26 September 2018

Vodafone Group Plc – Response to Access Now letter on Ranking Digital Rights 2018 Corporate Accountability Index

Ensuring our customers' right to privacy is respected is one of Vodafone's highest priorities. It is also a part of Vodafone's Code of Conduct which everyone who works for Vodafone has to follow at all times.

We welcome the contribution that the Ranking Digital Rights project has made to the debate on respecting privacy and freedom of expression in the sector. We participated actively in the project and were pleased to be ranked first among the telecommunications operators included in the 2018 Corporate Accountability Index, increasing our score by 3.47% from the ranking completed in 2017. Vodafone was also the only company in the 2018 Index to provide comprehensive information about how it handles data breaches.

Vodafone has strengthened its commitment to protecting its customers' human rights by becoming a board member of the Global Network Initiative (GNI) in March 2017 and publicly committing to implementing the GNI Principles on freedom of expression and privacy. The GNI is an international, multi-stakeholder group of companies, civil society organisations, investors and academics who have created a collaborative approach to protect and advance freedom of expression and privacy in the ICT sector and we work hard within that forum to help advance those protections globally.

Government Requests

In 2014, Vodafone became one of the first telecommunications companies to produce a comprehensive Law Enforcement Disclosure report. The report provided a detailed insight into the legal frameworks, governance principles and operating procedures associated with demands for assistance from law enforcement and intelligence agencies across 28 countries.

Within the report, we set out our views and approach to the disclosure of aggregate statistics relating to requests from law enforcement agencies and authorities. We believe that it is governments - not communications operators - who hold the primary duty to provide greater transparency on the number of agency and authority demands issued to operators and therefore within the report we provided links to all aggregate statistics published by governments in place of our own locally held information. Where the authorities did not publish aggregate statistical information but where we believe we can lawfully publish in our own right, we disclosed this information. However, legislation often includes stringent restrictions preventing operators from disclosing any information relating to agency and authority demands received, including disclosure of aggregate statistics. Where these restrictions existed, we did not publish. More details on our views, as well as our country-by-country disclosures, can be found within the Report.

Since then, we have published two more iterations of that report. In 2015, we updated all the material published in 2014, added a new section which focused on network censorship content blocking and the restriction of services which may impact our customers' ability to express

themselves freely, and updated the legal annexe which summarises the most important legal powers in force in our 28 countries of operation.

In 2017, we again updated our disclosures in this area. Much of the Report remains consistent with previous disclosures, including our core principles and practices, which remain unchanged. We updated our statistical information for those countries in which we received a lawful demand for assistance from a law enforcement agency or government authority. We also developed disclosures around customer privacy and the digital rights of the child, which we published for the first time in 2017.

Government agencies and authorities have legal powers that enable them to access customer communications. To provide further transparency on the topic of government's ability to demand such access, we published a Legal Annex: Overview of Legal Powers, which provides an analysis of the local laws that empower government agencies and authorities to demand that access, or to block or restrict access to communications. In 2017, we updated the Legal Annex to cover the laws that relate to encryption and law enforcement assistance, in the countries in which we operate. While the legal powers summarised in this annex form part of local legislation in each of these countries and can therefore be accessed by the public, in practice very few people are aware of these powers or understand the extent to which they enable agencies and authorities to compel operators to provide assistance of this nature.

Privacy and Handling User Data

In relation to how Vodafone respects our customers' privacy, our privacy policies are supported by our Privacy Commitments (which can be found in our Customer Privacy disclosure mentioned above), which set out the principles that govern our approach to privacy and how we seek to build customer trust through transparency, empowerment and reassurance. Our commitment to our customers' privacy goes beyond legal compliance, we are focused on building a culture that respects privacy in order to justify the trust that people place in us:

- **Accountability**: We are accountable for living up to these commitments throughout Vodafone, including when working with our partners and suppliers. We maintain privacy policies and compliance processes that we use to ensure we live up to these principles.
- **Fairness and lawfulness**: We comply with privacy laws and act with integrity and fairness. We work with governments, regulators, policy makers and opinion formers to help shape better and more meaningful privacy laws and standards.
- **Privacy-by-design**: Respect for privacy is a key component in the design, development and delivery of our products and services.
- **Openness and honesty**: If our actions could affect our customers' privacy, we communicate this clearly. We ensure our actions reflect our words, and we are open to feedback about our actions.
- **Choice and access**: We give people the ability to make simple and meaningful choices about their privacy and allow them – where appropriate – to access, update or delete their personal data.
- **Responsible data management and limited disclosures**: We apply appropriate data management practices to govern the processing of personal data. We limit disclosures of

personal data to our partners to what is described in our privacy notices or to what has been authorised by our customers.

- **Balance**: When we are required to balance the right to privacy against other obligations necessary to a free and secure society, we work to minimise privacy impacts.
- **Security safeguards**: We implement appropriate technical and organisational measures to protect personal data against unauthorised access, use, modification or loss.

As part of our programme to ensure compliance with the new EU General Data Protection Regulation, Vodafone launched new Privacy Portals for our customers which provide detailed information about the way a particular Vodafone market processes customer personal data. The portals bring together not only our generic privacy policy which applies to all our products and services, but also product specific privacy supplements which further explain what personal data is collected, how is processed for that particular product or service and what choices are available to manage the way the personal data is processed. We also published animations which explain the key information in an easily approachable format. The privacy portal includes all the information required by law and more. We believe this is an industry leading approach. We also used this as an opportunity to harmonise how we communicate about privacy between our various markets. The portal also helps customers to exercise their privacy rights, for example to request access to their personal data. The policy has an effective date to track changes.

While the format of presenting the policy changed and more detail was added, Vodafone did not introduce new processing purposes which would have been incompatible with the purposes we have earlier communicated. Therefore, a customer consent for the new policy was not required nor sought. Instead, the updated policy was communicated directly to our existing users through various communications channels, in addition to posting it on our websites. New customers are given the same information as part of the agreement for new products and services. Vodafone trained its retail and call-centre staff to understand our privacy policy and to be able to answer customers' privacy related questions.

Vodafone never shares personal data to independent third parties without consent. However, Vodafone has hundreds of suppliers who process our personal data on our behalf. It is not practical, nor required or even relevant, to provide a list of all such data processors. Such processors are only allowed to process personal data under strict instructions by Vodafone. All suppliers go through a rigorous supplier review process where Vodafone verifies their ability to meet our requirements, and a binding data protection agreement dictates what they are allowed to do with personal data controlled by Vodafone.

Vodafone has adopted a rigorous, comprehensive, end to end Privacy by Design and Default approach. For us, these concepts extend far beyond mere user settings. Vodafone has strict internal policy and standards, supported by operational processes to make the policy and standards effective and rigorous monitoring for compliance. All Vodafone products and service go through rigorous Security and Privacy Impact Assessments during which privacy risks are identified and mitigating controls are introduced to the design of the product from the outset and not as an afterthought. During financial year 2017-2018 Vodafone has done thousands of

security and privacy assessments. These assessments ensure that, by design, unnecessary data is not collected, personal data is not stored for longer than necessary, right privacy notices are served, required customer permissions are sought for, personal data is not shared without proper authorizations etc. Furthermore, rigorous Supplier Reviews ensure our processors will comply with the same standards to the extent relevant for the processing they carry out on our behalf.

Vodafone provides industry leading permissions approach. In terms of customer permissions, Vodafone has launched an industry leading multi-channel approach to allow customers to manage their permissions (through MyVodafone mobile app, through MyVodafone web portal, through retail and/or call-centres. These permissions are granular and openly presented to the customers "just in time" when they are relevant. These permissions are supported by "high-light" notices where the detailed impacts of the said permission are outlined to the customer prior to them choosing whether to agree to it. Permissions can be managed by the customers any time.

Whether or not the permissions are based on opt-in or opt-out depends on the local laws and on the sensitivity of the action in question. For example, in the UK our customers are informed that marketing messages may be sent to them and they can opt-out from it any time. Non-customers are not being marketed to without their permission. Use of location data and traffic data for marketing is based on opt-in. Customers can easily opt-out of the use of their personal data for direct marketing profiling. In addition, Vodafone is the only telco in the UK to provide its customers an opt-out from the use of traffic data for the purpose of creating anonymous and aggregated insights about the population movements to support e.g. public transport agencies improve their services to the public ("smart cities").

We value the inputs that we receive from stakeholders – including Access Now – as well as the insight provided by the Ranking Digital Rights index and the Business and Human Rights Resource Centre and will continue to use these to guide us on how we can improve our transparency on these critical issues.

ENDS