# ANS04 Fraudeonderzoek

(laatste update(controle): 13-03-2023)

## Verwerking

| | | |
|---|---|---|
| *Registratienummer* | ANS04 | |
| *Naam verwerking* | Onderzoek naar mogelijke fraude | |
| *Verantwoordelijke* | Ansvar Verzekeringen | |
| | Coengebouw<br>Kabelweg 37<br>1014 BA Amsterdam | Postbus 90386<br>1006 BJ Amsterdam<br>Nederland |
| *Intern verantwoordelijke* | Manager Volmacht- & Fraudebeheersing | |
| *Doel(en) van verwerking* | 1. Het ondersteunen van activiteiten gericht op het waarborgen van de veiligheid en de integriteit van de financiële sector, daaronder mede begrepen (het geheel van) activiteiten die gericht zijn op:<br>- het onderkennen, voorkomen, onderzoeken en bestrijden van gedragingen die kunnen leiden tot benadeling van de branche waar de financiële onderneming / verzekeraar deel van uitmaakt, van de economische eenheid (groep) waartoe de financiële onderneming / verzekeraar behoort, van de financiële onderneming zelf, alsmede van haar cliënten en medewerkers;<br>- Het onderkennen, voorkomen, onderzoeken en bestrijden van oneigenlijk gebruik van producten, diensten en voorzieningen gericht tegen de branche waar de financiële onderneming / verzekeraar deel van uitmaakt, de financiële onderneming / het concern zelf.<br>- Het onderkennen, voorkomen, onderzoeken en bestrijden van (pogingen) tot strafbare of laakbare gedragingen gericht tegen de branche waar de financiële onderneming deel van uitmaakt, de financiële onderneming / het concern zelf.<br>- Het gebruik van een intern waarschuwingssystemen. | |
| *Grondslag(en) van verwerking* | - De betrokkene heeft voor de verwerking zijn ondubbelzinnige toestemming verleend.<br>- De gegevensverwerking is noodzakelijk om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is.<br>- De gegevensverwerking is noodzakelijk ter vrijwaring van een vitaal belang van de betrokkene.<br>- De gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt | |

## Betrokkene(n)

| Hoedanigheid betrokkene | Categorieën van persoonsgegevens | Aard persoonsgegevens |
|---|---|---|
| *(rechts)personen, indien er sprake is van een gerede aanleiding, een en ander met inachtneming van de doeleinden* | Kenmerken van het incident | Algemeen |
| | NAW-gegevens | Algemeen |
| | Bedrijfsgegevens | Algemeen |
| | Geboortedatum | Algemeen |
| | Geslacht | Algemeen |
| | Polisnummer en polisgegevens | Algemeen |
| | Cliëntnummer | Algemeen |
| | Werkgeversgegevens (collectiviteit) | Algemeen |
| | Bankrekeningnummer en betaalgegevens | Gevoelig |
| | Voor identificatie en communicatie benodigde gegevens | Algemeen |
| | Acceptatie- en polisgegevens | Algemeen |
| | Schadegegevens | Algemeen |
| | Resultaat van het fraudeonderzoek | Gevoelig |
| | Maatregelen die naar aanleiding van het onderzoek zijn genomen | Gevoelig |
| | Indicatie of opname in het externe verwijzingsregister heeft plaatsgevonden | Gevoelig |
| | Gegevens over handelingen die op verzoek aan betrokkene hebben plaatsgevonden | Gevoelig |
| | Op het incident betrekking hebbende gegevensdragers zoals foto's, video geluidsdragers | Gevoelig |
| | Gegevens betreffende de gezondheid | Bijzonder |
| | Strafrechtelijke gegevens | Bijzonder |
| | Gegevens inzake onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag | Bijzonder |
| Hoedanigheid betrokkene | Categorieën van persoonsgegevens | Aard persoonsgegevens |
| *personen die gelieerd zijn aan de bij de eerste categorie van betrokken genoemde personen, zoals advocaten, partners, medeverdachten* | NAW-gegevens | Algemeen |
| | Bedrijfsnaam | Algemeen |
| | Telefoon, fax, e-mail | Algemeen |

| | | |
|---|---|---|
| | Polisnummer en polisgegevens | Algemeen |
| | Geslacht | Algemeen |
| | Voor identificatie en communicatie benodigde gegevens | Algemeen |
| | Gegevens over handelingen die op verzoek aan betrokkene hebben plaatsgevonden | Gevoelig |
| | Op het incident betrekking hebbende gegevensdragers zoals foto's, video geluidsdragers | Gevoelig |
| | Aard van de relatie | Algemeen |
| | Gegevens betreffende de gezondheid | Bijzonder |

## Ontvangers

| | Categorieën van (mogelijke) ontvangers | Doel(en)<br>(zie de erste tabel 'Verwerking' bij 'Doeleind(en) van verwerking' voor de betekenis van de nummers) |
|---|---|---|
| *Intern* | Uitdrukkelijk aangewezen fraudefunctionarissen en –contactpersonen van de afdeling of van andere afdelingen van de verantwoordelijke | 1 |
| | Medewerkers acceptatie die belast zijn met het nemen van precontractuele maatregelen waarop het fraudeonderzoek is gericht, alsook diegenen die daarbij noodzakelijk zijn betrokken. | 1 |
| | Medewerkers schadebehandeling die belast zijn met het nemen van een beslissing in een schadedossier waarop het fraudeonderzoek is gericht, alsook diegenen die daarbij noodzakelijk zijn betrokken. | 1 |
| | Categorieën van (mogelijke) ontvangers | Doel(en) |
| Extern | Externe Verwijzingsregisters als bedoeld in het Protocol incidentenwaarschuwingsregister Financiële Instellingen | 1 |
| | Personen en instanties die op grond van een wettelijke verplichting geïnformeerd moeten worden, dan wel op grond van een wettelijke verplichting geïnformeerd mogen worden. | 1 |
| | De fraudeloketten van de brancheorganisaties die verantwoordelijk zijn voor het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen | 1 |
| | Veiligheidszaken of de veiligheidsfunctionaris van andere financiële instellingen, een en ander voor zover<br>- die instelling lid is van het Verbond van Verzekeraars of Zorgverzekeraars Nederland<br>- verstrekking mogelijk is binnen de voorwaarden van paragraaf 4.2 van het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen, èn de financiële instelling een | 1 |

| | | |
|---|---|---|
| | toetredingsverklaring heeft ondertekend als bedoeld in artikel 7.1.2 van het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen | |
| | Veiligheidszaken van derde-organisaties voor zover is voldaan aan ieder van de volgende criteria als vermeld in artikel 4.2.7. PIFI | 1 |
| | Bewerkers zoals bijvoorbeeld het Stichting CIS/ABZ, Zorgverzekeraars Nederland | 1 |
| | Stichting Waarborgfonds Motorverkeer conform artikel 4.2.4 van het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen | 1 |
| | Afdeling Veiligheidszaken of veiligheidsfunctionaris van andere financiële instellingen, één en ander voor zover:<br>a) die instelling lid is van een brancheorganisatie verantwoordelijk voor het PIFI<br>b) verstrekking mogelijk is binnen de voorwaarden van par. 4.2 van het PIFI, en<br>c) de instelling een toetredingsverklaring heeft ondertekend als bedoeld in het PIFI | 1 |
| | Advocaten, voor zover in de hoedanigheid van vertegenwoordiger van een van de beschreven ontvangers | 1 |

## Doorgifte

| | |
|---|---|
| *Binnen EU* | Ja |
| *Buiten EU* | Nee |
| *Internationale organisaties* | Nee |
| *Passend* | N.v.t. |

## Bewaartermijnen

Persoonsgegevens worden maximaal 8 jaar bewaard, te rekenen vanaf moment van registratie.

## Algemene beschrijving technische en organisatorische beveiligingsmaatregelen

De bescherming van persoonsgegevens valt onder het informatiebeveiligingsbeleid van de organisatie. Dit informatiebeveiligingsbeleid is gebaseerd op negen pijlers:

- risicoanalyses, gericht op het bepalen van een beveiligingsclassificatie voor een (business)applicatie en eisen voor specifieke application controls;
- onderhouden van een basisbeveiligingsniveau voor de werkstations, netwerken, servers en storage. Hierbij valt te denken aan clear screen policy (schermbeveiliging), cryptografische versleuteling bij data-uitwisseling met externe partijen; beveiligde serverruimte; bescherming tegen kwaadaardige software.
- logische toegangsbeveiliging, gericht op het onderhouden van een set van regels voor het verlenen van toegang tot netwerk- en computersystemen, waaronder beveiliging van het

netwerk middels een inlogprocedure (persoonlijke inlognaam en wachtwoord waarbij wachtwoorden periodiek dienen te worden gewijzigd);

- fysieke beveiliging, gericht op het weren van onbevoegden (toegangsbeveiliging en fysieke beveiliging van gebouw en omgeving);
- integriteitmanagement, gericht op het vaststellen van de betrouwbaarheid van het personeel bij het in dienst nemen van personeel, tijdens de uitvoering van het dienstverband en het einde dienstverband;
- bedrijfscontinuïteitsplannen met betrekking tot informatie in geval van calamiteiten (waaronder maken van back-ups);
- Incidentenmanagement, gericht op de registratie, analyse, escaleren, oplossen en voorkomen van beveiligingsincidenten.
- Autorisatiemanagement, gericht op het voorkomen van ongeoorloofde toegang tot applicaties en onderliggende data.
- Awareness, om de medewerkers regelmatig te wijzen op de rol die zij zelf spelen in de informatiebeveiliging en bescherming van de persoonsgegevens (o.a. Clean desk policy).