TRANSPARENCY REPORT 2020

TRANSPARENCY REPORT 2020 BIT B.V. – VERSION 2021-08-30

In 2012, BIT issued a transparency report for the first time with the aim of providing insight into requests for personal data at BIT, the number of notice-and-takedown requests BIT has received and processed and how many responsible disclosure reports we have received. In this report we publish this information for the year 2020.

We publish this information because we consider it important, especially given the recent developments in the field of privacy, to provide openness about this to our relations and other interested parties. In order to provide insight into possible trends, we have included the figures from 2016 to 2020 in this report. We can also make the figures for 2016 available to you on request.

Below you find per category the number of complaints/requests/notifications received and the way in which they were handled.

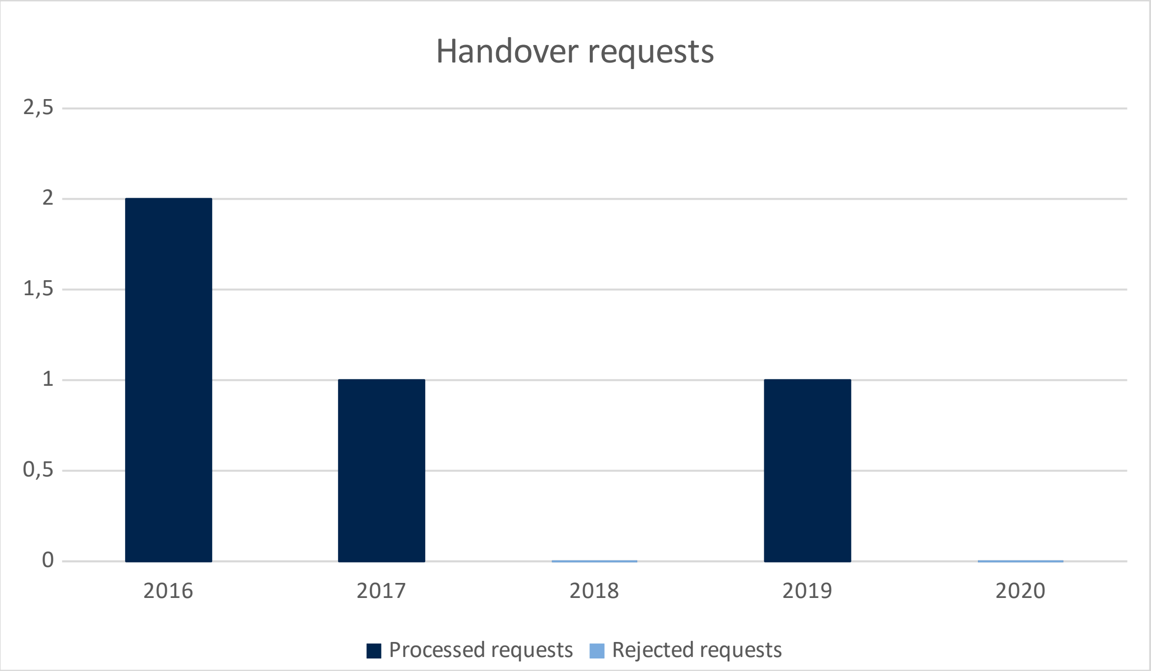
Handover of personal data

The table below shows the number of requests we have received for the handover of personal data of customers of BIT to law enforcements. The number of cases that were in compliance with this request are indicated as well.

	2016	2017	2018	2019	2020
Processed requests	2	1	0	1	0
Rejected requests	0	0	0	0	0
Total	2	1	0	1	0

Handover requests

The number of handover requests for personal data of customers are displayed in the graph below. This will give you a clear overview of the developments during the years.



Reports of data protection infringements

BIT is legally required to report any event of infringement of the protection of personal data they have stored. In 2020, BIT saw no reason to report this.

The prior reported personal data breaches in 2017 and 2018 can be explained by the fact that a mobile phone of a BIT employee was lost on which was access to the employee's company email. In both cases, the mobile phone was provided with a password and encryption.

	2016	2017	2018	2019	2020
Reports of data protection infringement	0	1	1	0	0

Legal interception orders

It is possible for the National Police, FIOD-ECT, Inspection SZW, IOD, AID, AIVD and MIVD to place a legal interception order at a provider. This can be an email intercept or an IP intercept. The table below shows the number of legal interception orders we have received.

	2016	2017	2018	2019	2020
Number of legal interception orders	0	2	0	0	0

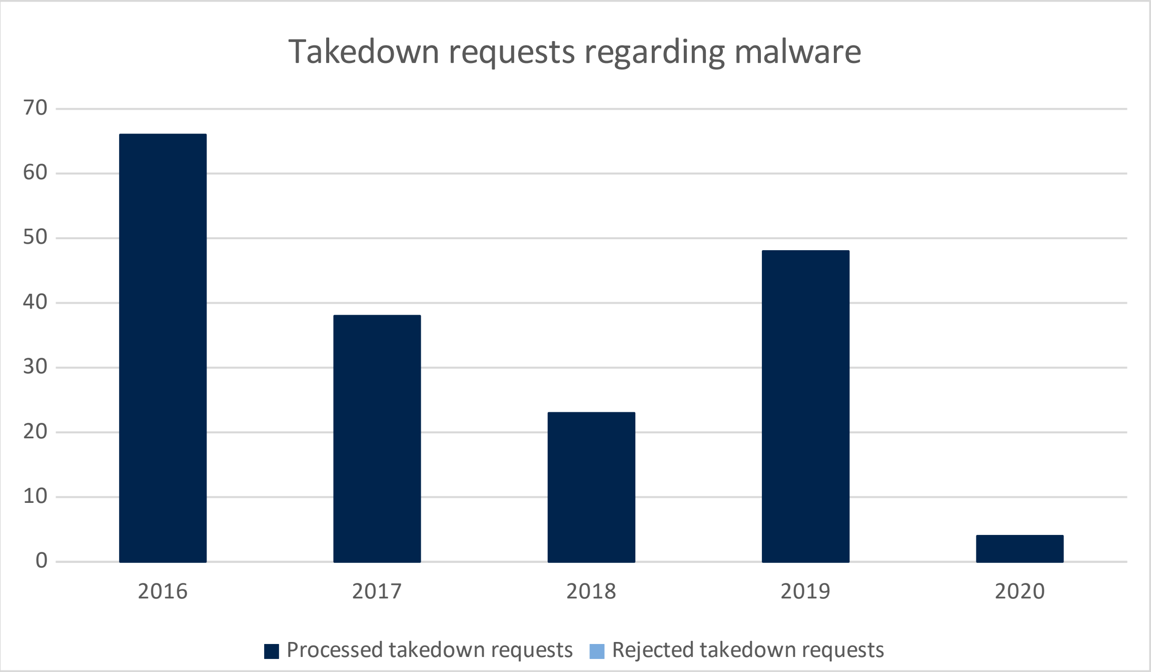
Malware

The table below shows how many complaints BIT received because of the (alleged) hosting of malware and how they were processed.

	2016	2017	2018	2019	2020
Processed takedown requests	66	38	23	48	4
Rejected takedown requests	0	0	0	0	0
Total	66	38	23	48	4

Takedown requests regarding malware

The number of takedown requests regarding malware are displayed in the graph below. This will give you a clear overview of the developments during the years.

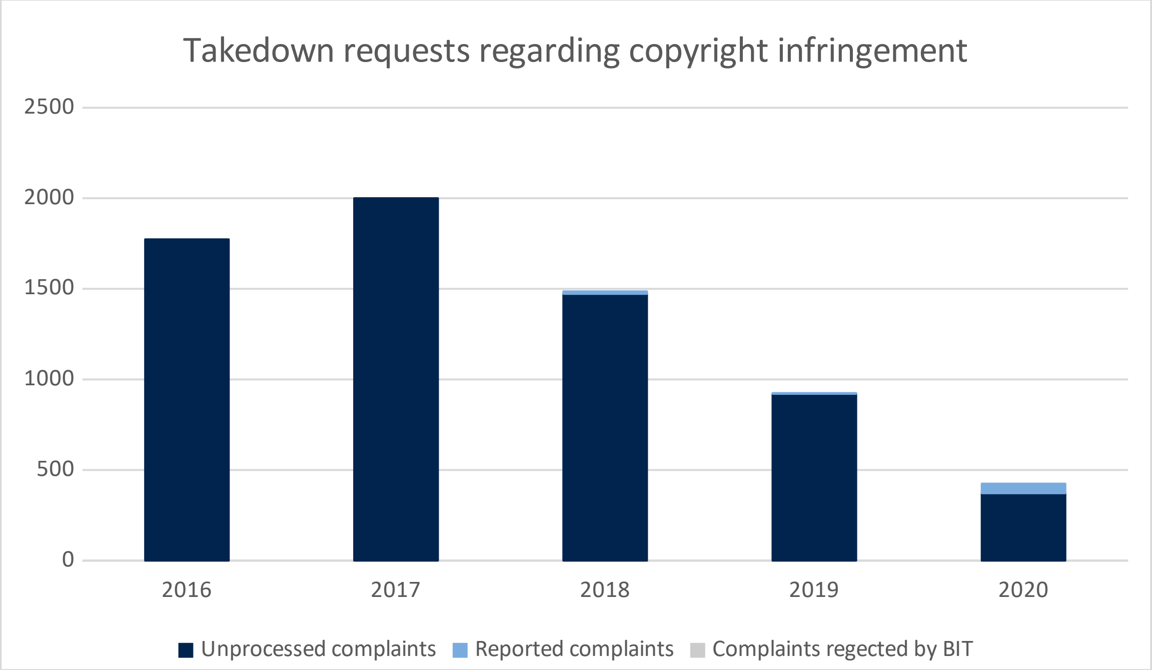


Takedown requests for alleged copyright infringement

In the Transparency Report of 2013 BIT has published data about received and processed notice-and-takedown requests for allegedly infringement of copyright. The numbers for the past five years can be found in the table below.

	2016	2017	2018	2019	2020
Unprocessed complaints	1773	2000	1472	921	372
Complaints rejected by BIT	0	0	0	0	0
Reported complaints	0	0	14	4	53
Total	1773	2000	1486	925	425

Takedown requests regarding copyright infringement
The number of takedown requests regarding copyright infringement are displayed in the graph below. This will give you a clear overview of the developments during the years.

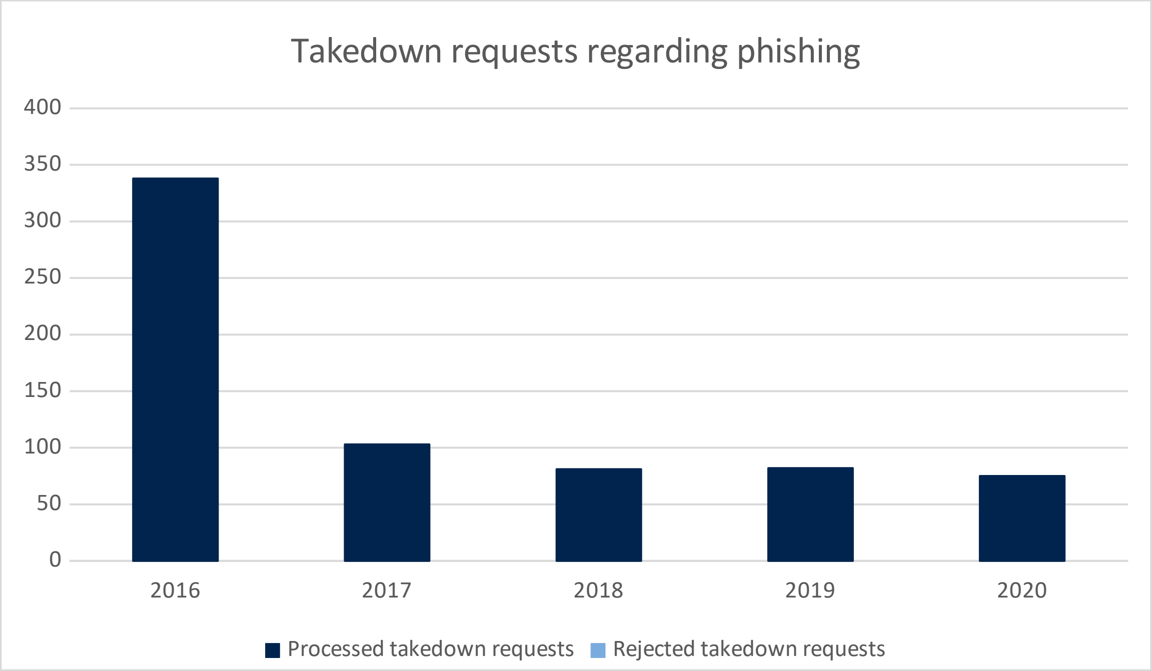


The large number of unprocessed complaints are filed by a small number of parties that automatically file complaints on behalf of the film and music industry. Since they do not comply with our notice and takedown procedure, we have not processed these complaints.

Phishing
The table below contains information about the amount of complaints concerning phishing sites BIT has received and how they were processed.

	2016	2017	2018	2019	2020
Processed takedown requests	338	103	81	82	75
Rejected takedown requests	0	0	0	0	0
Total	338	103	81	82	75

Takedown requests regarding phishing
he number of takedown requests regarding phishing are displayed in the graph below. This will give you a clear overview of the developments during the years.



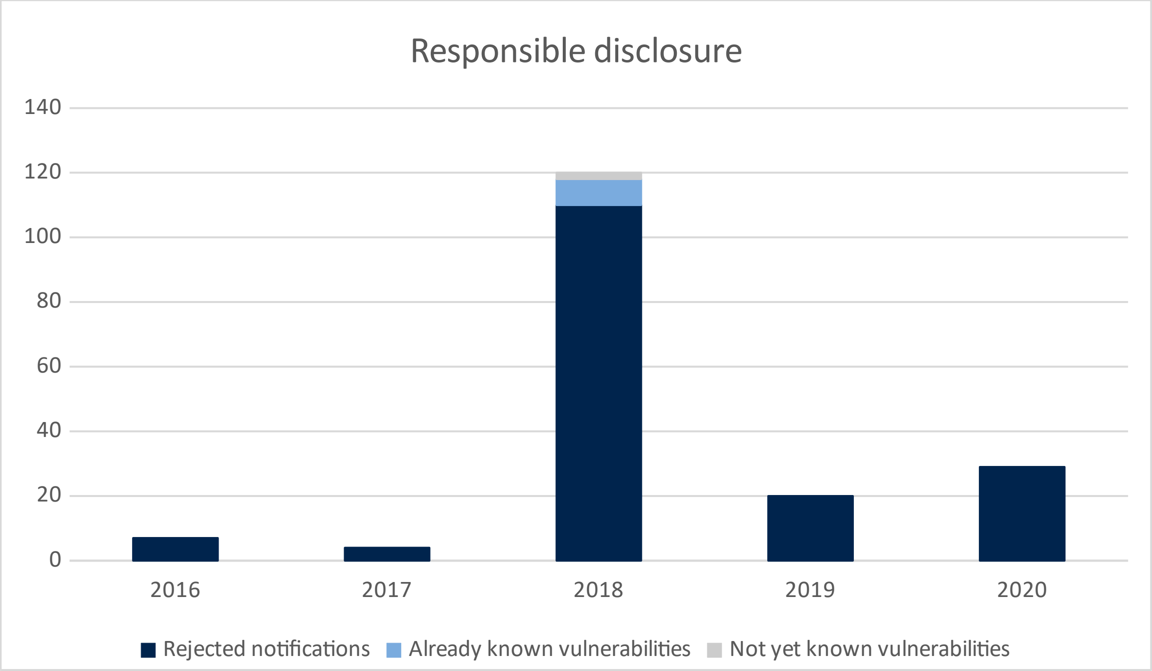
Child pornography
The table below contains information about the amount of complaints concerning child pornography BIT has received and how they were processed.

	2016	2017	2018	2019	2020
Number of complaints accepted	0	0	0	0	0
Number of complaints rejected	0	0	0	0	0
Total	0	0	0	0	0

Responsible disclosure
The table below indicates how many responsible disclosure reports have been made to BIT. In this overview we have made a distinction between rejected notifications, already known vulnerabilities and vulnerabilities that are not yet known to us.

	2016	2017	2018	2019	2020
Rejected notifications	7	4	110	20	29
Already known vulnerabilities	0	0	8	0	0
Not yet known vulnerabilities	0	0	2	0	0
Total	7	4	120	20	29

The number of responsible disclosure notifications that have been reported to BIT are displayed in the graph below. This will give you a clear overview of the developments during the years.



Conclusions and comments
The number of handover request for personal data and legal interception orders remains low. The explanation we gave previous years is that BIT is a corporate ISP and does not (directly) do business with consumers remains applicable here. We have no received tap orders in 2020.

The number of reported malware infections decreased sharply in 2020. This may be explained by the fact that these are reported via other classifications, such as RBL listings.

The number of claims of copyright infringements have decreased again this year. These claims are automatically emailed and all those claims do not comply with our notice and takedown policy.

In the 2019 figures, the number of responsible disclosure reports is reduced after the peak in 2018. Since 2019, we have no longer stated in our responsible disclosure policy that a compensation is given. We receive a relatively large number of reports about matters that are deliberately accessible to the public, where conscious choices have been made in terms of settings or where vulnerabilities have been concluded from version numbers while, for example, backports have been used.