



Country-by-Country Disclosure of Law Enforcement Assistance Demands 2015-16

Country-by-Country Disclosure of Law Enforcement Assistance Demands

As explained in our [Law Enforcement Disclosure Statement](#), Vodafone's global business consists largely of a group of separate subsidiary companies, each of which operates under the terms of a licence or other authorisation issued by the government of the country in which the subsidiary is located, and each of which is subject to the domestic laws of that country.

In this section, we provide a country-by-country insight into the nature of the local legal regime governing law enforcement assistance, together with an indication of the volume of each country's agency and authority demands, wherever that information is available and publication is not prohibited. In addition, a summary of some of the most relevant legal powers in each of our countries of operation can be found in our [Legal Annexe](#), which has been updated to include a new section covering the current laws that relate to encryption and law enforcement assistance – the first time such an analysis has been published, along with an update of the legal position in those countries that have new laws in force.

The latest version of the Legal Annexe includes an update on the legal position in 13 countries where new laws have come into force since our last report was published (and at the point in time – spring 2016 – when this most recent analysis was conducted). It is worth noting that

at the time of updating the existing content in the Legal Annexe (spring 2016), new laws were proposed or pending in several more of our countries of operation including Ghana, Hungary, Ireland, Lesotho, Malta, Mozambique, Netherlands, South Africa, Turkey and the UK.

As we explained [earlier](#), this remains a difficult section to compile. There is still no established model to follow: few international telecommunications operators have published a country-by-country report of this kind and very few have done so on the basis of data gathered by the local licensed telecommunications operator. Additionally, there are no standardised methods for categorising the type and volume of agency and authority demands: different governments, parliaments, regulators, agencies and authorities apply a variety of definitions when authorising or recording the types of demands outlined [earlier](#), as do operators themselves when receiving and recording those demands.

Over the last year, where possible, we have sought to engage with a number of governments, agencies and operators to explore options for a more consistent and meaningful approach to statistical recording and public disclosure which would enable a greater level of overall transparency. On the whole it has proven to be difficult to persuade others of the case for change which would bring a higher level of coherence to any statistical analysis of the data presented in this report. Updates on our efforts to enhance transparency in individual countries can be found in the relevant country reports.



How we prepared this report

Each of our local operating businesses has a nominated Disclosure Officer responsible for the management and administration of law enforcement assistance in response to a demand. The information collated and published here (wherever available and wherever publication has not been prohibited) has been overseen by the relevant Disclosure Officer.

As explained [earlier](#), only government-cleared Vodafone employees in each country in which we operate will be made aware of specific lawful demands issued by agencies and authorities and will not typically be made aware of the context of any demand.

Although the details of individual demands remain highly confidential and cannot be communicated, Vodafone's internal auditors conduct regular reviews of the overarching processes and policies that are in place to ensure the integrity of our law enforcement disclosure systems.

For the two categories of agency and authority demand reported here – lawful interception and communications data (as explained [earlier](#)) – we have robust processes in place to manage and track each demand.

It should be noted that, while the statistics for communications data demands are overwhelmingly related to communications

metadata, the statistics we report also include demands for other types of customer data such as name, physical address and services subscribed. Our reporting systems do not necessarily distinguish between the types of data contained in a demand, and in some countries a single demand can cover several different types of data.

Our global internal review, which analysed, on a country-by-country basis, the extent to which we can lawfully publish aggregate volumes of law enforcement assistance demands at a local level, remains relevant with no changes to note.

As was the case in 2014, we have also published a [Legal Annexe](#) in which we set out the laws and practices, on a country-by-country basis, that limit or prohibit disclosure. We believe this form of transparency is as important as the publication of aggregate demand statistics themselves in terms of ensuring greater public understanding. In 2016, we worked with Hogan Lovells to update the existing content of this Annexe for those countries that have new laws in force (as at May 2016). For the first time, we also cover the main laws relating to encryption in the context of law enforcement assistance in the telecommunications sector, in each of the 28 countries covered here.

As we noted in our first disclosure in 2014, it remains the case that in some countries there is a lack of legal clarity regarding disclosure of the aggregate number of law

enforcement demands. Where this continued to be the case, we have, once again, sought to engage with governments to ask for guidance wherever this was practicable in light of the potential risks to our employees.

In a small number of countries where the government does publish statistics but where there remain concerns regarding the methodology used in recording and/or reporting this information, we summarise the discussions undertaken to try to enhance transparency in the relevant country section. Further information about our approach under those circumstances is set out [earlier](#).

Some governments responded to our requests for guidance, and their views are summarised in the relevant country section in this section of the report. Others continued to decline to reply to our enquiries altogether or have made it known to us that they remain reluctant to provide any indication of their perspectives. Where this is the case, we have taken a precautionary approach to protect our employees.

Finally, in countries experiencing continuing periods of significant political tension, it remains challenging to ask any questions related to national security and criminal investigation matters – however seemingly innocuous – without potentially putting Vodafone employees at risk of harassment or criminal sanction.

Explanation of the information presented

In each country and for each of the two [categories](#) of law enforcement demands issued, there are a number of different outcomes arising from our enquiries.

Wherever there are no restrictions preventing publication and there are no alternative sources of information indicating total demand volumes across all operators in the country as a whole, we have published the data available from our own local operating business indicating the cumulative number of demands received by Vodafone during the period under review. However, we have noted our concerns about the considerable shortcomings inherent to this approach, as explained [earlier](#).

It remains clear to us that in those countries where the government publishes certain statistical information and individual operators also publish some of the statistics held for their own operations, the net effect is more confusing. In statistical terms, the data is irreconcilable and contradictory. It would be more effective if the governments involved played a greater role in enabling the provision of consistent and comprehensive metrics spanning the industry as a whole.

It is also important to emphasise that attempts to compare one country's metrics with those of another are essentially meaningless given the very wide variations between legal frameworks, recording methodologies and reporting regimes. There are no consistent points of common reference that could be used to underpin such analysis. Similarly, in many cases it is difficult to draw accurate conclusions from year-on-year changes in reported metrics within a country as these can be influenced by a range of factors. These could include amendments to legislation or new laws, developments in agency or authority practice, or changes to the approach used to log, aggregate and disclose lawful demands – which may not in themselves provide a reliable indication of actual trends in law enforcement activity. There are five circumstances under which we have not published Vodafone's own statistical information for a specific country, as set out below.

1. Vodafone disclosure unlawful

The law prohibits disclosure of the aggregate demand information held by Vodafone as well as any disclosure related to the mechanisms used to enable agency and authority access, as explained [earlier](#). This is particularly the case in matters related to national security. Wherever this is the case, we cite the relevant law that restricts us from disclosure, either in the main text or in the [Legal Annex](#).

2. No technical implementation of lawful interception

In some countries, there is no legal provision for implementation or we have not been

required to implement the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance. This includes circumstances under which lawful interception powers exist under the law but the technical arrangements to conduct this have not been mandated.

3. Unable to obtain guidance

The law on disclosure is unclear and we have been unable to engage with the government or a relevant agency or authority to discuss options for publication during a period of political tension and consequent risk to our employees.

4. Cannot disclose

Although local laws do not expressly prohibit disclosure, the authorities have told us directly that we cannot disclose this information.

5. Government/other public body publishes

In a number of countries, the government, parliament or a credible independent public body such as a regulator already publishes statistical information for certain types of demand issued to all operators in that country. Wherever this is the case, we provide a link to the information available online. In some countries – and where relevant – we also provide additional commentary on the status of that third-party information. Our views on disclosure of relevant information by governments rather than by operators are summarised [earlier](#).



Albania

	Type of demand	
	Lawful interception	Communications data
Statistics	Vodafone disclosure unlawful (1)	5,529 (2)
Key Note (1)	It is unlawful to disclose any aspect of how lawful interception is conducted.	
Key Note (2)	Prior to the 2014 report, the legal position was unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands. We asked the authorities for guidance and were informed that we could disclose this information in the 2014 report. There has been no change to the guidance since that report and we have therefore updated this statistic with the latest information we hold for our own local operating business.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

Australia

	Type of demand	
	Lawful interception	Communications data
Statistics	Government/other public body publishes (1, 2)	Government/other public body publishes (1, 2)
Key Note (1)	The Australian Communications and Media Authority publishes statistical information related to lawful interception and communications data demands issued by agencies and authorities.	
Key Note (2)	<p>On 13 October 2015, the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 came into force and amended the existing Telecommunications (Interception and Access) Act 1979 (the TIA Act) to include new mandatory data retention requirements.</p> <p>Under the TIA Act, the Attorney General provides a public report on an annual basis which summarises information provided to him/her by law enforcement agencies. This includes, at a high level, the number of law enforcement demands for access to communications data together with the age of the data sought, among a range of other information.</p> <p>With effect from the new data retention regime coming into force, the Attorney General's public report will be expanded to include additional information regarding (a) the cost to service providers of complying with the data retention obligations, and (b) the use of data retention implementation plans.</p> <p>Another operator in Australia publishes information related to some of the statistical data it holds for its own operations. As we explained earlier, we do not believe that individual operator disclosures are an effective route to achieve the level of transparency sought by the public as a whole.</p>	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

Belgium

	Type of demand	
	Lawful interception	Communications data
Statistics	No technical implementation (1)	0
Key Note (1)	We have not implemented the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

Czech Republic

	Type of demand	
	Lawful interception	Communications data
Statistics	8,321	Government/other public body publishes (1)
Key Note (1)	The Czech Telecommunications Office publishes statistical information related to communications data demands issued by agencies and authorities.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

Democratic Republic of Congo

	Type of demand	
	Lawful interception	Communications data
Statistics	0 (1)	635
Key Note (1)	All operators have been required to allow the installation of a lawful interception capability in accordance with an order from the Agence Nationale de Renseignement (ANR), the Democratic Republic of Congo (DRC) Intelligence Service Agency dated 11 November 2014. This order was issued in accordance with the applicable law. When receiving any agency or authority demands for lawful interception assistance, our local operating company in the DRC provides this assistance on the condition that activities are conducted in accordance with the law.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annexe .		

Egypt

	Type of demand	
	Lawful interception	Communications data
Statistics	Vodafone disclosure unlawful (1)	Vodafone disclosure unlawful (1)
Key Note (1)	While the precise legal position regarding disclosure of aggregate statistical information remains unclear, local criminal laws contain a large number of provisions prohibiting the disclosure of national security-related material and other matters related to law enforcement. The disclosure of statistical information related to agency and authority demands is therefore very likely to be considered to be a violation of such provisions.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annexe .		

France

	Type of demand	
	Lawful interception	Communications data
Statistics	No technical implementation (1)	0
Key Note (1)	We have not implemented the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annexe .		

Germany

	Type of demand	
	Lawful interception	Communications data
Statistics	Government/other public body publishes (1, 2)	Government/other public body publishes (1, 2)
Key Note (1)	The German Federal Office of Justice publishes annual statistics related to agency and authority lawful interception demands. The German Federal Office of Justice publishes annual statistics related to agency and authority demands for access to communications data. In its annual report, the Federal Network Agency (Bundesnetzagentur or BNetzA) publishes statistics related to access by the Regulatory Authority to customer details stored in accordance with Article 112 of the German Telecommunications Act (TKG).	
Key Note (2)	<p>Prior to the publication of the 2014 report, it was unclear whether or not we could lawfully publish the statistical information we held for our own operations. Furthermore, prior to the 2014 report we were instructed by the Federal Network Agency (BNetzA) that publication of the information we held for our own operations in Germany was prohibited.</p> <p>Subsequent to our discussions with BNetzA, the Federal Ministry of Justice (BMJV) clarified that publication of statistical information by individual operators was lawful. Another operator in Germany subsequently began to release certain categories of information it held for its own operations. However, disclosures presented by this individual operator offer were, at most, only a partial view of law enforcement demands (for example, they excluded the effect of German agency and authority automated access systems which allow rapid and large-scale interrogation of a central database of customer records) and could not be reconciled with the authorities’ publication of the number of warrants issued each year.</p> <p>In addition, the statistical information published by this operator was based on the number of targeted subscribers rather than warrants received. It is impossible to reconcile those metrics with the methodology used in the government’s own disclosure regime, raising an even greater risk of miscounting than arises when an individual operator publishes statistical information derived from the number of warrants it has received.</p> <p>While Vodafone Germany’s demand volumes when measured on a targeted subscriber basis are broadly in line with those of the other operator, to report using this methodology would be to ignore the fundamental misalignment between the two statistical reporting approaches – warrants versus targeted subscribers – and makes it impossible to draw any reliable conclusions from the data available.</p> <p>Over the last three years, Vodafone Germany has discussed the issue of transparency and the different methodologies being used by operators with the German Ministry of the Interior. Despite much discussion, the participants did not necessarily all agree that changes should be made, would not agree on a common methodology and will continue to report on the same basis for the foreseeable future.</p> <p>As a result, Vodafone Germany remains aligned with the Vodafone Group position: that there is no value in publishing statistics from an individual operator, particularly when there are statistics published by the government available publicly.</p>	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annexe .		

Ghana

	Type of demand	
	Lawful interception	Communications data
Statistics	No technical implementation (1)	Unable to obtain guidance (2)
Key Note (1)	We have not implemented the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance.	
Key Note (2)	<p>The legal position remains unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands.</p> <p>Under the Electronic Communications Act, 2008 (ECA), certain classes of information which are deemed to be of importance to the protection of national security may be declared to be critical electronic records and subject to restrictions in respect of access, transfer and disclosure. Under section 56 of the ECA, the Minister for Communications may by notice in the <i>Gazette</i> (the official government publication) declare certain classes of information which are deemed to be of importance to the protection of national security to be critical electronic records. Section 59 of the ECA therefore provides for the setting of minimum standards in respect of access to, transfer and control of a critical database.</p> <p>Additionally, Section 60 of the ECA imposes restrictions on the disclosure of information in a critical database to persons other than the employees of the National Information Technology Agency, a law enforcement agency, a ministry, department or other government agency. As a result, if the aggregate data in respect of the above agency and authority demands is designated as ‘critical electronic records’, the government will be able to prevent Vodafone from publishing it.</p> <p>Prior to the publication of the 2014 report, we approached the authorities to ask for clarity and guidance as to whether Vodafone was lawfully permitted to disclose aggregate statistics related to communications data demands received from government agencies and authorities. We did not receive a response in time for publication of the 2014 report.</p> <p>During 2014-15, we attempted to engage with the authorities to seek guidance but were unable to obtain clarity on the legal position and therefore did not publish aggregate statistics.</p> <p>During 2015-16, we continued to engage with the government to seek to establish whether or not Vodafone is lawfully permitted to disclose aggregate statistics related to communications data demands. We are again unable to confirm that we have been granted approval to disclose such statistics and we therefore remain unable to publish this information.</p>	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annexe .		

Greece

	Type of demand	
	Lawful interception	Communications data
Statistics	Government/other public body publishes (1)	Government/other public body publishes (1)
Key Note (1)	The Hellenic Authority for Communication Security and Privacy (ADAE) publishes statistical information related to lawful interception and communications data demands issued by agencies and authorities.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annexe .		

Hungary

	Type of demand	
	Lawful interception	Communications data
Statistics	Vodafone disclosure unlawful (1)	68,751 (2)
Key Note (1)	It is unlawful to disclose any aspect of how lawful interception is conducted.	
Key Note (2)	Under s.62 of the National Security Service Act, if the intelligence services demand information from communications service providers, the service provider is not allowed to disclose any information (including aggregate data or statistics) in relation to such cooperation without the prior explicit permission of the competent minister or director general of the particular intelligence agency. The statistics disclosed here therefore do not include demands for access to communications data related to matters of national security.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annexe .		

India

	Type of demand	
	Lawful interception	Communications data
Statistics	Vodafone disclosure unlawful (1)	Vodafone disclosure unlawful (1)
Key Note (1)	<p>Section 5 (2) of the Indian Telegraph Act 1885 – read with Rule 419 (A) of Indian Telegraph (Amendment) Rules 2007 obliges telecommunications service providers to ‘maintain extreme secrecy’ in matters concerning lawful interception.</p> <p>Further, under Rule 25(4) of the IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (Interception Rules) and Rule 11 of the IT (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 (the Traffic Data Rules), ‘strict confidentiality shall be maintained’ in respect of directions for lawful interception, monitoring, decryption or collection of data traffic. These prohibitions extend to the very existence of such directions, and could therefore authorise the government to prevent the publication of aggregate data relating to the number of directions received by the licensee.</p> <p>In addition, in respect of lawful interception directions made under the Information Technology Act, 2000 (IT Act) and its associated Rules, the government can prevent the publication of aggregate data in relation to lawful interception and other data disclosure demands from the government and law enforcement agencies. Finally, under Clause 40.5 of the Unified Access Service Licence (UASL: the licence governing access service in India), and Clause 33.5 of the Internet Service Provider (ISP) Licence (the licence governing internet access service in India), the licensee is bound to maintain the secrecy and confidentiality of any confidential information disclosed to the licensee for the proper implementation of the licences. Aggregate data regarding agency and authority demands comes under the purview of these provisions.</p>	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annexe .		

Ireland

	Type of demand	
	Lawful interception	Communications data
Statistics	Cannot disclose (1)	4,393
Key Note (1)	<p>Prior to publication of the 2014 report, we approached the authorities to seek clarity on the disclosure of aggregate statistics related to lawful interception demands. In response, the authorities instructed us not to disclose this information.</p> <p>During 2014-15 – and again in 2015-16 – we engaged with the Irish government to discuss whether or not such information could be published by the authorities themselves or – if not – by Vodafone and other operators. The government has again informed us that we cannot disclose this information.</p>	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

Italy

	Type of demand	
	Lawful interception	Communications data
Statistics	Government/other public body publishes (1)	451, 320 (2)
Key Note (1)	The Italian Ministry of Justice publishes statistical information related to the number of lawful interception demands issued by agencies and authorities.	
Key Note (2)	This statistic covers all warranted access to communications data as defined by the Ministry of Justice. It no longer includes customer registration records, as in previous reports, as these records form part of routine customer verification and do not relate directly to warranted agency or authority activity.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

Kenya

	Type of demand	
	Lawful interception	Communications data
Statistics	Cannot disclose (1)	Unable to obtain guidance (2)
Key Note (1)	All telecommunications operators can be required to allow the installation of a lawful interception capability in accordance with the Security Laws (Amendment) Act (2014), article 69, which is an amendment of the Prevention of Terrorism Act. We approached the authorities to seek clarity on whether or not we could disclose if (and when) we had received an agency or authority demand for lawful interception assistance; however, we did not receive a response in time for publication of this statement.	
Key Note (2)	<p>The legal position remains unclear regarding whether or not it would be lawful for Safaricom (Vodafone’s local associate operator) or Vodafone to disclose statistics related to agency and authority communications data demands.</p> <p>Section 3 of the Official Secrets Act provides certain instances where publication or disclosure of information is deemed an offence. The broad language of this Act includes publication of data collected by the security agency in Kenya.</p> <p>In addition, Section 37 of the National Intelligence Service Act (Act No. 28 of 2012) (NIS Act) limits a person’s constitutional right of access to information where such information is classified. When read with the Official Secrets Act (Chapter 187, Laws of Kenya), the government can prevent the publication of such data if such publication will be prejudicial to safety and the interest of the Republic of Kenya. The NIS Act defines ‘classified information’ as information of a particular security classification, whose unauthorised disclosure would prejudice national security. While the NIS Act does not define what would be deemed to prejudice national security, the 2010 Constitution of Kenya provides how national security shall be promoted and guaranteed. A National Security Council exists to exercise supervisory control over national security matters in Kenya and to determine what may prejudice national security.</p> <p>It is therefore under these umbrella powers regarding prejudice to national security that the government can prevent the publication of various agency and authority demands. It may follow that where there is no prejudice to national security these restrictions do not apply. However there is no legal definition of what would amount to a prejudice to national security.</p> <p>We have therefore concluded again that it is still not possible to engage with government, agencies and authorities on these matters at this point. We will update this section of the report in future if circumstances change.</p>	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex.		

Lesotho

	Type of demand	
	Lawful interception	Communications data
Statistics	No technical implementation (1)	1,586
Key Note (1)	We have not implemented the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

Malta

	Type of demand	
	Lawful interception	Communications data
Statistics	Vodafone disclosure unlawful (1)	3,693 (2)
Key Note (1)	It is unlawful to disclose any aspect of how lawful interception is conducted.	
Key Note (2)	Prior to the 2014 report, the legal position was unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands. We asked the authorities for guidance and were informed that we could disclose this information in the 2014 report. There has been no change to the guidance since that report: we have therefore updated this statistic with the latest information we hold for our own local operating business.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

Mozambique

	Type of demand	
	Lawful interception	Communications data
Statistics	No technical implementation (1)	Unable to obtain guidance (2)
Key Note (1)	We have not implemented the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance.	
Key Note (2)	The legal position remains unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands. We have again attempted to engage with the government regarding whether or not it would be lawful for Vodafone to disclose this information but have been unable to obtain any further clarity from the Ministry of Interior on the ability of Vodafone to disclose statistics related to agency and authority communications data demands.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

Netherlands

	Type of demand	
	Lawful interception	Communications data
Statistics	Vodafone disclosure unlawful (1) Government/other public body publishes (2) Further action to follow (3)	Government/other public body publishes (2) Further action to follow (3)
Key Note (1)	Article 85 of the Intelligence and Security Services Act 2002 (<i>Wet op de inlichtingen en veiligheidsdiensten 2002</i> or ISSA) requires all persons involved in the execution of the ISSA to keep the data obtained confidential. It would be unlawful for Vodafone to disclose statistical information related to lawful interception demands issued by agencies and authorities under the ISSA.	
Key Note (2)	The Dutch Ministry of Justice publishes statistical information related to lawful interception and communications data demands issued by agencies and authorities.	
Key Note (3)	<p>During 2015-16, and following our outreach in the previous year, we engaged with the Ministries of Security and Justice, Internal Affairs and Economic Affairs to urge the government to take action on computer criminality, law enforcement and data retention in their new proposals including:</p> <ul style="list-style-type: none">• better oversight on law enforcement;• more transparency about lawful interception statistics; and• only using the means necessary to collect data. <p>We did this individually and through our work with coalitions of telecoms companies and other parties and organisations who wish to see greater oversight and transparency in this area.</p> <p>We strongly recommended to the government that it adopt the ten standards for oversight and transparency in national intelligence services proposed by the University of Amsterdam. We also suggested that these standards could contribute to the efforts of other authorities.</p> <p>We have told the government that, in our view, it should take responsibility for the publication of aggregated statistical information related to agency and authority demands. We believe that the government has become more receptive to the rationale for improving transparency and oversight, as demonstrated in their approach to the legal procedures on interception statistics, the three draft bills (computer criminality, law enforcement and data retention) and the public debate around balancing security and privacy. We continue to engage with the government in an effort to improve the quality of transparency via the creation of a more coherent and robust disclosure framework.</p>	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

New Zealand

	Type of demand	
	Lawful interception	Communications data
Statistics	Government/other public body publishes/further action to follow (1)	Government/other public body publishes/further action to follow (1)
Key Note (1)	<p>Statistical information related to lawful interception and communications data demands issued by agencies and authorities is published by the following four organisations:</p> <p>The New Zealand Police</p> <p>The New Zealand Security Intelligence Service</p> <p>The New Zealand Serious Fraud Office</p> <p>The New Zealand Customs Service</p> <p>The statistical information published by the government is currently divided across a number of reports that are issued by different agencies with differing methodologies. This approach limits the quality of the overall disclosures and the extent of transparency.</p> <p>During 2015-16, we were asked to participate in a pilot project which the Office of the Privacy Commissioner conducted from July to September 2016. The pilot involved asking companies to record a standard set of information about demands for assistance from law enforcement agencies. The information from operators would then be gathered by the Privacy Commissioner – who is independent of government – and published.</p> <p>While we strongly welcome the Privacy Commissioner’s focus on this area, we consider that aggregate reporting of demands received by operators purely on the basis of the operators’ own records is not a desirable approach to disclosure. It is only the <i>source</i> of those demands for access – the government, via the agencies acting on its behalf – that can provide a clear and unambiguous view of the statistical data involved. We therefore declined the opportunity to take part in the pilot but look forward to further engagement with the Commissioner – and with the government – to try to develop the appropriate disclosure framework.</p>	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

Portugal

	Type of demand	
	Lawful interception	Communications data
Statistics	Government/other public body publishes (1)	38,142 (2)
Key Note (1)	The Portuguese government publishes statistical information related to lawful interception demands issued by agencies and authorities.	
Key Note (2)	Prior to the 2014 report, the legal position was unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands. We asked the authorities for guidance and were informed that we could disclose this information in the 2014 report. There was no change to that guidance in 2015 so we updated the statistic again. In 2016, with a new government in place, we requested guidance once more and were informed that we could disclose this information: we have therefore updated this statistic with the latest information we hold for our own local operating business.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

Qatar

	Type of demand	
	Lawful interception	Communications data
Statistics	Vodafone disclosure unlawful (1)	Cannot disclose (2)
Key Note (1)	It is unlawful to disclose any aspect of how lawful interception is conducted.	
Key Note (2)	<p>Prior to the 2014 report, the legal position was unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands.</p> <p>Article 59 of the Qatar Telecommunication Law states that telecommunications service providers must comply with the requirements of the security authorities which relate to the dictates of maintaining national security and the directions of the governmental bodies in general emergency cases and must implement orders and instructions issued by the General Secretariat regarding the development of network or service functionality to meet such requirements. Any government department interested in ‘state security’ can rely on Article 59 alongside use any enforcement powers vested directly in that government authority.</p> <p>We asked the authorities for guidance and were informed that we could not disclose this information in the 2014 report. There has been no change to the guidance since that report: we therefore cannot publish this information.</p>	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annexe .		

Romania

	Type of demand	
	Lawful interception	Communications data
Statistics	Vodafone disclosure unlawful (1)	Vodafone disclosure unlawful (2)
Key Note (1)	It is unlawful to disclose any aspect of how lawful interception is conducted.	
Key Note (2)	Article 142(3) and Article 152(3) of the Criminal Procedure Code (Law 135/2010) state that communications service providers are required to cooperate with criminal prosecution authorities with regards to lawful interception, and the supplier of retained communications data must keep the relevant operation a secret. Publishing aggregate statistics could potentially violate this obligation.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annexe .		

South Africa

	Type of demand	
	Lawful interception	Communications data
Statistics	Vodafone disclosure unlawful (1)	Vodafone disclosure unlawful (1)
Key Note (1)	Section 42 of the Regulation on Interception of Communication and Provision of Communication-related Information Act 2002 prohibits the disclosure of any information received pursuant to the Act. This includes, by virtue of Section 42(3), the disclosure of the fact that any demand for lawful interception or communications data has been issued under the Act. Accordingly, to publish aggregate statistics would be to disclose the existence of one or more lawful interception or communications data demands.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annexe .		

Spain

	Type of demand	
	Lawful interception	Communications data
Statistics	15,465 (1)	46,042 (1)
Key Note (1)	Prior to the 2014 report, the legal position was unclear regarding whether or not it would be lawful for Vodafone to disclose statistics related to agency and authority lawful interception and communications data demands. We asked the authorities for guidance and were informed that we could disclose this information in the 2014 report. There has been no change to the guidance since that report: we have therefore updated these statistics with the latest information we hold for our own local operating business.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

Tanzania

	Type of demand	
	Lawful interception	Communications data
Statistics	No technical implementation (1)	2,137
Key Note (1)	We have not implemented the technical requirements necessary to enable lawful interception and therefore have not received any agency or authority demands for lawful interception assistance.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

Turkey

	Type of demand	
	Lawful interception	Communications data
Statistics	Vodafone disclosure unlawful (1)	Vodafone disclosure unlawful (1)
Key Note (1)	It is unlawful to disclose any aspect of how lawful interception or access to communications data is conducted.	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex .		

United Kingdom

	Type of demand	
	Lawful interception	Communications data
Statistics	Vodafone disclosure unlawful (1) Government/other public body publishes (2)	Government/other public body publishes (2)
Key Note (1)	Section 19 of the Regulation of Investigatory Powers Act 2000 prohibits disclosing the existence of any lawful interception warrant and the existence of any requirement to provide assistance in relation to a warrant. This duty of secrecy extends to all matters relating to warranted lawful interception. Data relating to lawful interception warrants cannot be published. Accordingly, to publish aggregate statistics would be to disclose the existence of one or more lawful interception warrants.	
Key Note (2)	<p>The Interception of Communications Commissioner's Office publishes statistical information related to lawful interception and communications data demands issued by agencies and authorities.</p> <p>The Investigatory Powers Act 2016 received royal assent on 29 November 2016. The UK Parliamentary website describes the purpose of the Act to “make provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal datasets and other information; to make provision about the treatment of material held as a result of such interception, equipment interference or acquisition or retention; to establish the Investigatory Powers Commissioner and other Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes”.</p> <p>Throughout our engagement with the UK government and others, we have recognised the importance of lawfully authorised communications surveillance within a clear legal framework to support law enforcement and intelligence agencies in tackling serious crime, terrorism and threats to national security. Equally, we have also emphasised the need to protect UK citizens’ legal right to privacy: our customers’ trust is the bedrock of our business and respect for their privacy is paramount.</p> <p>We received a number of assurances from the UK government as the Bill moved through Parliament, including an amendment (brought forward by the government itself) to the effect that retention of third-party data by communications service providers would not be required.</p>	
For a summary of the most important legal powers relating to law enforcement demands, network censorship and encryption, on a country-by-country basis, see our Legal Annex.		