeschakeld om de toedracht en omvang van het incident te bepalen. Mede daardoor heeft de HAN op relatief korte termijn het meest prangende probleem (de mogelijkheid van SQL-injectie) geïdentificeerd en gerepareerd.

Vervolgens heeft de HAN bij het onderzoek naar de vraag welke categorieën van persoonsgegevens bij het

[4] De Boetebeleidsregels 2019 zijn opgevolgd door de Boetebeleidsregels 2023. Het uitgangspunt is echter dat de beleidsregels moeten worden toegepast die golden ten tijde van de overtreding, tenzij latere beleidsregels gunstiger zouden uitpakken voor de overtreder. De Boetebeleidsregels 2023 bevatten geen voor de HAN gunstigere bepalingen, zodat de Boetebeleidsregels 2019 worden toegepast.

incident zijn betrokken, het principe toegepast van “bij twijfel ruim uitleggen”. Daardoor zijn bijvoorbeeld persoonsgegevens die op zichzelf wellicht níet gelden als bijzondere persoonsgegevens, wel als zodanig behandeld. Door deze ruime classificatie is brede toepassing gegeven aan het melden van de inbreuk aan betrokkenen in verband met een hoog risico voor de rechten en vrijheden van betrokkenen. De HAN heeft er verder op gewezen dat zij bij bepaalde categorieën van betrokkenen, direct een financiële vergoeding heeft aangeboden om een nieuw identiteitsbewijs aan te vragen. Hierdoor is het risico gemitigeerd op identiteitsfraude door openbaar geworden persoonsgegevens zoals documentnummers.

Concluderend stelt de AP vast dat de HAN zich actief heeft ingezet om de gevolgen voor betrokkenen in kaart te brengen, de kwalificaties daarvan ruim op te vatten en de gevolgen waar mogelijk weg te nemen. Deze omstandigheden leiden tot matiging van de basisboete.

### Factor k) elke andere op de omstandigheden van de zaak toepasselijke verzwarende of verzachtende factor

Reeds gestart project over informatiebeveiliging

Op het moment dat het datalek zich voordeed, stond de HAN op het punt te beginnen aan het project ‘*Versterken Informatiebeveiliging en Privacy*’. In dat project werd gewerkt aan een vernieuwde versie van het informatiebeveiligingsbeleid, gebaseerd op Model Informatiebeveiligingsbeleid SCIPR (SURF Community voor Informatiebeveiliging en Privacy) en aan de implementatie van de maatregelen die uit dat nieuwe beleid voortvloeiden. Hiermee beoogde de HAN om te komen tot een verbeterde digitale weerbaarheid en een hoger volwassenheidsniveau.

De AP maakt hieruit op dat de HAN ten tijde van belang weliswaar onvoldoende maatregelen heeft getroffen om een op het risico afgestemd beveiligingsniveau te waarborgen, maar in diezelfde periode bezig was om het beveiligingsniveau naar een hoger niveau te tillen. Met deze omstandigheid dient rekening te worden gehouden bij het bepalen van de uiteindelijke boetehoogte.

Actieve voorlichting aan andere organisaties

De HAN heeft verder tegenover de AP verklaard dat zij de kennis en ervaringen rond het incident niet alleen intern onder de aandacht heeft gebracht, met lezingen en workshops, maar vanuit haar maatschappelijke rol als kennisinstituut ook bij verschillende externe aangelegenheden heeft gedeeld. Daarbij wijst de HAN op de SURF Security- en Privacyconferentie (2022), een seminar in het kader van vijf jaar AVG (2023), een evenement bij een landelijke energieleverancier (2025) en bij een grootbank. De HAN heeft de AP toegezegd om ook in 2026 een evenement te organiseren over de in artikel 32 van de AVG bedoelde maatregelen en de feitelijke en organisatorische gevolgen die zich bij de HAN hebben voorgedaan als gevolg van de geconstateerde overtreding. De HAN hoopt dat het open delen van ervaringen, incidenten bij andere organisaties helpt te voorkomen.

De AP constateert dat de HAN aantoonbare inspanningen heeft verricht en blijft verrichten om de beveiliging van verwerkingen van persoonsgegevens bij anderen onder de aandacht te brengen, en hen

lering te laten trekken uit de gebeurtenissen bij de HAN zelf. Ook met deze omstandigheid dient rekening te worden gehouden bij het bepalen van de uiteindelijke boetehoogte.

### 4.3. Boetehoogte

Gelet op enerzijds de in paragraaf 4.1 vermelde basisboete van € 310.000,00 en anderzijds op de in paragraaf 4.2 vermelde omstandigheden, dient de boete lager te worden vastgesteld dan de basisboete. De AP acht een boete van € 175.000,00 passend en geboden. Een boete van dit bedrag voldoet, gelet op de geconstateerde overtreding en de besproken omstandigheden, aan de vereisten van doeltreffendheid, evenredigheid en afschrikkendheid.

## 5. Besluit

De Autoriteit Persoonsgegevens legt aan de Stichting Hogeschool van Arnhem en Nijmegen een bestuurlijke boete op van € 175.000,00 (zegge: honderdvijfenzeventigduizend euro) voor het overtreden van artikel 32 van de AVG.[5]

Hoogachtend,
Autoriteit Persoonsgegevens

*w.g.*

mr. A. Wolfsen
voorzitter

**Rechtsmiddelenclausule**
Indien een belanghebbende het niet eens is met dit besluit, kan deze binnen zes weken na de datum van verzending van het besluit digitaal of op papier een bezwaarschrift indienen bij de AP. Ingevolge artikel 38 van de Uitvoeringswet AVG schort het indienen van een bezwaarschrift de werking van de beschikking tot oplegging van de bestuurlijke boete op. De AP zal pas tot invordering overgaan, nadat het besluit onherroepelijk is geworden.

Voor het digitaal indienen van bezwaar, zie https://www.autoriteitpersoonsgegevens.nl, onder het kopje Contact, blokje “Bezwaar of ontevreden over de AP”.[6] Het adres voor het indienen op papier is Autoriteit Persoonsgegevens, Postbus 93374, 2509 AJ DEN HAAG.

[5] De AP zal de invordering uit handen geven aan het Centraal Justitieel Incassobureau (CJIB).
[6] Of ga direct naar <https://www.autoriteitpersoonsgegevens.nl/contact/bezwaar-maken>.