

Introduction

In 2012, BIT published its first Transparency Report. The purpose of this report is to provide insight into the number of requests (by law enforcement agencies) for personal data of BIT’s customers, the number of notice-and-take-down requests, and how many Responsible Disclosure reports BIT has received. In this report, we share the information for the year 2024.

We present this data because we believe it is important to be transparent, especially with all the changes and developments in the field of privacy. We want to inform our customers and other interested parties about what is happening. To show any patterns or developments, we have included the figures from 2020 to 2024 in this report. Upon request, figures from before 2020 are also available.

In this report, you can read, per category, how many complaints, requests, or reports we have received and how we have handled them.

Contents

1	Disclosure of Personal Data	2
1.1	Personal Information Inquiries	2
1.2	Data Breach Notifications Related to Personal Data	2
1.3	Legal Interception Warrants	3
1.4	Other	3
2	Take Down Requests	3
2.1	Take Down Requests Related to Malware	3
2.2	Take Down Requests Related to Copyright Infringement	4
2.3	Take Down Request Related to Phishing	5
2.4	Take Down Requests Related to CSAM	5
2.5	Take Down Requests Related to Terrorist Content	6
3	Responsible Disclosure	6
4	Conclusions and Remarks	7

1 Disclosure of Personal Data

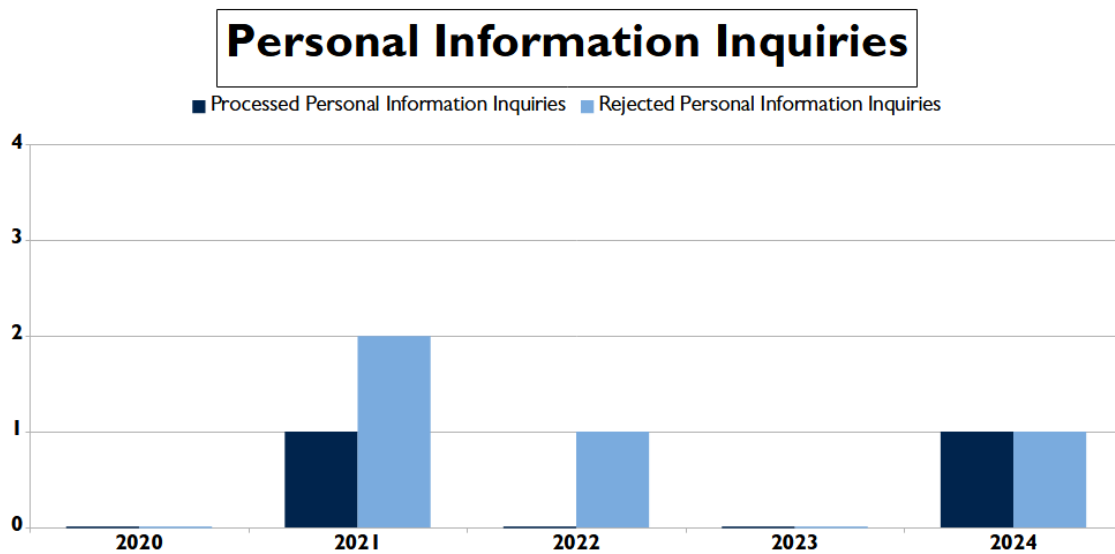
The section 'Disclosure of Personal Data' is divided into four subcategories, namely Personal Information Inquiries, data breach notifications related to personal data, interception warrants, and other. Each subcategory shows how many requests BIT received in 2024 and how they were handled.

1.1 Personal Information Inquiries

The table below shows the number of requests received for the disclosure of personal data of BIT's clients to law enforcement agencies. It also indicates how often we have of have not complied with such requests.

	2020	2021	2022	2023	2024
Processed Personal Information Inquiries	0	1	0	0	1
Rejected Personal Information Inquiries	0	2	1	0	1
Total	0	3	1	0	2

In the graph below, we have included the number of Personal Information Inquiries over the past five years to provide a clear overview of the annual developments.



1.2 Data Breach Notifications Related to Personal Data

BIT is legally required to report breaches of personal data. In 2024, we reported one breach related to personal data.

	2020	2021	2022	2023	2024
Data Breach Notifications	0	0	0	0	1

1.3 Legal Interception Warrants

The National Police, FIOD-ECT, Dutch Labour Inspectorate, IOD, AID, AIVD, and MIVD have the right to issue warrants to a provider for interception, such as email or IP taps. Below is a table showing the number of interception warrants BIT has received over the past five years.

	2020	2021	2022	2023	2024
Received Interception Warrants	0	0	0	0	2

1.4 Other

The 'Other' category within 'Disclosure of Personal Data' includes all requests/warrants/inquiries that do not fall under the previously mentioned categories. In 2024, we did not receive any other warrants.

2 Take Down Requests

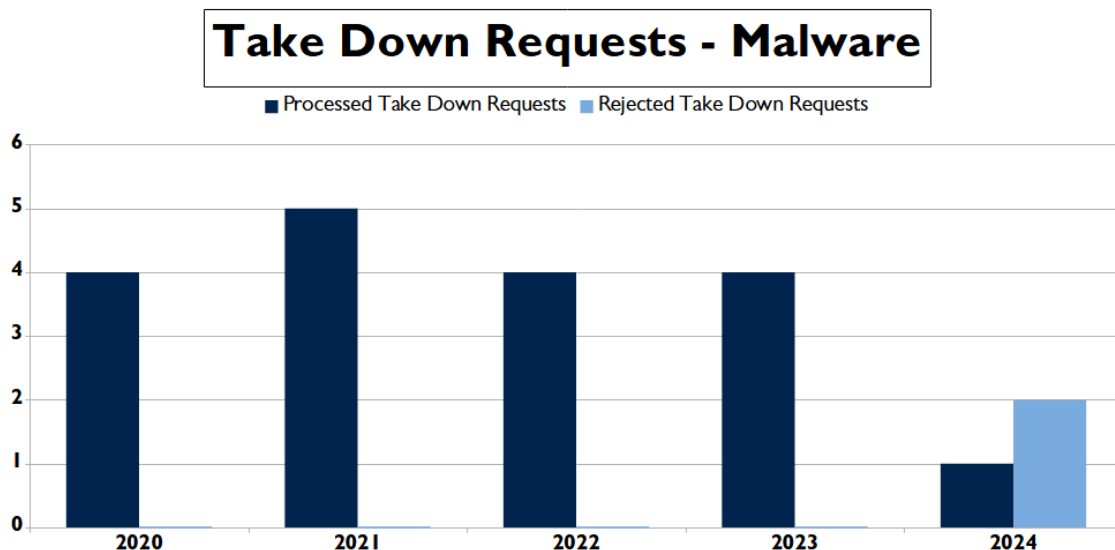
The section 'Take Down Requests' is divided into five subcategories, namely take-down requests related to malware, copyright infringement, phishing, child pornography, and terrorist content. Each subcategory shows how many requests BIT received in 2024 and how they were handled.

2.1 Take Down Requests Related to Malware

The table below provides an overview of the take-down requests BIT has received over the past five years due to (alleged) hosting of malware, including how these requests were handled.

	2020	2021	2022	2023	2024
Processed Take Down Requests	4	5	4	4	1
Rejected Take Down Requests	0	0	0	0	2
Total	4	5	4	4	3

In the graph below, we have included the number of take-down requests related to malware over the past five years to provide a clear overview of annual developments.



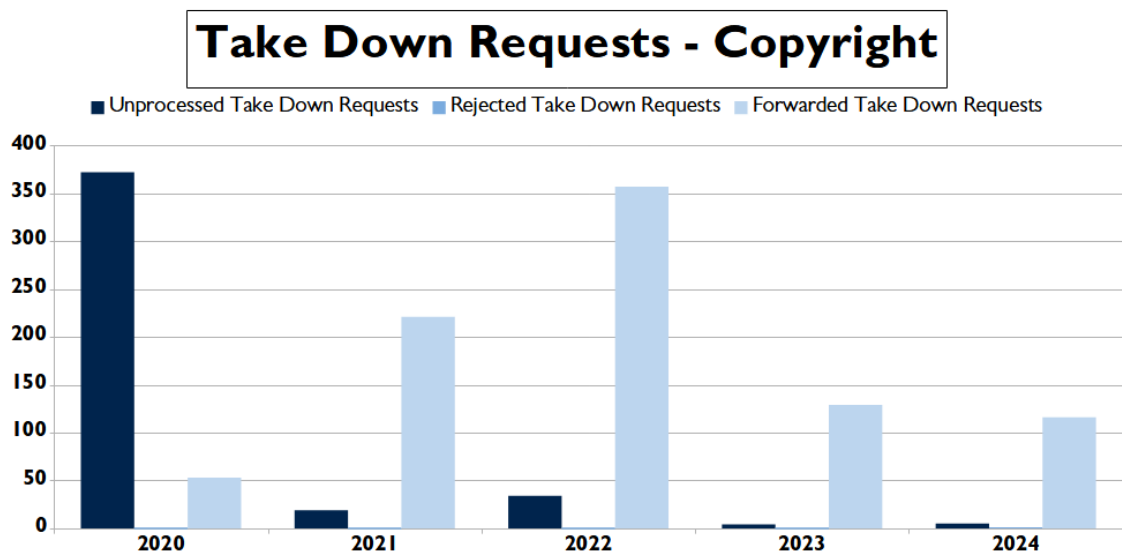
2.2 Take Down Requests Related to Copyright Infringement

In the 2013 transparency report, BIT first shared figures on received and processed notice-and-take-down requests related to (alleged) copyright infringement.

The table below provides an overview of the take-down requests BIT has received over the past five years due to (alleged) copyright infringement, including how these requests were handled.

	2020	2021	2022	2023	2024
Unprocessed Take Down Requests	372	19	34	4	5
Rejected Take Down Requests	0	0	0	0	1
Forwarded Take Down Requests	53	221	357	129	116
Total	425	240	391	133	122

In the graph below, we have included the number of take-down requests related to copyright infringement over the past five years to provide a clear overview of annual developments.



Until 2020, most unprocessed complaints were automatically submitted by a limited number of parties on behalf of the film and music industry. At that time, these complaints did not meet our notice-and-take-down procedure.

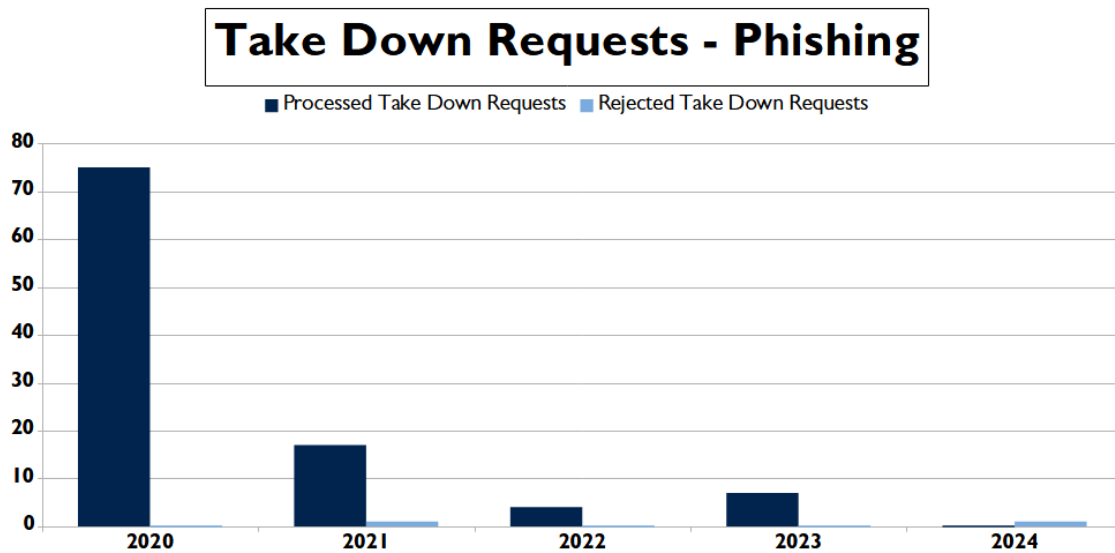
Since 2021, BIT has been forwarding complaints from these parties, which explains the significant increase in the number of forwarded complaints.

2.3 Take Down Request Related to Phishing

The table below provides an overview of the take-down requests BIT has received over the past five years related to phishing sites, including how these requests were handled.

	2020	2021	2022	2023	2024
Processed Take Down Requests	75	17	4	7	0
Rejected Take Down Requests	0	1	0	0	1
Total	75	18	4	7	1

In the graph below, we have included the number of take-down requests related to phishing over the past five years to provide a clear overview of annual developments.



2.4 Take Down Requests Related to CSAM

The table below provides an overview of the take-down requests BIT has received over the past five years related to CSAM, including how these requests were handled.

	2020	2021	2022	2023	2024
Processed Take Down Requests	0	0	0	0	0
Rejected Take Down Requests	0	0	0	0	0
Total	0	0	0	0	0

2.5 Take Down Requests Related to Terrorist Content

Since June 2022, a European regulation has been in effect that establishes rules to prevent the spread of online terrorist material. In the Netherlands, these rules are enforced by the ATKM.

The table below provides an overview of the take-down requests BIT has received since 2022 related to terrorist content, including how these requests were handled.

	2022	2023	2024
Processed Take Down Requests	0	0	0
Rejected Take Down Requests	0	0	0
Total	0	0	0

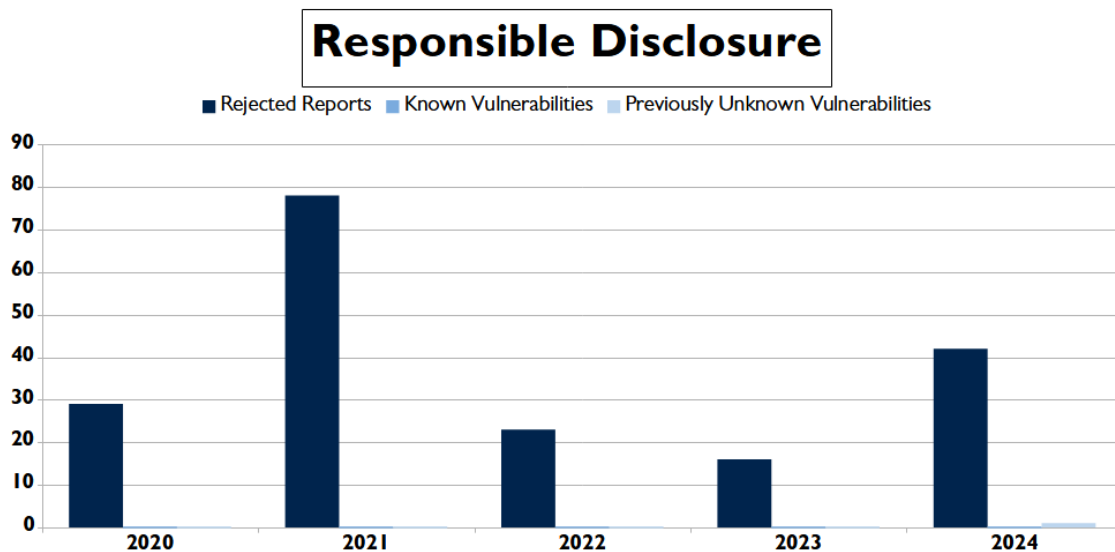
3 Responsible Disclosure

The table below indicates how many Responsible Disclosure reports have been submitted to BIT. In this overview, we have distinguished between rejected reports, already known vulnerabilities, and vulnerabilities not previously known to us.

In 2024, we forwarded 13 Responsible Disclosure reports to BIT’s customers.

	2020	2021	2022	2023	2024
Rejected Reports	29	78	23	16	42
Known Vulnerabilities	0	0	0	0	0
Previously Unknown Vulnerabilities	0	0	0	0	1
Total	29	78	23	16	43

In the graph below, we have included the number of Responsible Disclosure reports over the past five years to provide a clear overview of annual developments.



4 Conclusions and Remarks

In 2024, BIT received requests for the disclosure of personal data of customers to law enforcement agencies. This applies to NAW inquiries, where one request was granted, and this year also to interception warrants, as two warrants were received. The low number of inquiries regarding personal data can be explained by the fact that BIT does not provide services to private individuals. This year, there was a report of a breach of personal data.

Since 2023, the 'Other' category has also been reported. This category has existed for longer, but 2023 was the first year in which BIT received requests within this category. This year, no requests were received in this category.

The reported malware infections have significantly decreased since 2020. This may be explained by the fact that these are now reported through other classifications, such as RBL listings.

The number of copyright infringement reports has slightly decreased this year. However, since 2021, BIT has been forwarding complaints from parties representing the film and music industry.

Since 2019, we have decided not to mention a reward in our Responsible Disclosure policy, and since then, the number of reports has also decreased. We still receive relatively many reports about matters that are intentionally public, where deliberate choices have been made for settings, or where vulnerabilities have been identified from version numbers while, for example, backports have been used. Additionally, we receive reports about systems that are excluded from our Responsible Disclosure policy, such as customer systems. These reports are forwarded to the relevant customer. In 2024, one Responsible Disclosure report was rewarded, which concerned an XSS that was not actually exploitable.

Noteworthy is the data breach/breach of personal data that we have dealt with. There was a bug in our portal. Due to this bug, it was possible for logged-in users to request access logs from exactly one year earlier, and not only from their own organization.

Because we value privacy highly, it was not possible to determine whether someone had only accessed the portal page or had actually consulted the data. We therefore chose to personally inform all potentially affected individuals.

According to GDPR guidelines, we are not obliged to inform the affected parties of this data breach unless there is a high risk of negative consequences. Although we did not expect any adverse consequences, we place great value on openness and honesty. Therefore, we chose to inform the affected parties anyway. Of course, we also reported the breach to the relevant supervisory authorities.