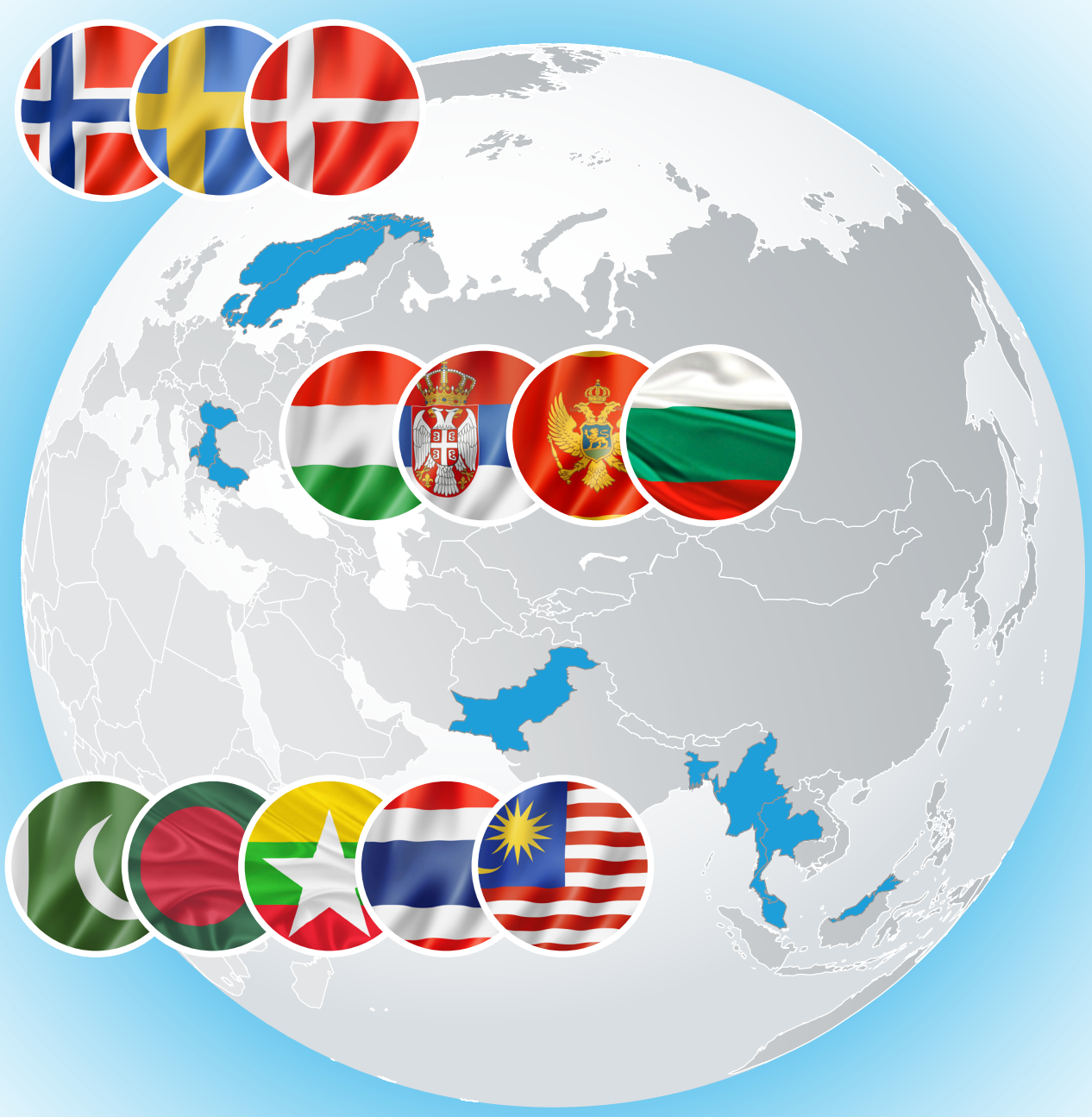
telenor group

AUTHORITY REQUESTS DISCLOSURE REPORT

2017



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. 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 fourth report[1]. We have also added one more country (Singapore) to our Legal Overview report.

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. First of all, the same governments that impose such laws should also make all reasonable efforts to ensure concerned citizens that these powers are used with due care. Furthermore, no operator has the complete overview of the authority requests throughout each country, as such requests are issued to all operators present. A complete overview would require that all operators issue similar reports.

Moreover, operators are likely to use different approaches when reporting the same kind of information, making comparison difficult. Some may for example count the actual number of requests received from the authorities, whereas others may count the total number of users, devices, etc., affected by the request. And when the authorities issue the same request to several operators, each operator would include this request in its statistics, risking an artificially inflated number. 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 visibility on the number of lawful interceptions or extraction of communication data taking place.

Some governments do 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.

WHY ARE WE REPORTING?

Telenor Group currently has mobile operators in 12 countries across Europe and Asia[2]. 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. 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.

HOW TO READ THIS REPORT

The purpose of this section is to help our readers better understand how we approach authority requests. Through provision of the motivation, scope, relevant limitations of the report as well as Telenor's position in this area, we hope that our readers will be equipped with context and background for reading this transparency reporting.

WHAT ARE AUTHORITY REQUESTS?

Most countries have laws that require telecom operators to assist the authorities on certain conditions. These requests can be categorized as:

- Communication data: Obtaining historical telecommunications data from the network;
- Lawful interception: Intercepting communication in real time;
- Network shutdowns: Requiring shut down of the operators network in part or in full;
- Content restrictions: Impose restriction on electronic content distributed through its network , such as blocking of URLs; and
- Content distribution: Require the operators to distribute information from the government to the public, typically through mass distribution of SMS.

[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/ Telenor India was considered a discontinued operation as of our Q1 2017 financial reportin: https://www.telenor.com/wp-content/uploads/2017/05/TEL-Q1-2017-f3c1652d76877ffa55827939ab8e11f0.pdf

[2] Telenor India was considered a discontinued operation as of our Q1 2017 financial reportin: https://www.telenor.com/wp-content/uploads/2017/05/TEL-Q1-2017-f3c1652d76877ffa55827939ab8e11f0.pdf

Expectedly, not all requests from authorities fall neatly into these 5 categories.

The circumstances in which the authorities can put forward these requests differ from country to country. Some of the grounds include:

- Investigation of suspected crime and fraud;
- National security purposes; and
- Protecting safety and security of people.

HOW DOES TELENOR PROCESS REQUESTS?

Telenor processes all requests from authorities based on a coherent set of rules outlined in our Authority Requests Manual. Under the Manual, all requests are processed by a competent team, who assess according to a set of criteria, including the legal basis and human rights impact of the requests.

Each request is assessed on an individual basis, and in the event that requests are assessed to be uncommon,[3] or pose substantial impact to human rights, such request is escalated to relevant function within a hierarchy of escalation points of contact, including CEO and a task force consisting of cross function experts in this area.

WHAT ARE WE REPORTING?

Our report indicates the number of requests received from authorities by our businesses in each country for the year 2017 in each of the categories mentioned above: communication data, lawful interception, network shutdowns, content restrictions and content distribution.

LIMITATIONS TO THIS REPORT

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

a. Limitation base 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 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 where the law on such disclosure is unclear, 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 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 these numbers 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 side, 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 further information on how we approach authority requests please see www.telenor.com/privacy

[3] Within Telenor, uncommon requests refer in general to 'major events' within Industry Dialogue Guiding Principle.

Grameenphone (Bangladesh)

General note on laws/regulations

Bangladesh has specific laws relating to interception of communications and acquisition of communications data. A single, widely drafted, provision outlined in the Bangladesh Telecommunications Regulatory Act, 2001 enables these monitoring activities to be undertaken on the grounds of national security and public order by the designated law enforcement agencies, security and intelligence agencies etc. Bound by the legal stipulations, the mobile network operators (MNOs) are required to comply with these lawful interception requests channelized under a defined process to the dedicated interface within the organization. The records of sharing such information are maintained as part of an in-built control mechanism of the process. Although the law provides for little or no regulatory oversight over the exercise of such interception powers of government, however, scope of general judicial oversight is available.

Communication data	Lawful interception	Network shutdowns	Content restrictions	Content distribution
-	-	-	72	-

Telenor Bulgaria

General note on laws/regulations

In Bulgaria, specified state security, intelligence and law enforcement authorities have powers to intercept communications. Interception and other powers are subject to a process of court approval set out in the Special Intelligence Means Act and the Electronic Communications Act. These powers can be authorized to investigate serious willful crimes, incl. national security-related offences. Currently same is applicable to acquiring communications data. There is overarching political oversight that includes a dedicated parliamentary committee in the legislature. Content restrictions in 2016 are executed only in compliance with the specific legislation as a measure against illegal gambling without court permission.

Communication data	Lawful interception	Network shutdowns	Content restrictions	Content distribution
27,291	-	0	562	0

Telenor Denmark

General note on laws/regulations

Under Danish Law, there is a general rule that the police may only order interceptions or acquire communications data from communication service providers (CSPs) having first obtained a court order to do so. An interception can only be authorised in relation to the most serious alleged offences. CSPs are obliged to cooperate with such orders. The Ministry of Justice has statutory authority to investigate any non-compliance by the police with the court approval process. Police may use radio frequencies without authorization in order to disturb and disrupt radio and telecommunications as part of interceptions undertaken pursuant to § 791c of the Administration of Justice regarding interception of communications, observation and data reading.

Communication data	Lawful interception	Network shutdowns	Content restrictions	Content distribution
1,686	2,646	0	5*	0

* Content restrictions only takes place on the basis of a court order. The blockings are DNS blockings. The industry association TI (TeleIndustrien) maintains a list of blocked websites which all telecom operators in Denmark are obligated to comply with: http://www.teleindu.dk/brancheholdninger/blokeringer-pa-nettet/

Telenor Hungary

General note on laws/regulations

In Hungary, interceptions of communications can only be requested by law enforcement authorities (e.g. police, public prosecutor, intelligence agencies) using a process for handling classified data. Requests may be applied only on the basis of a court order, or in case of certain intelligence agencies, an authorization from the Minister of Justice, which can be sought retrospectively in urgent cases. The interceptions are performed by a dedicated authority, the Special Services for National Security (SSNS). Therefore the SSNS is responsible for the verification of the court order or the authorization from the Minister of Justice. Further, besides law enforcement authorities, a range of other public authorities may request subscriber or traffic data directly from the communication service providers (CSPs), which is also regulated by the law and restricted in terms of the period and type of data.

Communication data	Lawful interception	Network shutdowns	Content restrictions	Content distribution
55,975	-	-	211	-

Digi (Malaysia)

General note on laws/regulations

Malaysia has various laws that allow the police extensive powers to intercept communications and the right to acquire communication data in order to assist their investigation on any criminal offence, for purposes of crime prevention and national security. However, the power to intercept communications is only exercisable with a prior authorization from the Public Prosecutor.

Under specific laws, Government Agencies have the authority to acquire specific types of communications data, issue an authoritative direction for network shut down and restrict the publication of sensitive content.

Communication data	Lawful interception	Network shutdowns	Content restrictions	Content distribution
13,564	-	0	-	2

Telenor Montenegro

General note on laws/regulations

In Montenegro, interception of electronic communications can be undertaken directly by the Agency for National Security (ANS) on national security grounds. There is a well-defined process of judicial approval. Only the Supreme Court has authority to allow the intelligence agencies to undertake an interception on national security grounds. The police can obtain customer communications data by submitting a court order (in cases of police activity related to finding or rescuing people which are not conducted for the purpose of criminal investigation or prosecution, network operators and service providers may, even without a court order, disclose the retained communication data to the police). As well as the role the judiciary plays in interceptions, there are constitutional rights in relation to confidentiality of communications, and regulatory oversight of the police and the ANS.

Communication data	Lawful interception	Network shutdowns	Content restrictions	Content distribution
485	-	0	0	0

Telenor Montenegro

General note on laws/regulations

In Montenegro, interception of electronic communications can be undertaken directly by the Agency for National Security (ANS) on national security grounds. There is a well-defined process of judicial approval. Only the Supreme Court has authority to allow the intelligence agencies to undertake an interception on national security grounds. The police can obtain customer communications data by submitting a court order (in cases of police activity related to finding or rescuing people which are not conducted for the purpose of criminal investigation or prosecution, network operators and service providers may, even without a court order, disclose the retained communication data to the police). As well as the role the judiciary plays in interceptions, there are constitutional rights in relation to confidentiality of communications, and regulatory oversight of the police and the ANS.

Communication data	Lawful interception	Network shutdowns	Content restrictions	Content distribution
485	-	0	0	0

Telenor Myanmar

General note on laws/regulations

The Telecommunications Law 2013 gives the government of Myanmar broad powers of interception on a number of broadly stated grounds, including when it is in the public interest, and when the security of the State or the rule of law is adversely affected. The Law also appears to provide for acquisition of communications data powers, though these are less clearly stated. There is no judicial approval or oversight of the use of these powers. There is a form of government approval required, but the Law does not state what this entails.

Communication data*	Lawful interception	Network shutdowns	Content restrictions	Content distribution
49	0	0	0	3

*Topic also addressed in Telenor Myanmar Sustainability Briefing

Telenor Norway

General note on laws/regulations

In Norway, only the Police or the Police Security Service (PST) can carry out interception of communications to investigate serious crimes or national security related offences. Generally they may only do so under a court order issued by a district court, but interceptions without a court order are allowed in a few tightly defined scenarios. Access to communications data is governed by similar rules. There is regulatory oversight of the activities of the police, and parliamentary oversight over the PST and other intelligence agencies.

Communication data	Lawful interception	Network shutdowns	Content restrictions	Content distribution
7144*	1,100**	0	0	0

*A summation of different type of requests related to historical traffic data (metadata), signaling data, terminal data, use of ip.-addresses., subscription information and customer information.

** A summation of requests related to emergency situations (positioning) and lawful interceptions. The distribution between these type of requests is 60(emergency):40(LI).

Telenor Pakistan

General note on laws/regulations

The Pakistan Telecommunications (Re-Organisation) Act 1996 gives the Federal Government of Pakistan powers to authorise any person to intercept communications for national security reasons or for the investigation of any crime. These powers also extend to the acquisition of communications data without any requirement of prior judicial approval for obtaining/intercepting such data. However for the terrorism-related offences listed in the Investigation for Fair Trial Act, 2013 (IFTA 2013), there is a process given therein, requiring Court's approval for interception and acquisition of communications data relating to such terrorism-related offences.

Communication data	Lawful interception	Network shutdowns	Content restrictions	Content distribution
-	-	-	-	-

Telenor Serbia

General note on laws/regulations

Serbian law allows the police and certain state security agencies to intercept communications for the purposes of criminal investigations, or linked to national security related offences. Court approval is required, from the Higher Court in Belgrade for national security purposes, or order from any Judge for preliminary criminal proceedings, for investigation of serious or organized crime. A court order is also required for disclosure of communications data. There is a degree of regulatory and political oversight over all these activities.

Communication data	Lawful interception	Network shutdowns	Content restrictions	Content distribution
482	-	0	0	-

Telenor Sweden

General note on laws/regulations

Interception by government agencies of domestic communications in Sweden can only be carried out under a court order, and only in relation to serious crimes, which include espionage and terrorism. Government agencies have discretion to access specified types of communications data in certain scenarios without a court order, notably the police. Domestic interceptions are subject to a process of judicial approval and supervision.

Communication data	Lawful interception	Network shutdowns	Content restrictions	Content distribution
6,065	2,521	0	0	0

dtac (Thailand)

General note on laws/regulations

Following a coup d'etat on 22 May 2014, Thailand is currently governed by the interim Government under the National Council for Peace and Order under the interim Constitution. A state of martial law which had been imposed since the beginning of the coup was lifted on 1 April 2015 and immediately replaced by NCPO Order No. 3/2558 (3/2015) re: Maintaining Public Order and National Security issued under Section 44 of the Interim Constitution for an indefinite period of time. This order empowers officials to gather, acquire and examine any data. Ordinarily the law broadly empowers officials to gather data for examination. In addition, some new legislation in this area is currently under consideration.

Communication data	Lawful interception	Network shutdowns	Content restrictions	Content distribution
-	-	-	-	-