# Aangifte datahandel

**Hulpmiddel bij aangifte**

Versie juni 2024

« waakzaam en dienstbaar »

# Datahandel, wat is dat?

Er is sprake van datahandel wanneer er vertrouwelijke gegevens op online platforms worden verkocht of worden gedumpt.  Het gaat in veel gevallen om credentials (unieke inloggegevens voor verschillende diensten) of om persoonsgegevens die voor verschillende doeleinden gebruikt kunnen worden. De gestolen of gelekte data wordt misbruikt bij talloze vormen van criminaliteit, zoals identiteitsfraude en oplichting.

Er kunnen verschillende methodes worden ingezet om data te verkrijgen, denk aan phishing of hacken. Data kan ook onbewust gelekt worden door medewerkers van een bedrijf.

# Vragen aangifte

U maakt een afspraak voor het doen van aangifte. Voordat u de afspraak heeft, is het belangrijk dat u alle benodigde gegevens al bij de hand heeft. Dit hulpmiddel helpt bij het verzamelen van de juiste informatie. De antwoorden kunt u invullen onder de vraagstelling.
U dient dit document op een *computer* in te vullen. Om het document in te vullen klikt u boven in beeld op “BEELD” en vervolgens op “Document bewerken”.

*Gegevens aangever*

- Voornaam
- Achternaam
- Geboortedatum
- Adres
- Postcode
- E-mailadres
- Telefoonnummer
- Burgerservicenummer

*Gegevens benadeelde*

- Naam bedrijf
- Adres
- Vestigingsplaats
- KVK-nummer
- E-mailadres
- Telefoonnummer

*Aanleiding*

1. In welke periode heeft het incident plaatsgevonden? Noteer zowel de eerste als laatste dag, inclusief de juiste tijd.
2. Kunt u in chronologische volgorde vertellen wat er is gebeurd?

*Algemene vragen*

1. Om wat voor soort data gaat het?
2. Wat is de omvang van het lek?
3. Op wat voor apparaten heeft het lek plaatsgevonden?
4. Om hoeveel slachtoffers gaat het?
5. Zijn er steeds hetzelfde soort persoonsgegevens gelekt of verschillende combinaties?
6. De data is online gedeeld. Van welke platformen is bekend dat de data er gedeeld is?
7. Hoe zit de aangevallen infrastructuur in elkaar?
    - Wat is het zwakke punt in de infrastructuur?
    - Welke beschermende maatregelen zijn er getroffen?
8. Welke vervolgstappen zijn er door u ondernomen?
9. Is de Autoriteit Persoonsgegevens in kennis gesteld?
10. Zijn de gedupeerden allen op de hoogte van het lek?
11. Zijn er aanwijzingen dat de persoonsgegevens zijn misbruikt?
12. Hebt u nog andere relevante informatie voor het onderzoek beschikbaar? Zijn u dingen opgevallen?

*Communicatie met een eventuele verdachte*
**(alleen indien van toepassing)**

13. Is/zijn de aanval(len) opgeëist? Zo ja, door wie?

14. Is er (open bronnen) onderzoek gedaan om te kijken of de aanval opgeëist is?

15. Wat wordt er geëist, denk aan een geldsom of informatie?

16. Is er een reden gegeven voor de aanval(len)?

17. Welk medium is gebruikt om de aanval(len) op te eisen? (Bijvoorbeeld e-mail, social media, etc.)

18. Is dit vastgelegd en zo ja, kan dit aangeleverd worden als bijlage bij de aangifte?

19. Is er contact opgenomen met de opeisende partij? Zo ja, hoe heeft dat contact plaatsgevonden? Met welke gegevens (accountnaam, etc.)?

20. Is er op dit moment nog contact met de opeisende partij?

*Schade*
Kunt u de schadebedragen specificeren (zie hiervoor de onderstaande vragen)

21. a. In het geval van uitval van dienstverlening: wat zijn de gederfde inkomsten en/of wat is de overige schade?
    b. In het geval van omzetverlies: alleen de winst die u over de gemiste omzet had kunnen realiseren is op te voeren als schadebedrag.

22. Is er onderzoek verricht waarvoor kosten gemaakt zijn?
    In het geval van extra inzet van bijvoorbeeld een systeembeheerder/IT-bedrijf, zijn de extra uren die aan dit voorval besteed worden/IT inhuur een schadepost.

*Slachtofferhulp*

Heeft u behoefte aan slachtofferhulp of nazorg? (zie informatie op https://www.politie.nl/informatie/ik-ben-slachtoffer-wat-nu.html)

- Deze vraag graag met **ja** of **nee** beantwoorden. Antwoord:

# Voorkom datahandel

Neem bijvoorbeeld de volgende acties:

- Installeer software updates altijd op tijd.
- Zorg voor een goede IT-beveiliging van alle digitale apparaten.
- Gebruik sterke en unieke wachtwoorden. Gebruik voor wachtwoorden bijvoorbeeld een onsamenhangende zin, die alleen u weet en/of gebruik een wachtwoordmanager en indien mogelijk tweestapsverificatie.
- Instrueer uw medewerkers hoe ze moeten omgaan met persoonsgegevens
- Zorg dat u goed op de hoogte bent van de wetgeving rond persoonsgegevens: de AVG.
- Geef niet zomaar wachtwoorden, klantgegevens en toegang tot uw systemen aan derden, zoals zelfstandigen die u inhuurt of leveranciers.
- Wanneer een derde partij voor uw bedrijf persoonsgegevens gaat verwerken, is het verplicht om te zorgen voor een verwerkersovereenkomst. Ook ZZP'ers moeten bij elke nieuwe opdracht controleren of zij met persoonsgegevens van de opdrachtgever werken, wanneer dat zo is dienen zij een verwerkersovereenkomst te tekenen.