Authority request
disclosure report
2019
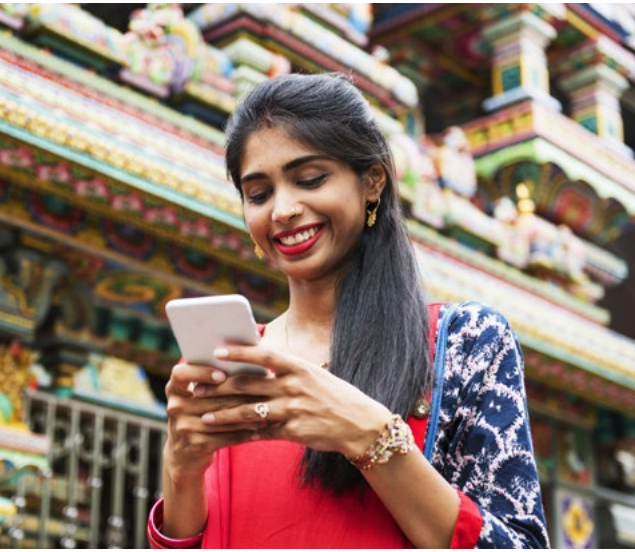
CONTENTS

INTRODUCTION

Respect for privacy and freedom of expression is important for how we at Telenor Group run our business. Our commitment to human rights is long standing and embedded in our top governing document – the Code of Conduct – as well as our Supplier Conduct Principles. Specific operational requirements are included in various policies, including Group-wide requirements for handling authority requests for access to our networks and customer data.

In all our markets there are laws that, in certain circumstances, require operators like Telenor, to disclose information about customers to the authorities or to restrict communication. Our efforts to minimise potentially negative impacts such requests may have on privacy and freedom of expression (e.g. possible misuse) extend to systematic monitoring of incoming requests, initiating dialogue with relevant authorities, the industry and other stakeholders on authority requests, and seeking to be transparent by reporting in this area. This is our sixth annual report[1]. In our 'Legal overview' reports, you can find relevant information about laws applicable within our markets.

Whilst adopting transparency as a default position, we continue to advocate that this report should not reduce the governments' responsibility to inform the public of the extent of such requests.

There are several reasons for this, but most centrally, the same governments who restrict privacy and freedom of expression should also make all reasonable efforts to ensure concerned citizens that these powers are used with due care. It is also important to note that in a few markets, the relevant authorities have direct access to operators' networks and/or communication data, which means that the operator would not have full visibility on how authorities intercept communication.

Some governments publish reports regarding their use of legal powers to access communication information on a regular basis. We encourage all governments to adopt this practice. In the meantime, we view this document as one of our contributions to increased transparency.

---

1 For our first report published in May 2015. Please see our website for more information and previous years' reports:
https://www.telenor.com/sustainability/responsible-business/privacy-and-data-protection/handling-access-requests-from-authorities/

WHY ARE WE REPORTING?

Telenor Group currently has mobile operators in nine countries across Europe and Asia. In each of these countries, there are laws that require telecom operators to disclose information about their customers to government authorities in certain circumstances.

Over the last few years, there has been an important global public debate about the scope, necessity and legitimacy of the legal powers that government authorities use to access the communications of private individuals or to restrict communication. Questions have also arisen as to the role that telecommunications network and service providers play in relation to such access.

Although the authorities have a legitimate need to protect national security and public safety, and to prevent or investigate criminal activities, we recognise that the application of these legal powers in some situations may challenge the privacy and freedom of expression of affected individuals. In light of this, since 2015, Telenor has contributed to transparency in this area.

GOVERNANCE

As a member of the **Global Network Initiative** (GNI), Telenor is fully committed to the **GNI Principles**. This includes a commitment to comply with all applicable laws and respect internationally recognised human rights, wherever we operate. Where national laws, regulations and policies do not conform to international standards, Telenor will seek to avoid, minimise, or otherwise address the adverse impact of government demands, laws, or regulations, and seek ways to honour the principles of internationally recognised human rights to the greatest extent possible.

Telenor's **Board of Directors** has approved the company's human rights policies and exercises oversight with the support of its Sustainability and Compliance Committee The Board of Directors also exercises oversight through its Risk and Audit Committee who has direct reporting from the Head of Group Internal Audit. Telenor's commitment to the GNI Principles is also overseen by the GNI Board of Directors through independent assessments.

At Telenor Group we find that implementation is the key to ensuring that we properly handle requests from authorities. This requires continuous improvement. We achieve this through a system of clear top management ownership, dedicated personnel both at Group and company levels, and systems for checking compliance. Ownership of the Privacy and Sustainability policies are with the Group Executive Vice President for People and Sustainability and they are managed by, respectively, the Group Privacy Officer and the Group Head of Sustainability and People Security.

Telenor Group's compliance management system for authority request is built on international standards. Risk assessments identify challenges and is the starting point for definition of group-wide requirements, controls, training ambitions and compliance follow-up. The specialised compliance management system for authority request is complemented by Telenor Group's general management system for human rights which covers activities ranging from overall human rights due diligence to project- or issue-specific risk assessments.
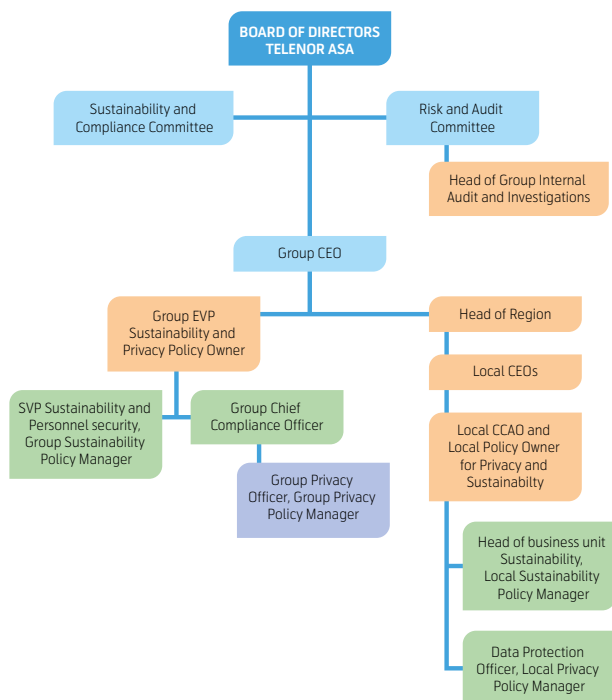
POLICY

In order to address requests from authorities for customer data or access to our networks professionally and systematically we have applied Group-wide requirements to all the mobile operators. These mandatory requirements are part of our **governance framework** and are included in our Sustainability and Privacy policies and underlying manuals.

The authority request manual is managed by the Group Privacy Officer and locally by our Data Protection Officers.
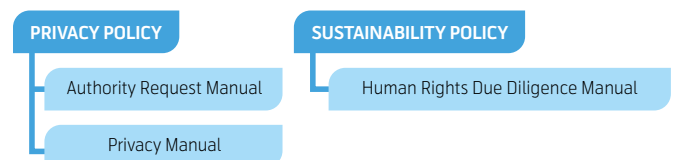
The purpose of our manual on handling authority requests is to ensure proper handling of authority requests in order to limit the risk that our companies' networks are being used to impose illegitimate restrictions to privacy or freedom of expression. It covers lawful intercept and access to historical data, blocking, network shutdown, distribution of authority information and other authority requests with a human rights impact. The manual includes requirements relating to:

- Organisation – including dedicated function(s), reporting to top management, staffed with qualified personnel

- Handling – including checking legal basis and risk of serious human rights impact, challenge and escalation criteria

- Consultation with Group – including process for notification in cases posing significant risk

- Information – including regular updates to company CEO

- Transparency – including a general requirement of transparency to the extent possible

- Record keeping – including legal basis and process steps taken

- Access to remedy – including a requirement to establish a process to receive complaints from users

- Risk assessment & mitigation – including regular reviews of legal frameworks, update of processes, and long-term strategies to minimise negative impact

- Improvement over time – including guidelines issued under the principle of comply or explain

To the extent legally possible and information available (where authorities do not have direct access to the networks), companies also report on an aggregated level the number of requests received annually in the Group non-financial reporting system, which forms the basis for our public reporting.

The privacy policy covers general data protection. In the context of authority request, it informs the principles applied when assessing requests for lawful interception and access to historical data.

The sustainability policy is managed by the Group Head of Personnel Security and Sustainability and by local heads of Sustainability. It covers among other requirements, principles of conducting human rights due diligence.

OUR PROCEDURES

Our local teams across our markets implement procedures for checking that authority requests meet procedural and material requirements for a valid legal basis under local law. When requests lack a clear legal basis or pose a significant risk of serious human rights impact, the local teams shall inform the authority accordingly and refrain from executing the request, to the extent reasonably possible without risking disproportionate reprisals. The local units are also required to interpret requests and legal basis as narrowly as possible.
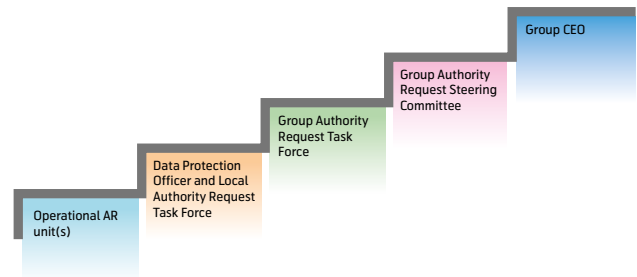
At the local unit level, experts from privacy, legal, sustainability, security, communications, and public and regulatory affairs will assess challenging cases and escalate if needed to the local CEO. A point of contact at the Group level responsible for privacy engages with the local units on these issues, receives the escalations, and summons a Group level team representing the same functions as the local escalation team as required. For any cases that are particularly challenging or of high risk, this team will escalate the request to a high-level steering committee to make a decision, in collaboration with the business unit CEO. If the request cannot be resolved at this level, Group CEO will decide on necessary actions.

Local units are further required to identify risks to customers by monitoring trends in authority requests and legislative initiatives. On that basis, our mobile operators are required to take appropriate action such as promoting incorporation of human rights safeguards into national law or following up historical requests to mitigate human rights impact.

LIMITATIONS

When reading this report, it is important to understand that there are inherent limitations to the report.

a. Limitation based on knowledge and permission

The disclosure in this report is based on what we are permitted to report and what we know:

- In some of the countries where we operate, there are laws that prohibit us from disclosing statistics on authority requests, or that such authority requests had been made at all.

- In some countries the relevant authorities have instructed us not to publish any such information. We have reason to believe that ignoring these instructions could lead to serious sanctions, and in some instances could even pose a threat to our employees.

- In some countries, the law is unclear on whether we are allowed to publish and at the same time, we have reason to believe that publishing could lead to serious sanctions, and in some instances could even pose a threat to our employees.

- In some countries we are legally obliged to allow permanent direct access to our network with no control or visibility over the interception activities that authorities carry out.

For countries where we are unable to report due to any of the reasons above, we have indicated this by inserting a dash (-) in the relevant box in the reporting form.

b. Limitation on impact demonstration

Although the number of requests that we have received and met provide a sense of scale, there are several reasons why these do not provide an accurate picture of the requests' actual privacy and freedom of expression impact. One reason for this is that a single request, depending on the legal framework in each country, may cover an unspecified number of individuals, or communications services or devices used by these individuals. On the other hand, one individual can in many circumstances be subject to several simultaneous or consecutive requests related to the same investigation.

As the above mentioned indicates, there are many variables to consider in order to give a picture that is as accurate as possible of the request's actual privacy and freedom of expression impact. To a large extent, these variables will also be incommensurable from one country to another.

For this reason, we have tried to complement the basic data about number of requests with other information where we have it available, such as the number of account that have had restrictions imposed, the number of sites that are blocked and the subject with which requests are concerned.

DEFINITIONS

LAWFUL INTERCEPT

Covers real-time interception (i.e. wire-tapping, positioning for emergency situations, etc.), in particular:

- Request for real-time access to the content of communications
- Request for real-time access to traffic data
- Request for access to real-time location information, i.e. access to information on the location of mobile terminals/phones

One single request can include several MSISDN, IMEI, USER-ID etc.

HISTORICAL DATA

Covers all requests for the provision of historical data:

- Request for access to any historical traffic or communications data
- Request for access to any subscription data
- Request for access to historical location information
- Request for any other personal information stored by operator – e.g. regarding employees, visitors and surveillance videos.
- Request for other types of customer data such as name, physical address, services subscribed and historical location data.

One single request can include several MSISDN, IMEI, USER-ID etc.

FREEZE OF HISTORICAL DATA

Covers all requests for freeze of data. Requests to provide authorities with access to frozen data are not covered by the concept.

BLOCKING

Covers all requests for blocking including blocking of specific IP-addresses, ports, URLs or of specific OTT services.Shutdown of a full network or of for instance 3G is not counted as blocking, see Network shutdown.

ELEMENTS BLOCKED

This is the total number of blocked elements including URLs, IP addresses, ports, and specific OTT services at the end of the year. Blocking implemented in previous reporting periods which continue to be in place are also included in the numbers we report.

NETWORK SHUTDOWN

Covers shut down of the mobile or fixed network or parts of it. Requests to close down 2G, 3G, 4G, 5G and/or data are also counted.

A single request to shut down a network over several time periods are counted as a single request. Similarly, a single request to shut down a network in several different areas are counted as a single request.

DISTRIBUTION OF AUTHORITY INFORMATION

Covers all requests for sending out information from an authority to all or part of our customer base irrespective of means. The means is typically SMS.

This category does not include requests for distribution of information on commercial basis by means of services that are already effectively offered to all political actors.

ACCOUNT RESTRICTION

This counts the number of requests for restriction(s) of specific accounts. Restrictions may take any form such as denial of access to a specific IP addresses or complete closure of an account

Requests to restrict all accounts, or all accounts with few exceptions, are not counted. See blocking and network shutdown.

NUMBER OF ACCOUNTS AFFECTED

The total number of account affected by requests. If a single account is affected by two different requests, the account is counted twice.

Where the number of accounts affected is not known, the number of MSISDNs may be provided instead. An MSISDN is a unique connection between a phone number and a SIM in a device. The number is in practice the number of SIM cards. Where the number concerns MSISDNs affected, it is explicitly stated.

COMPLAINTS RECEIVED

This includes all complaints received from users due to authority requests. If Telenor receives a complaint from a credible representative of the people impacted by an authority request or from a non-governmental organisation, the complaint is also counted.

POPULATION

As reported by The World Bank, numbers for 2018.

MOBILE SUBSCRIBERS

As reported by Telenor in 2019 Q4 Report.

GDP PER CAPITA (PPP)

As reported by IMF in World Economic Outlook Database, numbers for 2019.

UNDP HUMAN DEVELOPMENT INDEX, GLOBAL RANK

As reported by UNDP in Human Development Index 2019 report

WJP FUNDAMENTAL RIGHTS, GLOBAL RANK

As reported by World Justice Project in Rule of Law Index 2020

GRAMEENPHONE (BANGLADESH)

Basic facts:

Population	161.4 mill.
Mobile subscribers	76.5 mill.
GDP per capita (PPP)	$ 4,993
UNDP Human Development Index, global rank	#135/189
WJP Fundamental Rights, global rank	#122/128

Legal framework:

For details on legal basis, national security powers, crisis / emergency powers, legal restrictions to transparency, and independent oversight, please see our legal overview report.
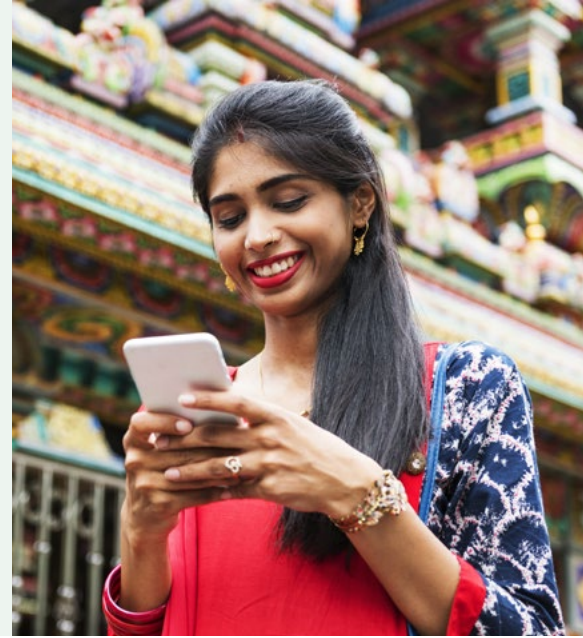
Lawful interception:

No information on requests available for disclosure.

Requests received:	Requests met:
–	–

Historical data:

No information on requests available for disclosure.

Requests received:	Requests met:
–	–

Freeze of historical data:

No information on requests available for disclosure.

Requests received:	Requests met:
–	–

Blocking:

No information on requests available for disclosure.

Requests received:	Requests met:
–	–

Network shutdown:

No information on requests available for disclosure.

Requests received:	Requests met:
–	–

Distribution of authority information:

Requests were received from Bangladesh Telecommunication Regulatory Commission. Requests related to the topics of observing different national/international days, awareness, emergency instructions on cyclones, vaccination, dengue and elections.

Requests received:	Requests met:
222	100%

Account restriction:

No information on requests available for disclosure.

Requests received:	Requests met:
–	–

Complaints received:

The company received no complaints.

Industry disclosure:

The company further contributes to public disclosure through the Association of Mobile Telecom Operators of Bangladesh.

TELENOR DENMARK

Basic facts:

Population	5.8 mill.
Mobile subscribers	1.6 mill.
GDP per capita (PPP)	$ 53,552
UNDP Human Development Index, global rank	#11/189
WJP Fundamental Rights, global rank	#1/128

Legal framework:

For details on legal basis, national security powers, crisis / emergency powers, legal restrictions to transparency, and independent oversight, please see our legal overview report.

Lawful interception:

Requests were received from National Police, including the Danish Security and Intelligence Service.

Requests received:	Requests met:
2,559	71%

Historical data:

Requests were received from National Police, including the Danish Security and Intelligence Service.

Requests received:	Requests met:
2,190	68%

Freeze of historical data:

Requests were received from National Police, including the Danish Security and Intelligence Service.

Requests received:	Requests met:
350	75%

Blocking:

Requests were received from National Police, Danish Gambling Authority, and "Rettighedsalliancen" (a private organisation composed of IP rights holders).

Requests related to the topics of Infringement of IP rights, Illegal Gambling and child sexual abuse materials.

Requests received:	Requests met:
16	100%

504 elements were blocked at the end of the year. For all elements, users will be notified of the blocking when trying to access the elements concerned.

Network shutdown:

No requests received.

Requests received:	Requests met:
0	–

Distribution of authority information:

No requests received.

Requests received:	Requests met:
0	–

Account restriction:

No requests received.

Requests received:	Requests met:
0	–

Number of accounts affected: 0.

Complaints received:

The company received no complaints.

Industry disclosure:

The company further contributes to public disclosure through Danish Telecom Industry Association.

See in particular the list of blocked sites: http://www.teleindu.dk/brancheholdninger/blokeringer-pa-nettet/

DIGI (MALAYSIA)

Basic facts:

Population	31.5 mill.
Mobile subscribers	11.3 mill.
GDP per capita (PPP)	$ 32,455
UNDP Human Development Index, global rank	#61/189
WJP Fundamental Rights, global rank	#80/128

Legal framework:

For details on legal basis, national security powers, crisis / emergency powers, legal restrictions to transparency, and independent oversight, please see our legal overview report.

Lawful interception:

No information on requests available for disclosure.

Requests received:	Requests met:
–	–

Historical data:

Requests were received from various Law Enforcement Agencies (LEA) i.e. the Royal Malaysian Police, Malaysian Communications and Multimedia Commission, Malaysian Anti-Corruption Commission, Royal Malaysian Custom, Ministry of Health, Securities Commission of Malaysia and others; directly or via a court order.

47% of requests concerned subscriber profile information only, 3% of requests concerned call data records (CDR) only, 37% of requests concerned a combination of subscriber profile information and CDR only, and 13% concerned other combinations of data. No requests concerned content.

Requests received:	Requests met:
24,214	94%

Freeze of historical data:

No requests received.

Requests received:	Requests met:
0	–

Blocking:

Requests were received from the Malaysian Communications and Multimedia Commission and The Ministry of Domestic Trade and Consumer Affairs. The requests are related to the topics of copyright issues, online gambling, phishing, pornography, trade description, unregulated health and cosmetic products, unverified news and other categories (breach to Accounting Act, Business Registration Act, Personal Data Protection Act, Dangerous Drug Act and Penal Code).

Requests received:	Requests met:
175	98%

1,611 elements were blocked at the end of the year[2]. Users will be notified of the blocking when trying to access the elements concerned.

Network shutdown:

No requests received.

Requests received:	Requests met:
0	–

Distribution of authority information:

83% of requests were received from the Royal Malaysian Police, and 17% from Malaysia: National Disaster Management Agency

Requests related to the topics of missing children and events of natural disaster.

Requests received:	Requests met:
23	87%

Account restriction:

Requests were received from the Malaysian Communications and Multimedia Commission, relating to illegal advertisements (breach to by-law) and advertisement by loan sharks.

Requests received:	Requests met:
9	100%

Number of accounts affected: 389 MSISDNs

Complaints received:

The company received no complaints.

2 Please note that the number includes blocking of pages containing child sexual abuse materials.

TELENOR MYANMAR

Basic facts:

Population	53.7 mill.
Mobile subscribers	22.3 mill.
GDP per capita (PPP)	$ 6,711
UNDP Human Development Index, global rank	#145/189
WJP Fundamental Rights, global rank	#125/128

Legal framework:

For details on legal basis, national security powers, crisis / emergency powers, legal restrictions to transparency, and independent oversight, please see our legal overview report.

Lawful interception:

No requests received.

Requests received:	Requests met:
0	–

Historical data:

86% of requests were received from Post and Telecommunication Department and 14% from the Anti-Trafficking in Persons Division.

27 % of requests concerned murder cases, 17% concerned drug cases, 14% concerned missing person cases, 13% concerned human trafficking, unlawful association and suspected terrorism cases, and 6% concerned kidnapping cases. Other topics of requests were arms/explosive device, terrorism, counterfeit currency, robbery, anti-corruption, intimidation, defamation, rape/child sexual abuse, fraud, theft, intention to cause death and mining.

Requests received:	Requests met:
70	86%

Freeze of historical data:

No requests received.

Requests received:	Requests met:
0	–

Blocking:

No requests received.

Requests received:	Requests met:
0	–

0 elements were blocked at the end of the year.

Network shutdown:

Requests were received from Ministry of Transport and Communications (MOTC).

Requests received:	Requests met:
1	100%

The company notified affected subscribers of the network shutdown.

Distribution of authority information:

Requests were received from Post and Telecommunication Department (PTD). Requests related to the topics of mainly earthquake, flood warning, vaccination, drugs and human trafficking.

Requests received:	Requests met:
116	28%

Account restriction:

No requests received.

Requests received:	Requests met:
0	–

Number of accounts affected: 0.

Complaints received:

The company received no complaints.

TELENOR NORWAY

Basic facts:

Population	5.3 mill.
Mobile subscribers	2.9 mill.
GDP per capita (PPP)	$ 76,738
UNDP Human Development Index, global rank	#1/189
WJP Fundamental Rights, global rank	#2/128

Legal framework:

For details on legal basis, national security powers, crisis / emergency powers, legal restrictions to transparency, and independent oversight, please see our legal overview report.

Lawful interception:

33% of requests were received from the Police. 22% of requests from the Police were related to emergency / rescue. The Rescue Centre sent 67% of requests, all of which were related to active positioning for emergency / rescue.

Total requests received:	Requests met:
1,046	100%

Historical data:

No requests related to content.

Total requests received:	Requests met:
6,047	100%

Freeze of historical data:

Total requests received:	Requests met:
102	100%

Blocking:

No requests received.

Requests received:	Requests met:
0	–

0 elements were blocked at the end of the year.

Network shutdown:

One request was received from National Police. The request related to a bomb threat on an airplane in Alta.

Requests received:	Requests met:
1	100%

The company did not notify affected subscribers of the network shutdown.

Distribution of authority information:

No requests received.

Requests received:	Requests met:
0	–

Account restriction:

No requests received.

Requests received:	Requests met:
0	–

Number of accounts affected: 0.

Complaints received:

The company received no complaints.

TELENOR PAKISTAN

Basic facts:

Population	212.2 mill.
Mobile subscribers	45.4 mill.
GDP per capita (PPP)	$ 5,839
UNDP Human Development Index, global rank	#152/189
WJP Fundamental Rights, global rank	#115/128

Legal framework:

For details on legal basis, national security powers, crisis / emergency powers, legal restrictions to transparency, and independent oversight, please see our **legal overview report**.

Lawful interception:

No information on requests available for disclosure.

Requests received:	Requests met:
-	-

Historical data:

No information on requests available for disclosure.

Requests received:	Requests met:
-	-

Freeze of historical data:

No information on requests available for disclosure.

Requests received:	Requests met:
-	-

Blocking:

No requests received.

Requests received:	Requests met:
0	-

0 elements were blocked at the end of the year.

Network shutdown:

Requests were received from telecom regulator Pakistan Telecommunication Authority on behalf of Ministry of Interior and all requests were in context of matters relating to National Security.

Requests received:	Requests met:
43	100%

The company did not notify affected subscribers of the network shutdown.

Distribution of authority information:

Requests were received from Pakistan Telecommunication Authority and were related to the topics of Public Awareness, Health and Safety.

Requests received:	Requests met:
37	97%

Account restriction:

No requests received.

Requests received:	Requests met:
0	-

Number of accounts affected: 0.

Complaints received:

The company received no complaints.

TELENOR SWEDEN

Basic facts:

Population	10.2 mill.
Mobile subscribers	2.8 mill.
GDP per capita (PPP)	$ 54,071
UNDP Human Development Index, global rank	#8/189
WJP Fundamental Rights, global rank	#4/128

Legal framework:

For details on legal basis, national security powers, crisis / emergency powers, legal restrictions to transparency, and independent oversight, please see our legal overview report.

Lawful interception:

All requests were received from the police authority.

Requests received:	Requests met:
2,466	98%

Historical data:

Requests were received from the police authorities, Swedish customs, the tax authority, the Swedish economic crime authority, and from private parties (intellectual property right holders) after a court order.

Requests received:	Requests met:
7,581	94%

Freeze of historical data:

No requests received.

Requests received:	Requests met:
0	-

Blocking:

Requests were received from private parties after court orders. The requests concerned blocking of sites on which content were made available without approval of the intellectual property right holder.

Requests received:	Requests met:
2	100%

Four elements were blocked at the end of the year. For all four elements, users will be notified of the blocking when trying to access the elements concerned.

Network shutdown:

No requests received.

Requests received:	Requests met:
0	-

Distribution of authority information:

Requests were received from the Swedish Civil Contingencies Agency (MSB). All request were emergency relief warning SMS-messages (fires, floods, etc.).

Requests received:	Requests met:
77	100%

Account restriction:

No requests received.

Requests received:	Requests met:
0	-

Number of accounts affected: 0.

Complaints received:

The company received no complaints.

Disclosure by public institutions:

Further information can be obtained from relevant public institutions. See in particular:

The Swedish Commission on Security and Integrity Protection: https://www.sakint.se/

The Swedish Prosecution Authority: https://www.aklagare.se/nyheter-press/pressmeddelanden/2019/maj/redovisning-av-hemliga-tvangsmedel/

DTAC (THAILAND)

Basic facts:

Population	69.4 mill.
Mobile subscribers	20.6 mill.
GDP per capita (PPP)	$ 20,474
UNDP Human Development Index, global rank	#77/189
WJP Fundamental Rights, global rank	#90/128

Legal framework:

For details on legal basis, national security powers, crisis / emergency powers, legal restrictions to transparency, and independent oversight, please see our legal overview report.

Lawful interception:

No requests received.

Requests received:	Requests met:
0	–

Historical data:

Requests received:	Requests met:
19,674	≈100%

Freeze of historical data:

No requests received.

Requests received:	Requests met:
0	–

Blocking:

Requests received:	Requests met:
191	99%

78,675 elements were blocked at the end of the year[3].

Network shutdown:

Requests received:	Requests met:
1	0%

Distribution of authority information:

Requests received:	Requests met:
5	100%

Account restriction:

No requests received.

Requests received:	Requests met:
0	–

Number of accounts affected: 0.

Complaints received:

The company received no complaints.

3 Please note that the number includes blocking of pages containing child sexual abuse materials.