# Country by Country Disclosure of Law Enforcement Assistance Demands 2018-19

Vodafone Group Plc

# 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 a local licence (or other authorisation) issued by the government of the country in which the subsidiary is located. Each of these subsidiary companies is therefore 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 regimes governing law enforcement assistance. We also disclose the volume of each country's agency and authority demands, wherever that information is available and publication is not prohibited. The data recorded in this Statement covers the period 1 April 2018 to 31 March 2019.

A summary of some of the most relevant legal powers in each of our countries of operation can be found in our separate Legal Annexe. The Annexe, which was last updated in spring 2016, sets out the laws and practices, on a country by country basis, that limit or prohibit disclosure and also includes a section covering the laws that relate to encryption and law enforcement assistance. The information contained within the Annexe, produced with the support of the law firm Hogan Lovells, remains an important part of our disclosures in this area as it helps to ensure greater public clarity on what is legally possible in each of the markets in which we operate.

There remains no established reporting model to follow when compiling the information contained within this report, nor a standardised method for categorising the type and volume of agency and authority demands. In addition, different governments, parliaments, regulators, agencies and authorities apply a variety of definitions when authorising or recording the types of demands made, as do operators themselves when receiving and recording those demands.

# How we prepared this report

Each local market in which Vodafone operates has a nominated and security-cleared point of contact responsible for the management and administration of law enforcement assistance. The information collated and published in this report (wherever available and wherever publication has not been prohibited) has been overseen by the relevant Disclosure Officer, although they will not typically be made aware of the context of any lawful demand issued by agencies and authorities.

For the two categories of agency and authority demand detailed in this report – lawful interception and communications data (see our explanation of these terms) – we have robust processes in place to manage and track each demand.

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

It should be noted that while the statistics for communications data demands are overwhelmingly related to communications metadata, the statistics we report might also include demands for other types of customer data such as names, physical addresses 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.

In some countries, there is a lack of legal clarity regarding whether we can lawfully disclose the aggregate number of law enforcement demands received. In countries experiencing continuing periods of significant political tension, it remains very challenging to ask questions related to national security and criminal investigation matters; as such, Vodafone has to strike a balance between asking legitimate questions and mitigating the potential risk this poses to Vodafone employees.

## Explanation of the information presented

In each country, and for each of the categories of law enforcement demands issued – lawful interception and communications data – there are a number of different possible outcomes that can arise from our decision to publish the information collated.

Where there are no restrictions preventing publication and there are no alternative appropriate sources of information indicating total demand volumes across all operators in a specific country, we have published the data available from our own local operating business. Our view of the shortcomings of this approach is set out in the accompanying Statement.

It remains our view that in countries where the government publishes certain statistical information on the law enforcement demands they issue and individual operators also publish some of the data they hold for their own operations, the net effect is confusion. In statistical terms, the datasets are irreconcilable and contradictory. We continue to advocate that it would be much more effective if governments provided consistent and comprehensive metrics spanning the industry as a whole, as this would provide the public with a better understanding of the law enforcement activity being undertaken in their country.

It is 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, record keeping and reporting regimes, as there are no consistent points of common reference that could be used to underpin such analysis. Similarly, it is difficult in many cases 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 or accepted industry practices; or changes to the approaches used to log, aggregate and disclose lawful demands. Any of these may apply and therefore year-on-year changes cannot provide a reliable indication of actual trends in law enforcement activity.

Our global internal review, which analyses the extent to which we can lawfully publish aggregate volumes of law enforcement assistance demands at a local level on a country by country basis, remains relevant with the exception of Italy, where we are now able to publish aggregate statistics related to these types of demands.

There are six 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. This is particularly the case in matters related to national security. Wherever this is the case, we cite the relevant law that restricts disclosure, either in the main text or in the Legal Annexe.

## 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 use them have not been mandated.

## 3. Capability not enabled

Despite the technical requirements necessary to enable lawful interception being in place, some countries have not yet enabled those capabilities.

## 4. 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. This could be during a period of political tension or where disclosure could expose our employees to consequent risk.

## 5. Cannot disclose

In some cases, although local laws do not expressly prohibit disclosure, the authorities have told us directly that we cannot disclose this information. In other cases, we are unable to supply the required data due to local and/or technical restrictions.

## 6. 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 demands issued to all operators in that country. Wherever this is the case, we provide a link to the information available online.

## Albania

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Statistics** | Disclosure unlawful | 5,133 |
| **Key Note (1)** | It is unlawful to disclose any aspect of how lawful interception 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 Annexe. | | |

## Australia

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Statistics** | Government/other public body publishes (1) | Government/other public body publishes (1) |
| **Key Note (1)** | The Minister for Home Affairs publishes an annual report containing statistics regarding the use of lawful interception and communications data access powers in Australia, including:<br>• statistics related to interception and stored communications warrants obtained by law enforcement agencies;<br>• statistics related to communications data disclosure requests by agencies and authorities;<br>• the number of prosecutions and convictions resulting from the use of intercepted or accessed telecommunications information; and<br>• the cost to service providers of complying with the data-retention obligations.<br>The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth) introduced in 2018 addresses law enforcement and intelligence agencies' challenges with the evolution of the communications environment, including the growth of encrypted communication, by amending existing legislation. The changes are outlined in more detail in Key Note 2. | |
| **Key Note (2)** | **Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)**<br>*The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)* (Assistance and Access Act), introduced in 2018, introduced key reforms to address law enforcement and intelligence agencies' challenges with the evolution of the communications environment, including the growth of encrypted communication. The Assistance and Access Act provides an official framework for agencies to seek assistance from carriers and is set out in five schedules.<br>Schedule 1 allows Australian agencies to request voluntary assistance from carriers by way of a Technical Assistance Request (TAR) or a Technical Assistance Notice (TAN), which relates to an existing capability. It also allows the Attorney-General and the Minister of Communications to issue a Technical Capability Notice (TCN), requiring a carrier to build a new product/service for agencies. Any assistance or capability requested under Schedule 1 must be reasonable, proportionate, practicable and technically feasible, must relate to an offence with a maximum penalty of at least three years' imprisonment and must be targeted access that does not jeopardise the security of general users.<br>Schedule 2 allows law enforcement agencies to covertly access devices to investigate serious crimes, including mobile phones via a computer access warrant, and to conceal the fact that the device has been accessed.<br>Schedules 3 and 4 extend the maximum penalties considered in the requirement to unlock a device under the *Crimes Act 1914 (Cth)* and the *Customs Act 1901 (Cth)* and extend the time available for examining electronic devices seized under warrant under each of these acts. Schedule 3 also allows access by the police to account-based data, including social media accounts, via a search warrant.<br>Schedule 5 provides protections to persons/bodies that voluntarily assist Australian Security Intelligence Organisation (ASIO) or who make unsolicited disclosures to ASIO. | |
| 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. | | |

## 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 Annexe. | | |

## Czech Republic

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Statistics** | 7,716 | 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 Annexe. | | |

## Democratic Republic of Congo

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Statistics** | Cannot disclose (1) | 1,288 |
| **Key Note (1)** | All operators were 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 Agency, dated 11 November 2014. This order was issued in accordance with the applicable law.<br>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 the requirement and any associated 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 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) | 1 |
| **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 (Bundesamt fur Justiz) publishes annual statistics related to agency and authority lawful interception demands, as well as annual statistics related to agency and authority demands for access to communications data.<br>In its annual report, the Federal Network Agency (Bundesnetzagentur or BNetzA) publishes statistics (in German and English) 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)** | In the past, Vodafone Germany has discussed the issue of transparency and the different methodologies being used by operators and governmental bodies with the German Ministry of the Interior. Despite much discussion, the participants did not necessarily all agree that changes should be made, nor did they agree to a common reporting methodology, and they have stated they will continue to report on the same basis for the foreseeable future.<br>As a result, Vodafone Germany remains aligned with the Vodafone Group's position: that there is no value in publishing statistics from an individual operator, particularly when there are statistics published by the government available publicly. | |
| 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** | Vodafone disclosure unlawful (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.<br>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 to access, transfer and disclosure. Under Section 56 of the ECA, the Minister of Communications may, by notice in the Gazette (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 to the access, transfer and control of a critical database.<br>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, ministry, department or other government agency. As a result, if the aggregate data with respect to the above agency and authority demands is designated as 'critical electronic records', the government will be able to prevent Vodafone from publishing it.<br>Despite continued representation, it is not possible to establish whether or not Vodafone is lawfully permitted to disclose aggregate statistics related to communications data demands. As we have not been granted approval, we remain unable to publish this information. | |
| 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) | 125,688 (2) |
| **Key Note (1)** | It is unlawful to disclose any aspect of how lawful interception is conducted. | |
| **Key Note (2)** | Under Section 62 of the National Security Service Act, if the intelligence services demand information from a communications service provider, 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.<br>The statistic disclosed here, therefore, does 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** |
| **Key Note (1)** | On 31 August 2018, Vodafone India merged with Idea Cellular to form a new entity named Vodafone Idea Limited. Therefore, we will no longer be including India in future reporting. | |

## Ireland

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Statistics** | Cannot disclose (1) | 3,118 |
| **Key Note (1)** | 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.<br>We have regularly engaged with the 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 not changed its position since that time and has informed us that we cannot disclose this information. | |
| 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. | | |

## Italy

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Statistics** | 37,633 (1) | 111,152 |
| **Key Note (1)** | The Italian Ministry of Justice no longer publishes statistical information related to the number of lawful interception demands issued by agencies and authorities. Vodafone will now therefore publish such data. | |
| 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. | | |

## 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.<br>It remains unclear whether we can provide any detail regarding lawful interception capability. | |
| **Key Note (2)** | 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.<br>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 it 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 outlines 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.<br>It is 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. | |
| 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. | | |

## Lesotho

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Statistics** | No technical implementation (1) | 1,195 |
| **Key Note (1)** | We have not implemented the technical requirements necessary to enable lawful interception as there is no law requiring us to do so, and therefore we 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. | | |

## Malta

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Key Note (1)** | On 1 April 2020, Vodafone Group Plc announced it had completed the sale of 100% of Vodafone Malta to Monaco Telecom SAM. We therefore will no longer be including Malta in our disclosure reporting. | |
| 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. | | |

## Mozambique

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Statistics** | Capability not enabled (1) | Unable to obtain guidance (2) |
| **Key Note (1)** | The technical requirements necessary to enable lawful interception within Vodacom Mozambique's control are now in place but those capabilities have not yet been enabled. | |
| **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.<br>We have attempted to engage 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 Annexe. | | |

## Netherlands

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Statistics** | Vodafone disclosure unlawful (1)<br>Government/other public body publishes (2) | Government/other public body publishes (2) |
| **Key Note (1)** | Article 85 of the Intelligence and Security Services Act 2002 (Wet op de inlichtingen- en veiligheidsdiensten 2002; 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 and Security 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. | | |

## New Zealand

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Statistics** | Government/other public body publishes (1) | Government/other public body publishes (1) |
| **Key Note (1)** | Statistical information related to lawful interception and communications data demands issued by agencies and authorities is published by the following organisations:<br>• The New Zealand Police<br>• The New Zealand Security Intelligence Service<br>• The New Zealand Serious Fraud Office<br>• The New Zealand Customs Service<br>• The New Zealand Government Communications Security Bureau<br>• The New Zealand Inland Revenue Department<br>• The New Zealand Ministry of Social Development<br>• The New Zealand Ministry of Business, Innovation & Employment<br>• The New Zealand Department of Internal Affairs<br>• The New Zealand Ministry for Primary Industries<br>• The New Zealand Financial Markets Authority<br>• The New Zealand Commerce Commission<br>• Coronial Services of New Zealand<br>The statistical information published by the government is currently divided across a number of reports issued by different agencies with differing methodologies. This approach limits the quality of the overall disclosures and the extent of transparency. | |
| 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. | | |

## Portugal

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Statistics** | Government/other public body publishes (1) | 40,220 (2) |
| **Key Note (1)** | The Portuguese government publishes statistical information related to lawful interception demands issued by agencies and authorities. | |
| **Key Note (2)** | In 2016, with a new government in place, we requested guidance regarding whether it would be lawful for Vodafone to disclose statistics related to agency and authority communications data demands. We were informed that we could disclose this information, and continue to include 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 Annexe. | | |

## Qatar

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Key Note (1)** | On 29 March 2018, Vodafone Group Plc announced that Qatar Foundation has completed its acquisition of Vodafone Europe B.V.'s 51% stake in the joint venture company – previously owned by Vodafone and Qatar Foundation LLC – that controls Vodafone Qatar Q.P.S.C. ('Vodafone Qatar'). We will, therefore, no longer be reporting on Vodafone Qatar as part of our disclosure reporting. | |

## 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.<br>Following discussions with the relevant authorities during 2016-17, it has become clear that we will not receive written confirmation that publication of aggregate statistics is permitted. Given this and the extent of the potential risk to our employees associated with publication, we are not in a position to disclose aggregate statistics related to communication 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. | | |

## South Africa

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Statistics** | Vodafone disclosure unlawful (1) (2) | Vodafone disclosure unlawful (1) (2) |
| **Key Note (1)** | The Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA Act) regulates, among other things, the provision and disclosure of information. In particular, Section 42 of the RICA Act prohibits the disclosure of any information which was obtained in exercising powers and performing duties under the Act (e.g. the disclosure of information contained in the RICA database). Furthermore, employees of telecommunications service providers are prohibited from disclosing any information obtained in the course of employment and which is connected to exercising any powers or performance of any duties under the terms of the RICA Act. The RICA Act does, however, make provision for the disclosure of information in certain circumstances:<br>(i) to any person who requires it for the performance of his or her duties under the Act;<br>(ii) if he or she is the person who supplies it in the performance of his or her functions under the terms of the Act;<br>(iii) information required under the terms of any law or as evidence in a court of law; or<br>(iv) to any competent authority (including law enforcement agencies) which requires it for the institution of an investigation with a view to prosecuting a crime. | |
| **Key Note (2)** | In 2017 and 2018, Right2Know (a non-profit advocacy organisation that campaigns for the free flow of information in South Africa) made requests for access to information in accordance with the Promotion of Access to Information Act No. 2 of 2000 (PAIA), requesting that all telecommunication operators provide information on the total number of disclosures made to law enforcement agencies in each financial or calendar year for 2015, 2016, 2017 and 2018.<br>Any request for access to information in accordance with PAIA is carefully considered on a case-by-case basis, taking into account all applicable competing and/or complementary legislation. Given the competing legislative requirements between the disclosure restrictions of the RICA Act and the requirement to disclose via PAIA, we sought expert opinion and decided to supply the statistical information as requested by Right2Know in compliance with PAIA. The statistical information provided can be viewed via the following links.<br>Link 1 – 2017<br>Link 2 – 2018<br>Link 3 – 2018 | |
| 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** | 13,519 | 58,165 |
| 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. | | |

## Tanzania

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Statistics** | Vodafone disclosure unlawful | 8,698 |
| 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. | | |

## 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 Annexe. | | |

## United Kingdom

| | Type of demand | |
|---|---|---|
| | **Lawful interception** | **Communications data** |
| **Statistics** | Government/other public body publishes (2) | There were substantial changes to the legal framework during this reporting period (1)<br>Government/other public body publishes (2) |
| **Key Note (1)** | The Communications Data Code of Practice took effect from 1 November 2018.<br>Restrictions on the powers of public authorities to acquire communications data from telecommunications operators, and additional safeguards relating to oversight, were introduced in February 2019 through the Data Retention and Acquisition Regulations 2018. These amendments included the introduction of independent authorisation of requests by public authorities to access communications data, conferring on the Investigatory Powers Commissioner a new power to authorise communications data requests. The Commissioner carries out this function through the Office for Communications Data Authorisations.<br>Amendments were also made in respect of the powers available to the Secretary of State to compel a telecommunications operator to retain communications data. The amendments restrict the purposes for which the Secretary of State may give a notice to a telecommunications operator requiring the retention of communications data. A notice may be given where it is necessary and proportionate to retain data in the interests of national security or of the economic wellbeing of the UK so far as is relevant to national security, in the interests of public safety, for the purpose of preventing death or injury or to assist investigations into alleged miscarriages of justice. A notice may be given for the purpose of the prevention or detection of serious crime so far as it relates to events data, or for the purpose of the prevention or detection of crime or of preventing disorder so far as it relates to entity data.<br>The amendments were made in response to the judgment of the Court of Justice of the European Union (CJEU), in joined cases C-203/15 and C-698/15, setting out safeguards required in order that a communications data retention regime is compliant with EU law. | |
| **Key Note (2)** | In September 2017, the Interception of Communications Commissioner's Office was formally replaced by the Investigatory Powers Commissioner's Office (IPCO). The IPCO publishes statistical information related to lawful interception and communications data demands issued by agencies and authorities.<br>The Investigatory Powers Act 2016 received royal assent on 29 November 2016. The UK Parliamentary website describes the purpose of the Act as 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'. | |

**© 2020 Vodafone Group Plc**
Registered Office:
Vodafone House
The Connection
Newbury
Berkshire
RG14 2FN

Registered in England No. 1833679