

TRANSPARANTIERAPPORT 2023

Transparantierapport 2023 BIT B.V.

Versie: 16 januari 2024

Introductie

In 2012 bracht BIT voor het eerst een transparantierapport uit. Het doel van dit rapport is om inzicht te geven in het aantal bevestigingen (door opsporingsinstanties) naar persoonsgegevens van klanten van BIT, het aantal notice-and-take-down-verzoeken, en hoe veel Responsible Disclosure-meldingen BIT heeft ontvangen. In dit rapport delen we de informatie over het jaar 2023.

We laten deze gegevens zien omdat we het belangrijk vinden om eerlijk te zijn, vooral met alle veranderingen en ontwikkelingen op het gebied van privacy. We willen onze klanten en andere mensen die geïnteresseerd zijn laten weten wat er gaande is. Om eventuele patronen of ontwikkelingen te laten zien, hebben we de cijfers van 2019 tot en met 2023 in dit verslag gezet. Op verzoek zijn ook de cijfers van voor 2019 beschikbaar.

In dit rapport is per categorie te lezen hoeveel klachten, verzoeken of meldingen we hebben ontvangen en hoe we ermee zijn omgegaan.

Inhoudsopgave

I	Verstrekking van persoonsgegevens	2
I.1	NAW-bevragingen	2
I.2	Melding van inbreuk in verband met persoonsgegevens	2
I.3	Tapbevelen	3
I.4	Overige	3
2	Take-down-verzoeken	4
2.1	Take-down-verzoeken inzake malware	4
2.2	Take-down-verzoeken inzake copyrightscheiding	5
2.3	Take-down-verzoeken inzake phishing	6
2.4	Take-down-verzoeken inzake kinderporno	6
3	Responsible Disclosure	7
4	Conclusies en opmerkingen	8

I Verstrekking van persoonsgegevens

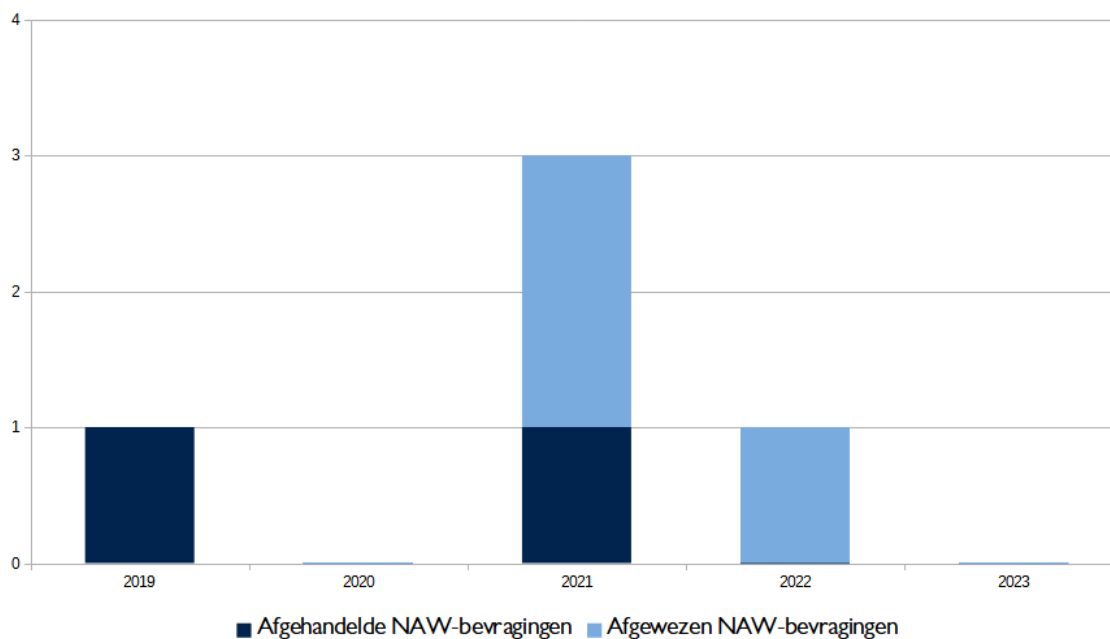
In de tabel hieronder zie je het aantal ontvangen verzoeken voor het verstrekken van persoonsgegevens van klanten van BIT aan opsporingsinstanties. Ook staat aangegeven hoe vaak we wel of niet aan dat verzoek hebben voldaan.

	2019	2020	2021	2022	2023
Afgehandelde NAW-bevragingen	1	0	1	0	0
Afgewezen NAW-bevragingen	0	0	2	1	0
Totaal	1	0	3	1	0

I.1 NAW-bevragingen

In onderstaande grafiek hebben we het aantal NAW-bevragingen van de afgelopen 5 jaar geplaatst, zodat er een duidelijk overzicht is van de jaarlijkse ontwikkelingen.

NAW-bevragingen



I.2 Melding van inbreuk in verband met persoonsgegevens

BIT is wettelijk vereist om melding te maken van inbreuken op persoonsgegevens. In 2023 was er geen aanleiding tot dergelijke melding(en).

	2019	2020	2021	2022	2023
Melding inbreuk persoonsgegevens	0	0	0	0	0

1.3 Tapbevelen

De Nationale Politie, FIOD-ECT, Nederlandse Arbeidsinspectie, IOD, AID, AIVD en MIVD hebben het recht om bij een provider een bevel neer te leggen voor (af)tappen, zoals e-mail- of IP-taps. Hieronder staat de tabel met het aantal tapbevelen dat BIT heeft ontvangen in de afgelopen 5 jaar.

	2019	2020	2021	2022	2023
Aantal ontvangen tapbevelen	0	0	0	0	0

1.4 Overige

De categorie overige binnen verstrekking van persoonsgegevens omvat alle verzoeken/bevelen/bevragingen die niet binnen de eerder genoemde categorieën vallen. In 2023 hebben we 4 overige bevelen ontvangen. Deze zijn afgewezen omdat ze niet van toepassing zijn op de diensten van BIT.

2 Take-down-verzoeken

In deze sectie vind je een overzicht van de verschillende take-down-verzoeken die BIT heeft ontvangen en de manier waarop deze zijn afgehandeld.

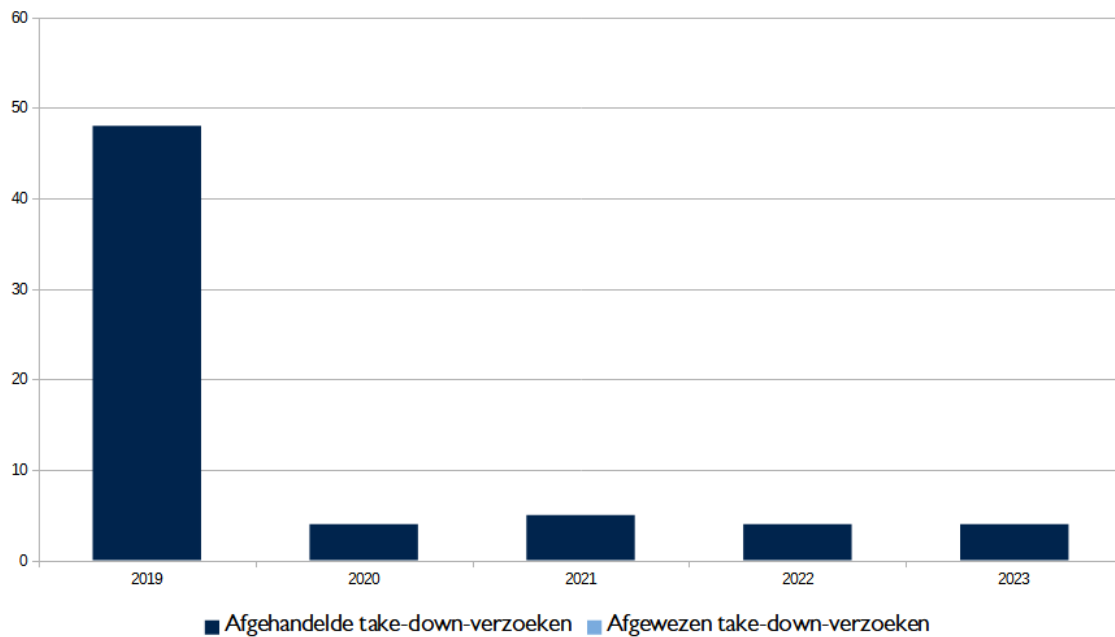
2.1 Take-down-verzoeken inzake malware

De onderstaande tabel geeft een overzicht van de take-down-verzoeken die BIT de afgelopen 5 jaar heeft ontvangen vanwege het (vermeend) hosten van malware, inclusief hoe deze verzoeken zijn afgehandeld.

	2019	2020	2021	2022	2023
Afgehandelde take-down-verzoeken	48	4	5	4	4
Afgewezen take-down-verzoeken	0	0	0	0	0
Totaal	48	4	5	4	4

In onderstaande grafiek hebben we het aantal take-down-verzoeken met betrekking tot malware van de afgelopen 5 jaar geplaatst, zodat er een duidelijk overzicht is van de jaarlijkse ontwikkelingen.

Take-down verzoeken inzake malware



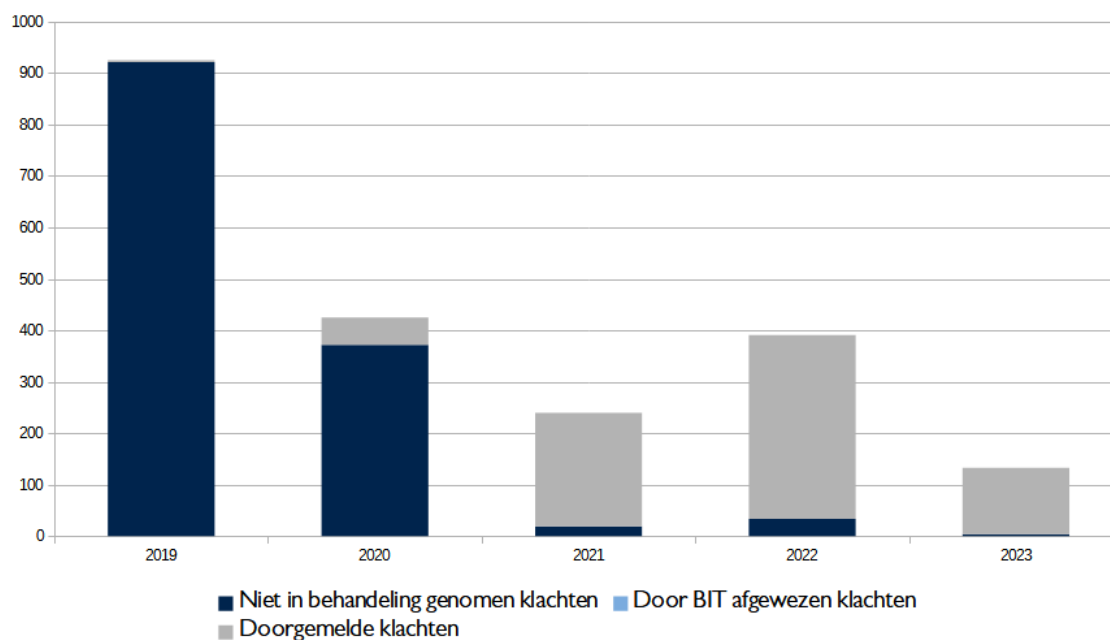
2.2 Take-down-verzoeken inzake copyrightschiending

In het Transparantierapport van 2013 heeft BIT voor het eerst de cijfers gedeeld over ontvangen en afgehandelde notice-and-take-down-verzoeken met betrekking tot vermeende copyrightschiending. Hieronder vind je de aantallen van de afgelopen vijf jaar overzichtelijk weergegeven in een tabel.

	2019	2020	2021	2022	2023
Niet in behandeling genomen take-down-verzoeken	921	372	19	34	4
Door BIT afgewezen take-down-verzoeken	0	0	0	0	0
Doorgemelde take-down-verzoeken	4	53	221	357	129
Totaal	925	425	240	391	133

In onderstaande grafiek hebben we het aantal take-down-verzoeken inzake copyrightschiending van de afgelopen 5 jaar geplaatst, zodat er een duidelijk overzicht is van de jaarlijkse ontwikkelingen.

Take-down verzoeken inzake copyrightschiending



Tot 2020 werden de meeste niet in behandeling genomen klachten geautomatiseerd ingediend door een beperkt aantal partijen namens de film- en muziekindustrie. Destijds voldeden deze klachten niet aan onze notice-and-take-down-procedure.

Vanaf 2021 meldt BIT echter wel klachten van deze partijen door, wat de aanzienlijke stijging verklaart in het aantal doorgemelde klachten.

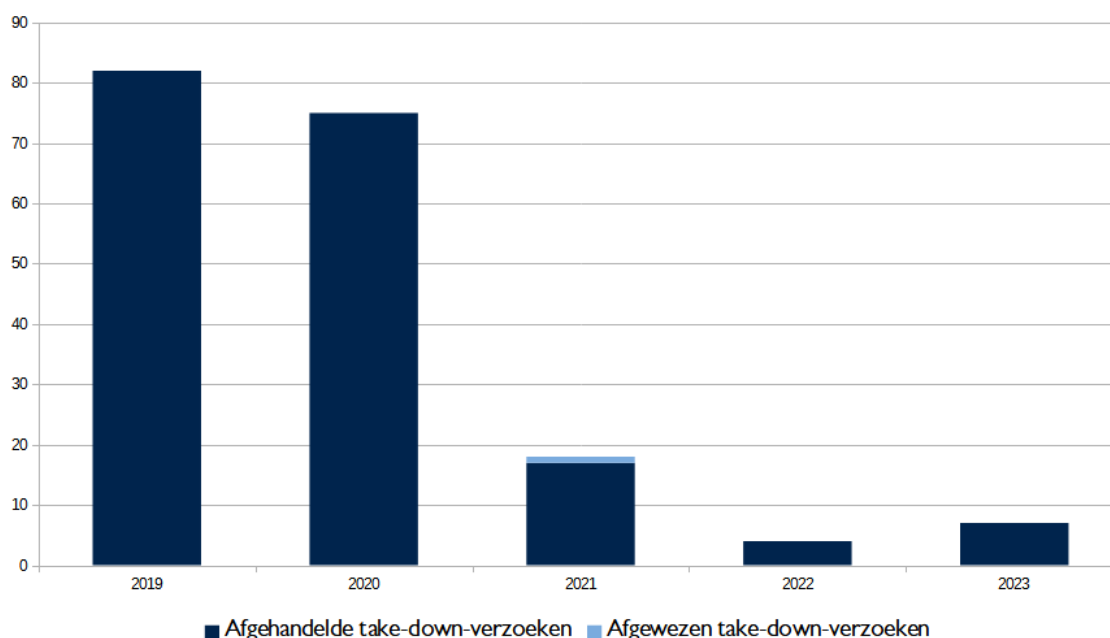
2.3 Take-down-verzoeken inzake phishing

De onderstaande tabel geeft een overzicht van de take-down-verzoeken die BIT de afgelopen 5 jaar heeft ontvangen inzake phishing-sites, inclusief hoe deze verzoeken zijn afgehandeld.

	2019	2020	2021	2022	2023
Afgehandelde take-down-verzoeken	82	75	17	4	7
Afgewezen take-down-verzoeken	0	0	1	0	0
Totaal	82	75	18	4	7

In onderstaande grafiek hebben we het aantal take-down-verzoeken met betrekking tot phishing van de afgelopen 5 jaar geplaatst, zodat er een duidelijk overzicht is van de jaarlijkse ontwikkelingen.

Take-down-verzoeken inzake phishing



2.4 Take-down-verzoeken inzake kinderporno

De onderstaande tabel geeft een overzicht van de take-down-verzoeken die BIT de afgelopen 5 jaar heeft ontvangen inzake kinderporno, inclusief hoe deze verzoeken zijn afgehandeld.

	2019	2020	2021	2022	2023
Afgehandelde take-down-verzoeken	0	0	0	0	0
Afgewezen take-down-verzoeken	0	0	0	0	0
Totaal	0	0	0	0	0

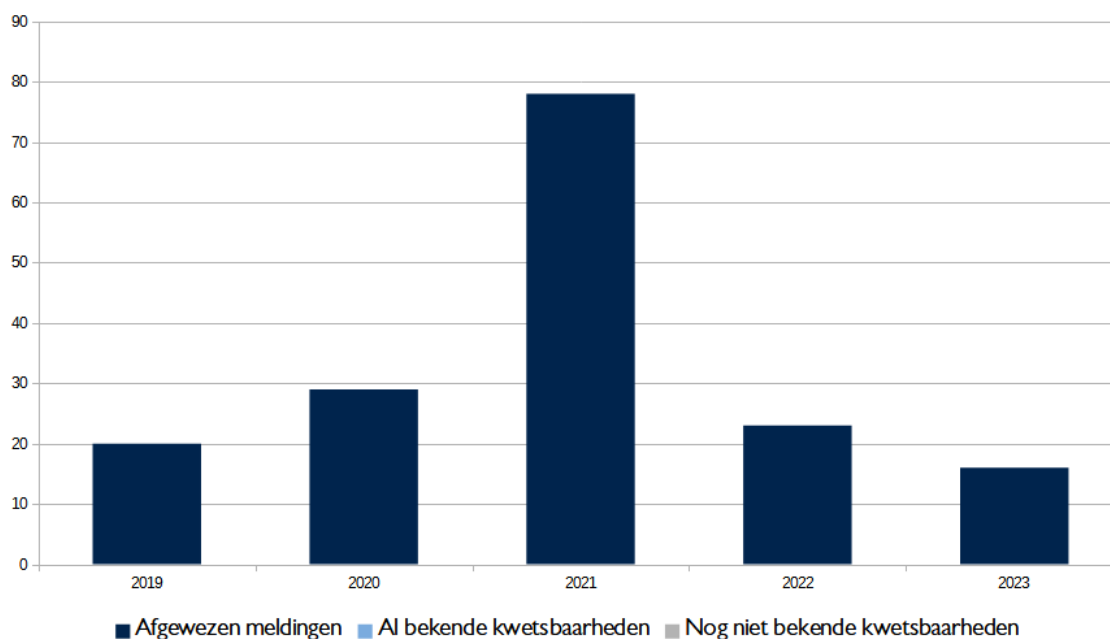
3 Responsible Disclosure

In onderstaande tabel wordt aangegeven hoeveel Responsible Disclosure-meldingen er bij BIT zijn gedaan. In dit overzicht hebben we onderscheid gemaakt in afgewezen meldingen, reeds bekende kwetsbaarheden en nog niet bij ons bekende kwetsbaarheden.

	2019	2020	2021	2022	2023
Afgewezen meldingen	20	29	78	23	16
Al bekende kwetsbaarheden	0	0	0	0	0
Nog niet bekende kwetsbaarheden	0	0	0	0	0
Totaal	20	29	78	23	16

In onderstaande grafiek hebben we het aantal Responsible Disclosure-meldingen die BIT heeft ontvangen in de afgelopen 5 jaar geplaatst, zodat er een duidelijk overzicht is van de jaarlijkse ontwikkelingen.

Responsible Disclosure meldingen



4 Conclusies en opmerkingen

In het jaar 2023 heeft BIT geen verzoeken ontvangen voor het verstrekken van persoonsgegevens van klanten aan opsporingsinstanties. Dit geldt zowel voor NAW-bevragingen, waarbij geen enkel verzoek werd ingewilligd of afgewezen, als voor tapbevelen, waarbij geen enkel bevel werd ontvangen. Ook waren er geen meldingen van inbreuken op persoonsgegevens. Het lage aantal bevragingen omtrent persoonsgegevens is te wijten aan het feit dat BIT geen diensten aan particulieren levert.

Sinds dit jaar wordt er ook over de categorie 'Overige' gerapporteerd. Deze categorie bestaat al langer, maar 2023 was het eerste jaar waarin BIT vorderingen binnen deze categorie heeft ontvangen. In deze categorie kwamen vier vorderingen binnen, maar deze zijn afgewezen omdat ze niet van toepassing waren op diensten van BIT.

De gerapporteerde malwarebesmettingen zijn sterk afgenomen sinds 2020. Dit wordt mogelijk verklaard doordat deze nu gemeld worden via andere classificaties, zoals RBL-listings.

Het aantal meldingen van schendingen van auteursrechten (copyrightmeldingen) is opnieuw gedaald. Sinds 2021 meldt BIT echter wel klachten van partijen die namens de film- en muziekindustrie meldingen doen door, wat verklaart dat het aantal doorgemelde klachten is gestegen.

Sinds 2019 hebben we besloten om geen vergoeding meer te vermelden in ons Responsible Disclosure-beleid, en sindsdien is het aantal meldingen ook lager geworden. We ontvangen wel nog relatief veel meldingen over zaken die bewust openbaar zijn, waar bewuste keuzes zijn gemaakt voor instellingen, of waar kwetsbaarheden zijn vastgesteld uit versienummers terwijl er bijvoorbeeld backports zijn gebruikt. Daarnaast krijgen we ook meldingen over systemen die zijn uitgesloten in ons Responsible Disclosure-beleid, zoals klantsystemen. Deze meldingen sturen we wel door naar de betreffende klant.