Introduction

In 2012, BIT published its first Transparency Report. The purpose of this report is to provide an overview of the number of requests (from law enforcement agencies) for personal data relating to BIT's customers, the number of notice-and-take-down requests, and the number of Responsible Disclosure reports received by BIT. In this report we share the information relating to the year 2025.

We are publishing this data because we believe in transparency, particularly in the light of the numerous changes and developments in the field of privacy. We want our customers and other interested parties to be aware of what is happening. To highlight any patterns or trends, we have included figures from 2021 to 2025 in this report.

For each category, this report details how many complaints, requests or reports we have received and how we have handled them.

Contents

1 Disclosure of Personal Data

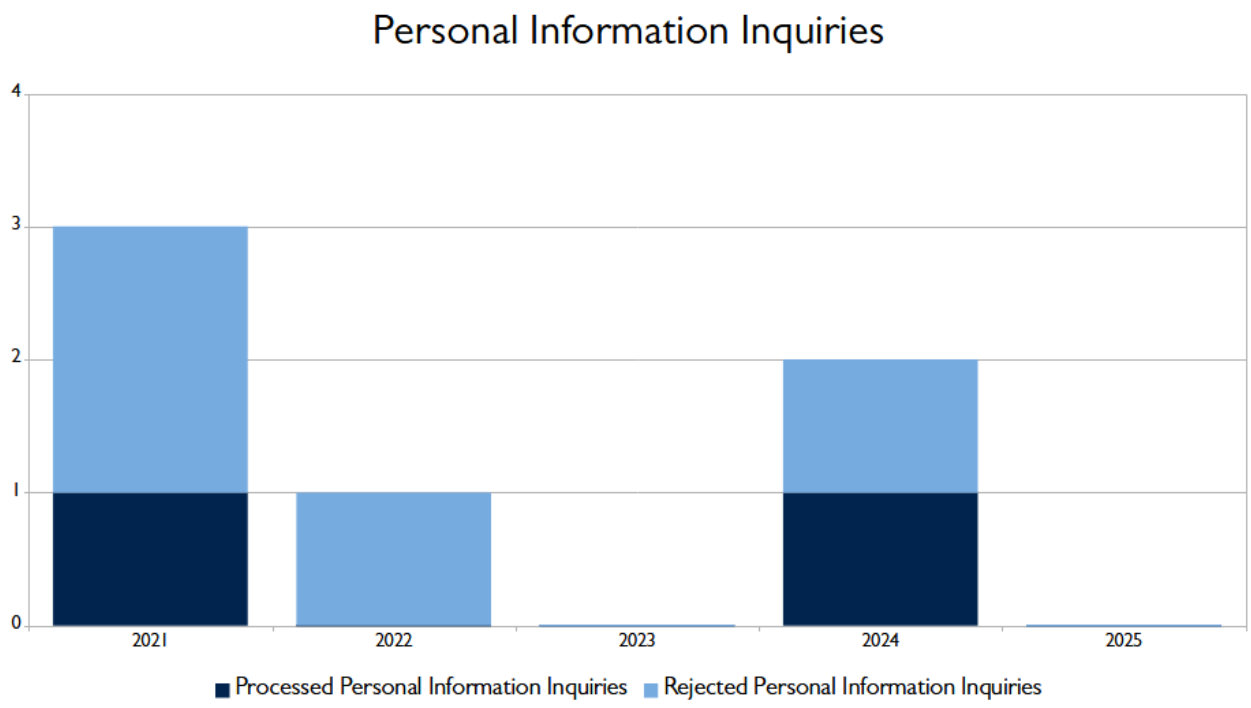
The section 'Disclosure of Personal Data' is divided into four subcategories, namely personal information inquiries, data breach notifications related to personal data, legal interception warrants and other. Each subcategory shows how many requests BIT received in 2025 and how they were handled.

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 shows how often we have or have not complied with such requests.

	2021	2022	2023	2024	2025
Processed personal information inquiries	1	0	0	1	0
Rejected personal information inquiries	2	1	0	1	0
Total	3	1	0	2	0

In the graph below, we have included the number of personal information inquiries of 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 any personal data breaches. In 2025, there was no need to make such a report.

	2021	2022	2023	2024	2025
Data breach notifications	0	0	0	1	0

1.3 Legal Interception Warrants

The National Police, FIOD-ECT, the Dutch Labour Inspectorate, IOD, AID, AIVD and MIVD are authorised to issue a warrant to an internet service provider for the interception of communications, such as email or IP traffic. Below is a table showing the number of interception warrants received by BIT over the past five years.

	2021	2022	2023	2024	2025
Received interception warrants	0	0	0	2	0

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 2025, we did not receive any other warrants.

2 Take Down Requests

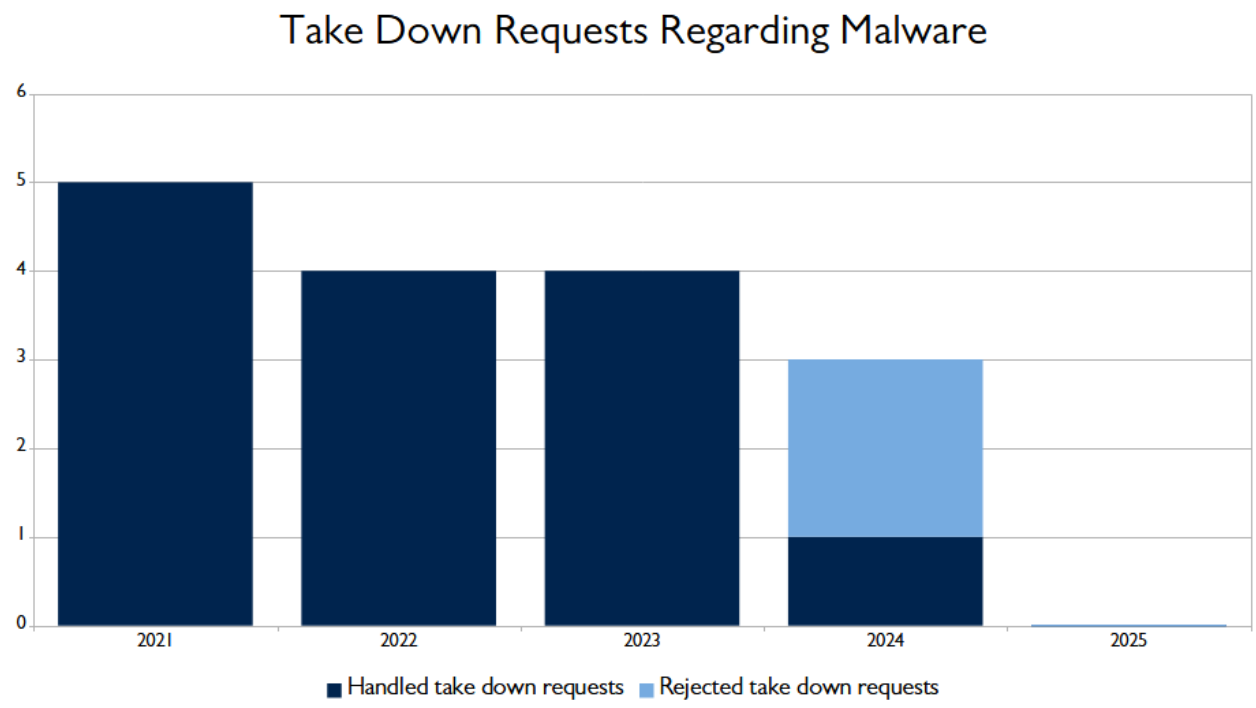
The section 'Take Down Requests' is divided into five subcategories, namely take down requests related to malware, copyright infringement, phishing, CSAM and terrorist content. Each subcategory shows how many request BIT received in 2025 and how they were handled.

2.1 Take Down Requests Regarding Malware

The table below shows an overview of the take down requests BIT received in the past five years regarding the (alleged) hosting of malware, including whether these requets were handled or rejected.

	2021	2022	2023	2024	2025
Handled take down requests	5	4	4	1	0
Rejected take down requests	0	0	0	2	0
Total	5	4	4	3	0

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.



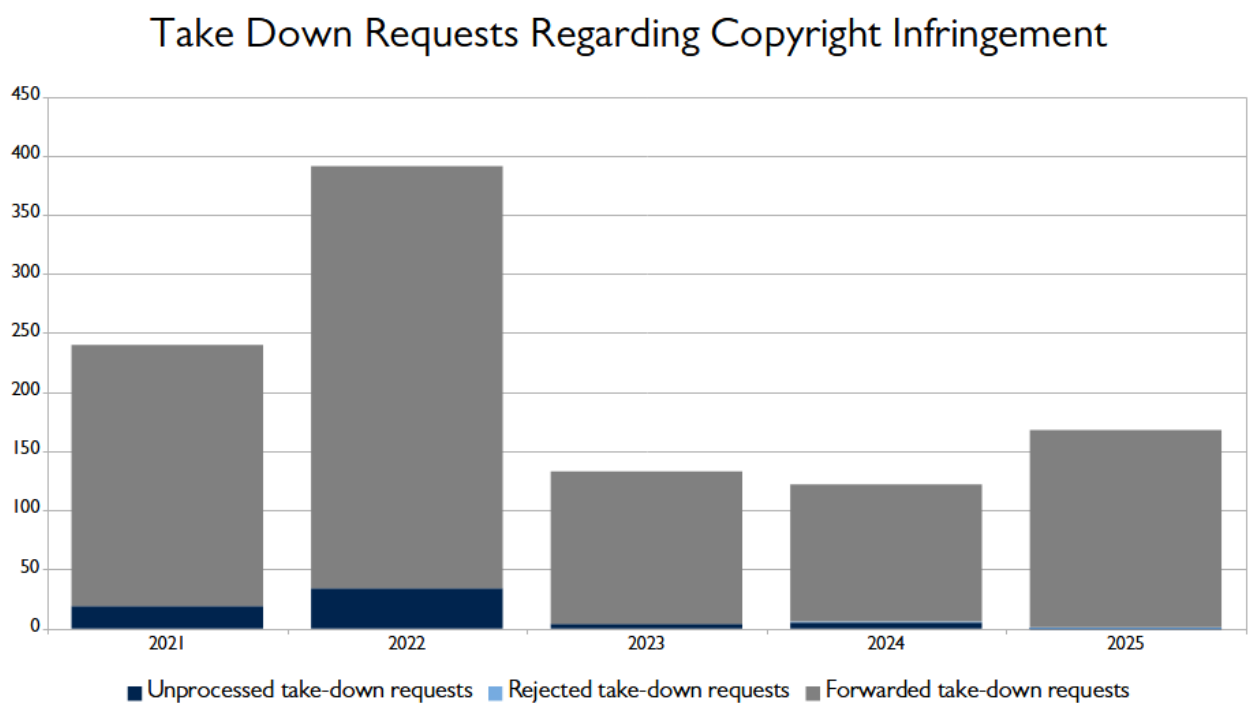
2.2 Take Down Requests Regarding Copyright Infringement

In the 2023 Transparency Report, BIT shared figures for the first time on notice-and-take-down requests received and processed in relation to (alleged) copyright infringement.

The table below provides an overview of the take-down requests received by BIT over the past five years concerning (alleged) copyright infringement, and whether these requests were handled, rejected or forwarded.

	2021	2022	2023	2024	2025
Unprocessed take-down requests	19	34	4	5	0
Rejected take-down requests	0	0	0	1	1
Forwarded take-down requests	221	357	129	116	167
Total	240	391	133	122	168

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.

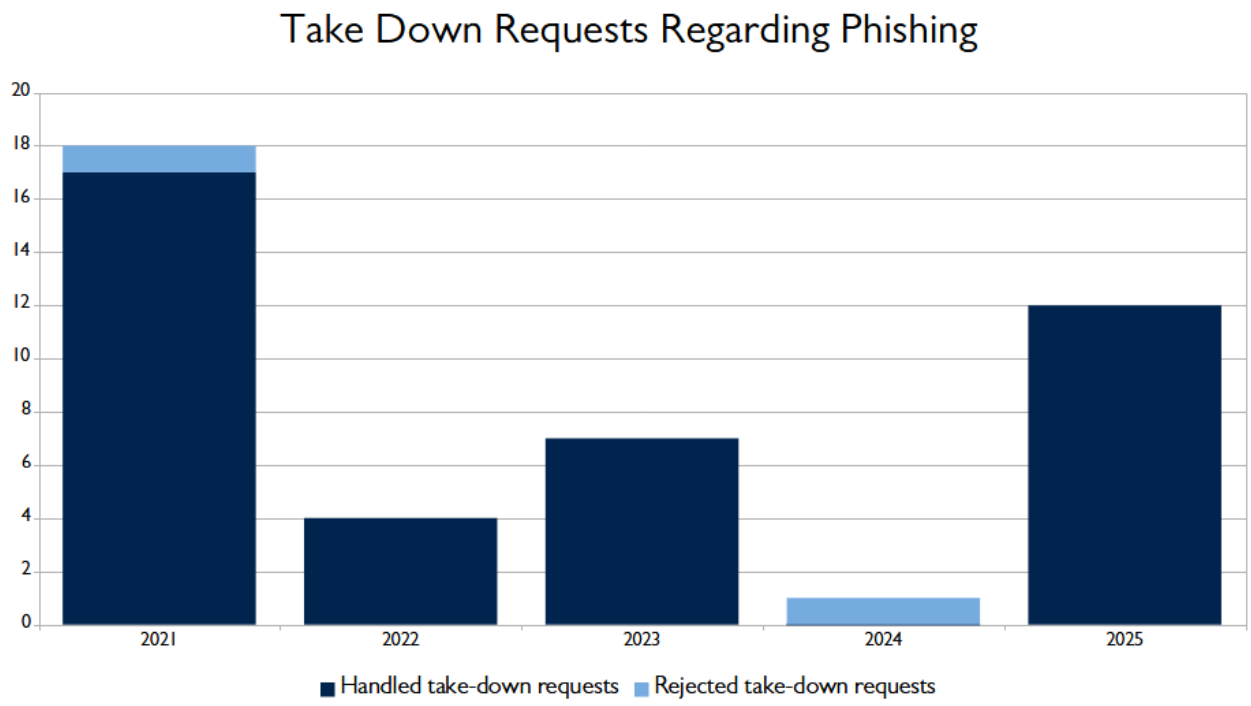


2.3 Take Down Requests Regarding Phishing

The table below provides an overview of the take-down requests BIT received in the past five years regarding phishing(sites), including whether these requests were handled or rejected.

	2021	2022	2023	2024	2025
Handled take-down requests	17	4	7	0	12
Rejected take-down requests	1	0	0	1	0
Total	18	4	7	1	12

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 Regarding CSAM

The table below provides an overview of the take-down requests BIT received in the past five years regarding CSAM, including whether these requests were handled or rejected.

	2021	2022	2023	2025	2025
Handled 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 Regarding 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 whether these requests were handled or rejected.

	2022	2023	2024	2025
Handled take-down requests	0	0	0	0
Rejected take-down requests	0	0	0	0
Total	0	0	0	0

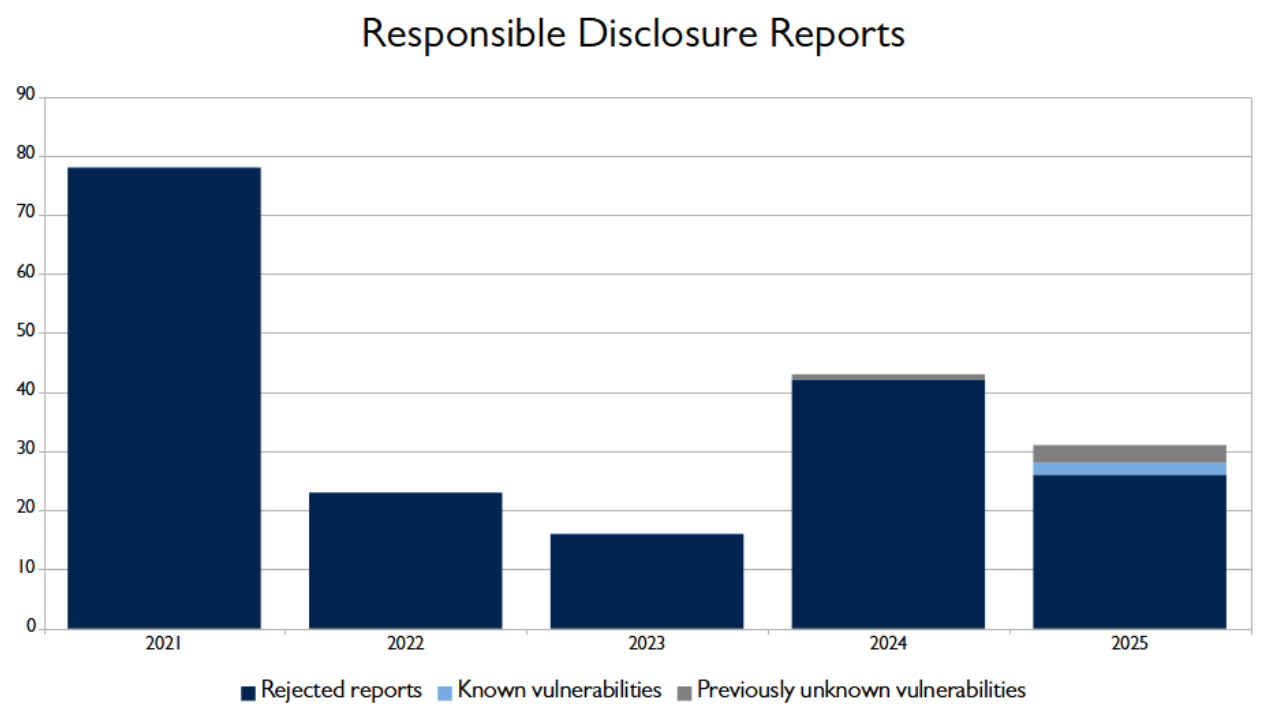
3 Responsible Disclosure

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

In 2025 we also forwarded six (6) Responsible Disclosure reports to BIT customers.

	2021	2022	2023	2024	2025
Rejected reports	78	23	16	42	26
Known vulnerabilities	0	0	0	0	2
Previously unknown vulnerabilities	0	0	0	1	3
Total	78	23	16	43	31

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 2025, BIT did not receive any requests for the disclosure of personal data of customers to law enforcement agencies. There were also no reports of personal data breaches. The generally low number of requests for personal data is due to the fact that BIT does not provide services to private individuals.

Since 2023, the 'Other' category has also been reported on. This category has existed for some time, but 2023 was the first year in which BIT received requests within this category. In 2025, no requests were received in this category.

The number of copyright infringement reports has risen compared to 2024. The vast majority of these are requests that have been forwarded to our customers.

Since 2019, we no longer mention any financial reward in our Responsible Disclosure policy, and since then the number of reports has decreased. We still receive quite a few reports on 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 2025 we paid out bounties on three occasions following Responsible Disclosure reports. These reports involved instances where the researcher demonstrated that information could potentially be disclosed or that input was not sufficiently validated.

The first report concerned a publicly accessible Grafana instance in which Grafana's own metrics were visible. Although this instance did not display any customer data or other sensitive information, we have further restricted access to prevent unintended viewing and further reports.

The second report concerned the display of stack traces from a Tomcat environment. Although these stack traces did not contain any sensitive information, they could provide attackers with information to launch targeted attacks. Furthermore, this is on the list of issues that ethical hackers are expected to report.

The third and final report concerned a reflected Cross-Site Scripting (XSS) vulnerability whereby the target URL of a redirect could be manipulated. Although there was no direct impact on customer data, such a vulnerability could be exploited through targeted phishing.