Vodafone Group Plc
FY21 SASB Disclosures

Together we can

vodafone

Introduction

The Sustainability Accounting Standards Board ('SASB') is an independent organisation that provides voluntary industry-specific standards ('SASB Standards') for companies to disclose information on environmental, social and governance ('ESG') topics. In this document, we have provided responses in line with the Telecommunication Services industry-specific criteria. Where appropriate, we have provided additional context for our responses. Where available, we have also provided references to supporting disclosures available elsewhere on our website.

Under the SASB's assessment of materiality, the majority of industries in the Technology & Communications sector are asked to report on 'employee engagement, diversity and inclusion', however the SASB has not included the topic within the specific Standards applicable to the telecommunications industry. We have voluntarily responded to this additional topic as we operate in adjacent businesses and we are committed to developing a diverse and inclusive global workforce that reflects the customers and societies we serve.

Unless otherwise stated, the disclosures have been made with respect to all controlled operations within the Vodafone Group and reflect performance during the financial year ended 31 March 2021.

Contents

Activity Metrics

Topic	Code	Accounting Metric	Supporting Disclosures
Activity metrics	TC-TL-000.A	Number of wireless subscribers	2021 Web Spreadsheet
	TC-TL-000.B	Number of wireline subscribers	
	TC-TL-000.C	Number of broadband subscribers	

Vodafone is the largest mobile and fixed network operator in Europe and a leading global IoT connectivity provider. We operate mobile and fixed networks in 21 countries[1] and partner with mobile networks in 49 more.

On 31 March 2021, we had 315 million[1] mobile customers across 21 markets, 22 million[2] fixed line voice customers across 11 markets and 28 million[1] broadband customers across 17 markets.

[1] Includes VodafoneZiggo and Safaricom

[2] Includes VodafoneZiggo

Topic	Code	Accounting Metric	Supporting Disclosures
Activity metrics	TC-TL-000.D	Network traffic	2021 Web Spreadsheet

In the year ending 31 March 2021, data traffic volumes across our mobile and fixed network totalled 84,301 petabytes.

Additional Information

We monitor and report on data traffic volumes carried on our mobile and fixed network across all markets where such services are provided. Data traffic volume is reported in petabytes according to industry standard definitions using decimal values and conversion factors. Data usage represents the sum of downlink traffic and uplink traffic, all APNs (for example web, wap, corporate APNs, MMS), inbound roamers and MVNOs.

The total data traffic volumes reported above exclude Associates, Joint Ventures and Investments.

Environmental footprint

Topic	Code	Accounting Metric	Supporting Disclosures
Environmental footprint of operations	**TC-TL-130a.1**	**(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable**	2021 Annual Report, Planet (pages 38-40) and 2021 ESG Addendum

Our total global energy consumption was 5,832 GWh during FY21, equivalent to 21 million Gj. Our base stations and technology centres accounted for 96% of energy consumed, with the balance attributable to retail stores and offices.

During the year, 96% of total energy consumed was provided via the grid. During the year, 54% of total energy consumed was from renewable sources.

In July 2020, we committed that all of our European operations would purchase 100% renewable electricity no later than July 2021, significantly accelerating our previous target of 2025. We also aim to purchase 100% renewable electricity for our entire global footprint by 2025. This year, 80% of our purchased electricity in Europe was from renewable sources and we are confident that we will meet our July 2021 target. UPDATE (JULY 2021): We have since announced that from 1 July 2021, our entire operations across Europe are 100% powered by renewable electricity, with all electricity generated from solar, wind or water sources.

Additional Information

Optimising energy usage

Our strategy to optimise energy usage and improve energy efficiency involves the latest technologies; high performance equipment for servers, storage and our network; highly efficient passive infrastructure for power conversion and cooling; and smart metering and controls using IoT technology and artificial intelligence ('AI').

When selecting and procuring equipment, we consider factors such as environmental footprint and availability of features which can modulate consumption. During the product lifecycle, we avoid overcapacity and surplus resource surplus and also efficiently manage power and cooling. As an example, we use sophisticated AI-based algorithms to optimise cooling in our technology centres and big data analytics to benchmark energy consumption against traffic and monitor any inefficiencies or opportunities to reduce energy consumption.

In order to provide fast, reliable and secure connectivity services, we need to continue to invest in our network to increase capacity and deploy 5G, ultimately enabling an inclusive and sustainable digital society. As a result of the major trends shaping our industry, there will be an increase in energy consumption, however, we are committed to upgrading our networks in a way that maximises energy efficiency.

Many operators, including Vodafone, use Massive MIMO ('M-MIMO') antennas when deploying 5G on the 3.5 GHz band. M-MIMO is a relatively new technology that provides very high capacity but has high energy consumption needs. We are working closely with our network vendors to improve both hardware efficiency and software features that will enhance the energy efficiency of 5G M-MIMO. We estimate that more efficient hardware will reduce energy consumption by 10%, while software features will enable a further reduction of 15%.

We also continue to upgrade our network and use more energy efficient hardware. We are deploying multi-band radio units that achieve greater energy efficiency by including multiple frequency bands in a single product (previously radio units only supported one frequency band). On frequency bands that are upgraded, we estimate that energy consumption will be reduced by 30%.

Finally, we are making more capacity available for 4G and 5G by shutting down our 3G networks. 3G networks make less efficient use of our spectrum, and by shifting to the more spectrally efficient 4G and 5G technologies, our networks can better support large volumes of data. In turn, that translates into higher energy efficiency. This can be illustrated by comparing the energy consumption required to download 1 GB of data: 3G – 110 Wh, 4G – 30 Wh, 5G M-MIMO – 8 Wh.

Overall, by driving these efficiencies, we can significantly expand our networks, while ensuring only a relatively small increase in energy consumption.

Energy efficient investments

During FY21, we invested €65 million of capital expenditure in energy efficiency and on-site renewable projects across our business, which has led to annual energy savings of 135 GWh. Over the next three years, we will continue to invest in passive infrastructure and renewable energy and benefit from cost savings as a result.

Power usage effectiveness ('PUE') for data centres

The data centre industry uses the measurement PUE to measure efficiency. A PUE of 2.0 means that for every watt of IT power, an additional watt is consumed to cool and distribute power to the IT equipment. A PUE closer to 1.0 means nearly all of the energy is used for computing.

The trailing-twelve-month ('TTM') energy-weighted average PUE for all our owned and operated data centres was is 1.6 in FY21.

Data privacy and security

Topic	Code	Accounting Metric	Supporting Disclosures
Data privacy	TC-TL-220a.1	Description of policies and practices relating to behavioural advertising and customer privacy	2021 Annual Report, Data privacy (pages 43-45)

We believe that everyone has a right to privacy wherever they live in the world, and our commitment to our customers' privacy goes beyond legal compliance. As a result, our privacy programme applies globally, irrespective of whether there are local data protection or privacy laws.

Our privacy management policy is based on the European Union General Data Protection Regulation ('GDPR') and this is applied across Vodafone markets both inside and outside the European Economic Area. Our privacy management policy establishes a framework within which local data protection and privacy laws are respected and sets a baseline for those markets where there are no equivalent legal requirements.

We always seek to respect and protect the right to privacy, including our customers' lawful rights to hold and express opinions and share information and ideas without interference. At the same time, as a licensed national operator, we are obliged to comply with lawful orders from national authorities and the judiciary, including law enforcement.

Additional Information

Our privacy programme governs how we collect, use and manage our customers' personal data to ensure we respect the confidentiality of their communications and any choices that they have made regarding the use of their data. Our privacy programme is based on the following principles:

- **Accountability:** We are accountable for living up to our commitments throughout Vodafone and with our partners and suppliers.
- **Privacy by design:** Respect for privacy is a key component in the design, development and delivery of our products and services.
- **Fairness and lawfulness:** We comply with privacy laws and act with integrity and fairness. We also actively engage with stakeholders, including civil society, academic institutions, industry and government, in order to share our expertise, learn from others, and shape better, more meaningful privacy laws and standards.
- **Openness and honesty:** We communicate clearly about our actions that may impact privacy. We ensure our actions reflect our words and we are open to feedback.
- **Choice and access:** We give people the ability to make simple and meaningful choices about their privacy and allow individuals, where appropriate, to access, update or delete their personal data.
- **Responsible data management:** We apply appropriate data management practices to govern the processing of personal data. We carefully select external partners and we limit disclosure of personal data to what is described in our privacy notices or to what has been authorised by our customers. We also ensure personal data is not stored for longer than necessary or as is required by applicable laws and to maintain accuracy of data.
- **Security safeguards:** We implement appropriate technical and organisational measures to protect personal data against unauthorised access, use, modification or loss.
- **Balance:** When we are required to balance the right to privacy against other obligations necessary for a free and secure society, we work to minimise privacy impacts.

Data privacy and security (continued)

Topic	Code	Accounting Metric	Supporting Disclosures
Data privacy	TC-TL-220a.2	Number of customers whose information is used for secondary purposes	2021 Annual Report, Data privacy (pages 43-45)

We want to enable our customers to get the most out of our products and services. In order to provide these services, we need to use our customers' personal information. We are committed to looking after our customers' data, using it for its stated purpose, and we are always open about what we collect.

Each local market publishes a Privacy Statement to provide clear, transparent and relevant information on how we collect and use personal data, what choices are available regarding its use and how customers can exercise their rights.

Under the SASB Standards, the definition of 'secondary purposes' includes using customer data to improve our products and services. As we monitor the quality and use of our connectivity so that we can continually improve and optimise our services, this accounting metric is not meaningful.

Additional Information

Key uses of customer data are outlined below.

- **Provision of services:** We process customer personal data to provide our customers with the products and services they have requested, to fulfil our contractual and legal obligations, and to provide customer care. To provide our services and to charge our customers the correct amount, we must process communications metadata regarding calls, texts and data usage.
- **Quality, development and security of services:** We monitor the quality and use of our connectivity and other services so that we can continually improve and optimise them. This information also helps detect and prevent fraud, as well as keep our networks and services secure. We also do not sell data tied to specific individuals to third parties.
- **Marketing:** With customer permission, we will use customer data to market our products and services and provide more accurate recommendations. This means we can present our customers with offers when they need them most; for example, when they are about to run out of data.
- **Permissions:** Our multi-channel permission management platforms, deployed across all our channels (MyVodafone app, website, call centres and retail stores) allow our customers to control how we use their data for marketing and other purposes. For example, customers can express their opt-in consent to the use of their communications metadata for marketing purposes or for receiving third-party marketing messages, or they can opt-out from marketing entirely. All permissions can be revoked and choices can be changed at any time.
- **Rights of individuals:** Our businesses provide their customers with access to their data through online and physical channels. These channels can be used to request deletion of data that is no longer necessary or correction of outdated or incorrect data. Our customer privacy statements and other customer facing documents provide information on how these rights can be exercised and how to raise complaints. Our frontline staff are trained to respond to the customers' requests.
- **Sharing of data:** Where we rely on external suppliers and service providers to process data on our behalf, they are subject to security and privacy due diligence processes, and appropriate data processing agreements govern their activities. We do not share customers' personal data otherwise, unless required by law or with the consent of the customer.

Data privacy and security (continued)

Topic	Code	Accounting Metric	Supporting Disclosures
Data privacy	TC-TL-220a.3	Total amount of monetary losses as a result of legal proceedings associated with customer privacy (including a description of nature, context and any corrective actions taken)grid electricity, (3) percentage renewable	2021 Annual Report, Data privacy (pages 43-45)

We have a strong culture of data privacy and our assurance and monitoring activities are capable of identifying potential issues before they materialise. However, during the financial year, Vodafone was fined a combined €20 million for separate data privacy issues in Italy, Spain and Romania.

The fines in Italy and Spain related to Vodafone's use of third-party marketing agencies, some of which had conducted direct marketing activities towards people who had opted-out. These activities were in violation of existing supplier agreements. In limited instances, there were also delays and issues in adding people to opt-out lists as a result of human and system errors, as well as related fraudulent activities which Vodafone reported to the relevant authorities. In addition, we received a fine in Spain due to a supplier's sub-contractor's noncompliance with international data transfer rules. The fine in Romania related to a delayed response to a subject access request.

Our rules on telesales have been reviewed and compliance with these rules is subject to increased assurance and monitoring. Where necessary, improved controls have been introduced to monitor and enforce suppliers' compliance. Such measures include, for example, introduction of tools to automatically prevent or detect calls to opted-out customers, verification that commission is only paid for authorised calls, enforcement of contractual penalties for non-compliance, and discontinuation of contracts with a number of suppliers.

Data privacy and security (continued)

Topic	Code	Accounting Metric	Supporting Disclosures
Data privacy	TC-TL-220a.4	(1) Number of law enforcement requests for customer information, (2) number of customers whose information was requested, (3) percentage resulting in disclosure	Law Enforcement Disclosures

As a global telecommunications provider, our most significant human rights risks relate to our customers' rights to privacy and freedom of expression. We acknowledge that we can be faced with challenges in this area, and we collaborate with our stakeholders. We are an active member of the Global Network Initiative, alongside other initiatives such as the United Nations B-Tech Project which convenes business, civil society and government to advance implementation of the UN Guiding Principles in the tech sector.

Law enforcement and national security legislation often includes stringent restrictions preventing operators from disclosing any information relating to agency and authority demands received, including the disclosure of aggregated statistics. As a result, we are unable to publish the requested aggregated statistics with respect to the Vodafone Group as a whole.

In 2014, Vodafone was one of the first global telecommunications operators to provide country-by-country insight into the nature of the local legal regimes governing law enforcement assistance and the volume of each country's agency and authority demands (wherever that information is available and publication is not prohibited). We publish information regarding Law Enforcement Assistance on our website:

vodafone.com/handling-law-enforcement-demands

Additional Information

Vodafone's global business consists largely of a group of separate subsidiary companies, each operating 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 the relevant country.

As a licensed national communications services provider, Vodafone must address the balance between our customers' right to privacy and freedom of expression and the statutory requirements to provide law enforcement assistance to government agencies and authorities, through either lawful interception or retention of communications data.

Law enforcement and national security legislation often includes stringent restrictions preventing operators from disclosing any information relating to agency and authority demands received, including the disclosure of aggregated statistics.

In a number of countries, the law governing disclosure remains unclear; it can also be difficult to engage with the relevant authorities to discuss these issues. Where we are unable to obtain any clarity regarding the legality of disclosure, we have refrained from publishing any statistics.

Vodafone first published statistics on the number of law enforcement demands in 2014 and our core principles and practices are unchanged. For those markets where disclosure is possible, we provide a breakdown of the number of demands received on a country-by-country basis. This covers the number of demands received to conduct lawful interception, or to disclose communications data.

Despite our ongoing transparency in this area, there remains no established reporting model to follow when compiling the information requested, 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.

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.

Data privacy and security (continued)

Topic	Code	Accounting Metric	Supporting Disclosures
Data privacy (continued)	**TC-TL-220a.4 (continued)**	**(1) Number of law enforcement requests for customer information, (2) number of customers whose information was requested, (3) percentage resulting in disclosure**	Law Enforcement Disclosures

Additional information (continued)

Law Enforcement Assistance policy

Vodafone has a clear set of principles that are used to determine when communications data (which could include metadata such as names, addresses and services subscribed) should be disclosed:

We do not:

- Allow any form of access to any customer data by any agency or authority unless we are legally obliged to do so;
- Go beyond what is required under legal due process when responding to demands for access to customer data other than in specific safety or life emergencies (such as assisting the police with an active kidnapping event) or where refusal to comply would put our employees at risk; or
- Accept any instructions from any agency or authority acting beyond its jurisdiction or legal mandate.

We do:

- Insist that all agencies and authorities comply with legal due process;
- Scrutinise and, where appropriate challenge the legal powers used by agencies and authorities in order to minimise the impact of those powers on our customers' right to privacy and freedom of expression;
- Honour international human rights standards to the fullest extent possible whenever domestic laws conflict with those standards;
- Communicate publicly any threats or risks to our employees arising as a consequence or our commitments to these principles, except where doing so would increase those risks; and
- Seek to explain publicly the scope and intent of the legal powers available to agencies and authorities in all countries where it is lawful to do so.
- In each of our operating companies, a small group of employees are tasked with liaising with agencies and authorities in order to process demands received. Those employees are usually security cleared and are bound by strict national laws to maintain confidentiality regarding both the content of those demands and the methods used to meet them.

Conditions for disclosing customer data

We will provide assistance in response to a demand issued by an agency or authority with the appropriate lawful mandate and where the form and scope of the demand is compliant with the law. Each of our local operating businesses is advised by senior legal counsel with the appropriate experience to ensure compliance with both the law and with our own principles.

Notifying customers

Local laws will dictate whether operators are able to notify a customer in the event of being in receipt of a lawful demand to disclosure their data. Law enforcement demands are sensitive in nature and we believe it is for governments to provide clear guidelines to operators on any risks associated with notifying a customer.

Data privacy and security (continued)

Topic	Code	Accounting Metric	Supporting Disclosures
Data security	**TC-TL-230a.1**	**(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of customers affected (including a description of any corrective actions taken)**	2021 Annual Report, Cyber security (pages 45-47)

As a global connectivity provider, we are subject to cyber threats, which we work to identify, block and mitigate with our robust control environment without any impact. Where a security incident occurs, we have a consistent incident management framework and an experienced team to manage our response. The focus of our incident responders is always fast risk mitigation and customer security.

Vodafone classifies security incidents according to severity, measured by business and customer impact. The highest severity category corresponds to a significant data breach or loss of service caused by the incident. In the past financial year, there was one incident that fell within this category.

In the event of a cyber breach, disclosure is made in line with local regulations and laws, and we ensure any risks are transparently communicated with law enforcement, relevant authorities, our external auditor and customers. The European Union's General Data Protection Regulation ('GDPR') provides a framework for notifying customers in the event there is a loss of customer data as a result of a data breach and this framework is a baseline across all our markets.

Additional Information

In December 2020, ho. Mobile, a second brand in Italy, suffered a data breach and part of a database holding customer data was accessed by a third-party; no financial information, passwords, or mobile traffic data relating to calls, texts or web activity was involved. We utilised our existing global incident management framework. Ho. Mobile took a proactive approach and immediately informed affected customers and regulators, enhanced security protections, remotely reissued SIM serial numbers to prevent any misuse, and offered free replacement SIMs to the entire customer base. Ho. Mobile also notified local law enforcement and made the required disclosures to the Italian Data Protection Authority. Ho. Mobile uses distinct and separate IT systems to Vodafone Italy and the rest of the Vodafone Group.

Data privacy and security (continued)

Topic	Code	Accounting Metric	Supporting Disclosures
Data security	**TC-TL-230a.2**	**Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards**	2021 Annual Report, Cyber security (pages 45-47) and Risk management (pages 53-61)

Our networks connect millions of people, homes, businesses and things to each other and the internet. The security of our networks, systems and customers is a top priority and a fundamental part of our purpose. Our customers use Vodafone products and services because of our next-generation connectivity, but also because they trust that their information is secure.

Cyber security is a principal risk. We recognise that if not managed effectively, there could be major customer, financial, reputation or regulatory impacts. Risk and threat management are fundamental to maintaining the security of our services across every aspect of our business.

To help us identify and manage emerging and evolving risks, we constantly evaluate and challenge our business strategy, new technologies, government policies and regulation, and cyber threats. We conduct regular reviews of the most significant security risks affecting our business and develop strategies to detect, prevent and respond to them. Our cyber security approach focuses on minimising the risk of cyber incidents that affect our networks and services.

Additional Information

Controls can prevent, detect or respond to risks. Most risks and threats are prevented from occurring and most will be detected before they cause harm and need a response. A small minority will need recovery actions.

We use a common global framework called the Cyber Security Baseline and it is mandatory across the entire Group. The baseline includes key security controls which significantly reduce cyber security risk, by preventing, detecting or responding to events and attacks. Our framework was initially developed based on an international standard mapped to our key risks in the way that provides the most comprehensive protection. Each year, we review the framework in the light of changing threats and create new or enhanced controls to counter these threats.

A dedicated assurance team reviews and validates the effectiveness of our security controls, and our control environment is subject to regular internal audit. The security of our global networks is also independently tested every year to assure we are maintaining the highest standards and our controls are operating effectively. We maintain independently audited information security certifications, including ISO 27001, which cover our global technology function and 15 local markets. We also comply with local requirements or certifications and actively contribute to consultations and debates with regard to laws and regulations that aim to improve and assure the security of communications networks.

Circular economy

Topic	Code	Accounting Metric	Supporting Disclosures
Product end-of-life management	**TC-TL-440a.1**	**(1) Materials recovered through take back programs, percentage of recovered materials that were (2) reused, (3) recycled, and (4) landfilled**	2021 Annual Report, Planet (pages 38-40), 2021 ESG Addendum and EcoRating press release

Apart from carbon emissions, electronic waste is a material environmental issue for our business. We have consistently sought to manage our own impact in a responsible manner and also support our customers with their efforts. We are increasingly adopting circular economy approaches to reduce this impact through extending useful life, repairing, refurbishing and responsibly recycling electronic equipment across our business.

Most of our markets operate trade-in and device buyback schemes and repair services to encourage customers to repair or return their old devices. We also strive to refurbish and reuse fixed-line equipment multiple times, with significant associated environmental and cost savings.

During FY21, we collected, refurbished and resolved 1,500 metric tonnes of consumer devices, such as handsets, routers and IoT devices. We recycled a further 1,900 metric tonnes of consumer devices that could not be refurbished or resold.

Additional Information

Local schemes include trade-in and device buy-back schemes, drop-off boxes in retail stores, freepost return envelopes and repair services to encourage customers to repair or return their old devices and routers. Returned devices are refurbished and resold. Where this is not possible, we work with specialist partners to separate and recycle components. We also work with our suppliers to improve the efficiency of material use, reduce unnecessary material and promote the use of recycled and recyclable materials; as well as extending useful life, repairability and recyclability.

Given a large part of the solution to drive circularity for devices depends on industry action, we recently joined the Circular Electronics Partnership, which brings together leaders across the value chain – from manufacturing, reverse logistics, material recovery, to e-waste management – to drive circularity solutions for electronics.

In May 2021, five of Europe's leading mobile operators – including Vodafone – announced that they had jointly created a new pan-industry Eco Rating labelling scheme that will help consumers identify and compare the most sustainable mobile phones and encourage suppliers to reduce the environmental impact of their devices. From June 2021, the participating mobile operators will begin to introduce the distinct Eco Rating labelling at point of sale where they are present across Europe.

Customers can learn more about the initiative and see how the rating is calculated by visiting a new website at:

ecoratingdevices.com

Competitive behaviour

Topic	Code	Accounting Metric	Supporting Disclosures
Competitive behaviour & open internet	**TC-TL-520a.1**	**Total amount of monetary losses as a result of legal proceedings associated with anticompetitive behaviour regulations (including a description of nature, context and any corrective actions taken)**	2021 Annual Report, Responsible business (page 43)

Vodafone has a zero-tolerance approach to competition law breaches. We understand that a lack of competition adversely affects customers and the potential for investigations, fines, reputational damage and subsequent damages claims is high and potentially financially material.

There were no cases where Vodafone was found to have been involved in any anti-competitive conduct in FY21.

Additional Information

The telecommunications sector is characterised by a high level of competitive intensity, with many alternative providers giving customers a wide choice of suppliers. In each of the countries in which we operate, there are typically three or four mobile network operators ('MNOs'), such as Vodafone, which own their own network infrastructure, as well as several resellers that 'wholesale' network services from MNOs.

Operators face significant investment cycles in the context of ever-increasing levels of demand for network capacity and deflationary prices. Where industry costs are expected to increase, it is part of the competitive process that operators individually start to consider their options. Operators, including Vodafone, need to ensure they are able to keep up with the increasing need for further investment in network infrastructure to enable societies to remain connected. The options available to operators include cost saving initiatives, such as entering into active and/or passive network sharing arrangements, acquisitions of attractive businesses belonging to other operators and adjustments to commercial practices, including pricing.

Fixed telecoms markets in most countries are still dominated by the historic incumbent operator (typically the former state-owned operator), in particular at the wholesale level. Access to many wholesale services from the incumbent, such as fixed access and leased lines, is still regulated in most countries.

Despite the inherently complex nature of the telecommunications sector and the rapidly changing market dynamics, there have been relatively few examples of anti-competitive behaviour or accusations made against Vodafone in recent years.

Historically, in cases where Vodafone was found to have engaged in anti-competitive conduct, penalties were relatively low. The only exception in recent years has been a case regarding billing cycles in Italy, involving four operators, including Vodafone, and the national telecom industry association ('Asstel'). In January 2020, the Italian Competition Authority ('AGCM') decided that the operators went beyond legitimate joint lobbying of the regulators, ministries and legislators and reached an agreement or understanding that the operators would all apply the same price increase to their monthly pricing so as to maintain annual revenues after the shift back from 28 day billing to monthly billing (as required by the legislator). The AGCM imposed fines totalling €229 million against the operators; Vodafone's fine was €60 million. Vodafone strongly disputed all the allegations against it and appealed against the AGCM's decision. UPDATE (JULY 2021): Following appeal, the Regional Administrative Court of Lazio annulled the fines imposed by the Italian Competition Authority, including Vodafone's €60 million fine. The Court rejected the Italian Competition Authority's argument because of limited evidence and ruled that operators were acting within their rights and no anti-competitive behaviour had occurred. The Italian Competition Authority has the right to appeal the judgement to the Italian Council of State (last instance).

Nonetheless, during the investigation, Vodafone took further steps to strengthen its competition law compliance programme by introducing additional procedures aimed at minimising the risk of anti-competitive information sharing and engagement with competitors, including via trade associations, These additional procedures are applicable to all local employees, including senior management. Examples of the additional procedures include specific training for individuals that are exposed to higher risks from information exchange and engagement with actual or potential competitors, including via trade associations and other external meetings, and a system of economic disincentives and disciplinary measures to deter non-compliance.

Competitive behaviour (continued)

Topic	Code	Accounting Metric	Supporting Disclosures
Competitive behaviour & open internet	TC-TL-520a.2	Average actual sustained download speed of (1) owned and commercially associated content and (2) non-associated content	

We consider all content carried on our Mobile and Fixed networks as non-associated content under the definition within the SASB Standards.

We provide our customers with Mobile and Fixed connectivity products and services and operate across multiple countries and continents. Given the distinct differences between technologies and regions, we have provided average sustained download speeds across multiple categories below.

Mobile networks

	Average sustained download speed Mbps	
Region	5G-preferred mode	4G-preferred mode
Europe	101Mbps	44Mbps
Africa	n/a	39Mbps

Fixed networks – Europe

Access Technology	Typical speed tier/proposition range	Average sustained download speed Mbps
FTTH / Hybrid Fibre Coaxial	100 - 500Mbps	285Mbps
xDSL	38 - 100Mbps	61Mbps

Additional Information

We use various tools and techniques to measure our customers' user experience on our mobile and fixed access networks. Part of our approach involves the use of independent third-party benchmark providers who conduct regular active field-testing on our behalf in the markets where we operate.

Mobile networks

Vodafone uses the industry-recognised benchmark provider to perform annual testing of all our mobile networks in the markets where we operate. The testing tool is equipped with 5G-capable devices to measure the 5G network performance where available. In locations where 5G coverage is not deployed, the tests are executed using the 4G networks. The testing configuration is defined to represent the achievable customer experience.

The regional averages presented above are calculated by combining the results of the Vodafone markets in scope using the size of the customer base in each market as a weighting factor. The weighted average sustained download speeds for Europe include all our markets in Europe, as well as VodafoneZiggo and Turkey. The average sustained download speeds for Africa reflect data from Vodacom (South Africa) and Ghana.

Fixed networks

Similar to the Mobile measurement methodology, Vodafone engages with independent third-party benchmark companies to regularly test typical customer experience on our Fixed networks.

Active probes connected to Vodafone customers' routers and internet switches perform regular speed tests to ensure a statistically valid sample across the most penetrated speed tiers/propositions in each market. Network performance is measured to the closest content delivery network for each customer.

Download speeds, defined as data throughput in Mbps, are observed over a 24-hour period and reported as an average according to the underlying access technology, either xDSL or FTTH/Hybrid Fibre Coaxial technologies.

The regional averages presented above are calculated by combining the results of the Vodafone markets in scope using the size of the customer base in each market as a weighting factor. The weighted average sustained download speeds for Europe reflect data for Italy, UK, Spain, Portugal, Ireland, Greece and Romania only.

Competitive behaviour (continued)

Topic	Code	Accounting Metric	Supporting Disclosures
Competitive behaviour & open internet	TC-TL-520a.3	Description of risks and opportunities associated with net neutrality, paid peering, zero rating, and related practices	

We are subject to rules governing our business activities in the markets in which we operate. The rules typically take the form of sector-specific laws and regulations.

Net Neutrality laws and regulations seek to safeguard equal and non-discriminatory treatment of traffic in the provision of internet access services and related end-users' rights.

Our services are always designed with these obligations in mind, reflective of our commitments to our customers and digital society at large, as part of our 'social contract'.

We support the open internet and believe that consumers should be in control of what they do online.

Additional Information

Our purpose is to 'connect for a better future'. We believe we can play a critical role in delivering the next-generation connectivity that will create a resilient and transformative digital future that works for everyone. That is why introduced our 'social contract' in 2019, which represents the partnerships we continue to develop with governments, policy makers and civil society. Our social contract is aimed at ensuring that the connectivity sector is able to succeed in a way that enables the entire economy and the wider world to thrive. Delivering high quality digital connectivity is a prerequisite to a global digital economy that benefits all of our customers (individuals, SMEs and enterprises) and wider society.

The events of the last year have underscored the importance society places on fast, reliable and secure connectivity with lower latency. We are committed to expanding and future-proofing our network infrastructure for the benefit of all our customers. Overcoming the deep digital divides – between people, businesses and communities – that the pandemic has exposed requires both public and private investment in digital, along with policy reforms that are pro-investment, pro-innovation and supportive of returns. Beyond the availability of connectivity, we need to ensure that connectivity is secure and fit for purpose as more of the economy becomes increasingly reliant on secure and reliable digital connectivity. We see our regulatory obligations to be reflective of this commitment, and in return, work closely with policymakers and regulators to ensure that regulation remains supportive of network deployment, investment and digital connectivity.

We support the open internet and believe that consumers should be in control of what they do online. Our role is to enable consumers to benefit from that freedom.

We are committed to safeguarding the principle of the best-efforts public internet, accessible to all:

- for consumers, so that they can choose different tariffs and packages that best fit their needs;
- for enterprise services, which require guaranteed speeds and quality; and
- for 5G and connected devices, which rely on specific quality requirements such as speed, jitter and latency.

Differentiated services and commercial propositions encourage operators to invest in their networks and offer innovative services to businesses and consumers. This differentiation ultimately translates into further opportunities to fund investment in network capacity, benefitting all content and application providers, as well as customers. As operators invest and innovate, through the deployment of new technologies and services, the breadth of services and the speeds available to customers and broader society will continue to improve.

During a global health emergency, we all need to do our part, which is why since the start of the COVID-19 pandemic we have undertaken initiatives to zero-rate access to many websites for essential public services, such as healthcare and domestic violence. For example, in the UK, we zero-rated the National Health Service ('NHS') website and also domestic abuse charity sites. In South Africa, we zero-rated the website of South African Unemployment Fund (UIF), as well as for public hospitals and clinics. These are just a few examples of such activity across our footprint.

More broadly, Vodafone regularly engages with regulatory authorities in the countries in which we operate – not least through public consultation processes or in our role as a member of industry groups – to provide our technical and technological expertise and business perspectives on net neutrality policy and regulation as the market and technology continues to evolve.

Technology resilience

Topic	Code	Accounting Metric	Supporting Disclosures
Managing systemic risks from technology disruptions	TC-TL-550a.1	(1) System average interruption frequency and (2) customer average interruption duration (including a description of each significant issue and corrective actions)	

In line with industry best practice, Vodafone classifies and prioritises the resolution of each service disruption or incident according to the severity of its customer and business impact. The figures presented below reflect 15 high-impact and critical incidents identified and resolved during FY21.

(1) System average interruption frequency

Mobile: 0.17 interruptions per customer throughout FY21
Fixed: 0.03 interruptions per customer throughout FY21

(2) Customer average interruption duration

Mobile: 0.0017 hours (equivalent to 6 seconds throughout FY21)
Fixed: 0.0750 (equivalent to 4 minutes, 30 seconds throughout FY21)

Vodafone drives a culture of continuous improvement and seeks to identity lessons learned from all service interruptions reported. In FY21, we reported a 18% year-on-year reduction for the total number of high impacting/critical incidents across our Mobile and Fixed networks within our European footprint.

Additional Information

The averages presented above are calculated by combining the results for the following Vodafone markets: Germany, Italy, UK, Spain, Portugal, Ireland, Czech Republic, Hungary, Romania and Albania. Assets acquired in Germany and Central and Eastern Europe in FY20 are not within scope of the calculations for FY21 but will be included in future years.

The number of customer interruptions was calculated by multiplying the number of customers impacted by an interruption to one or more service (Mobile: 2G, 3G, 4G or Fixed: Data, Voice and TV) and aggregating the results for the 15 high-impact and critical incidents within scope. If any customers experienced more than one interruption to one or more services during the year, each individual interruption is reflected in the calculations.

System average interruption frequency

We calculate the System average interruption frequency by aggregating all the customer interruptions within the reported incidents and dividing this by the number of unique customer accounts with active service during the period.

Customer average interruption duration

We calculate the average interruption duration by aggregating the total downtime (in hours) and dividing this by the number of customer accounts affected during the period.

Technology resilience (continued)

Topic	Code	Accounting Metric	Supporting Disclosures
Managing systemic risks from technology disruptions	**TC-TL-550a.2**	**Discussion of systems to provide unimpeded service during service interruptions**	2021 Annual Report, Risk management (pages 53-61)

We define technology failure as network, system or platform outages resulting from internal or external events leading to reduced customer satisfaction, reputational damage and/or regulatory penalties. Technology failure could arise as a result of technical failures, cyber-attacks, or weather events.

In our FY21 TCFD Report, we identified a long-term climate-related physical risks to our business. An increase in temperature and frequency of extreme weather events could result in damage to our technology equipment. Damage to our infrastructure as a result of sea-level rise, flooding and fire is therefore considered one of the top physical risks impacting our operations.

Technology failure is one of our principal risks and is therefore subject to oversight from the Group's Risk and Compliance Committee ('RCC') and the Audit and Risk Committee ('ARC'). The Chief Technology Officer is the assigned executive-level risk owner and is accountable for confirming adequate controls are in place and that the necessary treatments plans are implemented to bring the risk profile within an acceptable tolerance. The recovery of key services and platforms must be fast and robust if we are to maintain customer trust.

Additional Information

Our approach to managing the risk of technology failure is to ensure that we reduce the impact of disruptions within our risk appetite. This is achieved by categorising our operations and services according to business criticality and customer impact. Business continuity and disaster recovery plans are then created for critical operations and datacentres. These plans are reviewed at least annually and regularly tested.

Our datacentres are situated across multiple sites and our network infrastructure is designed to ensure that we can quickly and easily recover from any hardware faults. Data is replicated in real-time, backed-up and secured. Should a major incident occur, we are able to automatically transition to another datacentre and ensure continuous service availability for our customers.

In the event of a major incident, we follow the Group's global business continuity and disaster recovery plans, as well as our established emergency and crisis management plans and incident management processes. Communications processes are designed to escalate major incidents/disasters to key employees, as well as establish critical communications teams to manage the disaster. We strongly believe in the importance of prevention; however, we also believe that incidents should be treated as an opportunity for learning.

Our technology resilience policy is applied across all markets and business areas that operate technology. The technology resilience policy includes a number of key controls, such as:

- **Physical site risk assessments:** All our sites and business operations are regularly reviewed for environmental (e.g. flooding/climate change), physical security, infrastructure and technology risks. Mitigation plans such as flood defences, fire suppression systems or perimeter fencing, are then applied to ensure risks are appropriately managed.
- **Service level targets:** Critical business operations are identified and evaluated regularly to ensure they are recoverable within a specified timeframe (for example, requiring that 95% of services are recoverable within 4 hours). Service level targets apply to individual mobile sites, IT applications, datacentres, and services such as video and payment services.
- **Continuity testing:** All our sites are required to complete simulated site-loss tests on an annual basis. This must include a live-traffic component and teams are required to produce detailed reports and reflect on lessons learned. Local markets are also required to test individual components, applications and services regularly.

Additionally, Vodafone Group holds insurance policies that cover the costs of damage to infrastructure and resulting network interruption, in whole or in part. Vodafone's cyber liability insurance covers the costs for of technology failure through cyber attacks, viruses, or programming errors and any resulting data loss.

Employees

Topic	Code	Accounting Metric	Supporting Disclosures
Employee engagement, diversity & inclusion: Global headcount	**TC-SI-330a.1**	**Percentage of employees that are (1) foreign nationals and (2) located offshore (including a description of potential risks of recruiting foreign nationals and/or offshore employees, and management's approach to addressing these risks)**	2021 ESG Addendum, Headcount tab

Vodafone Group Plc is registered and headquartered in the United Kingdom. We operate mobile and fixed networks in 19 countries throughout Europe and Africa (excluding Associates and Joint Ventures) and partner with mobile networks in 49 other countries. We also have employees based in a further 22 countries, primarily supporting our Vodafone Business customers.

Our UK operating company provides connectivity products and services to consumers, businesses and the public sector. We also have a number of Group support functions based in the UK. Overall, 10% of our global workforce, comprising employees and contractors, is based in the UK. As a global business, we do not consider non-UK based employees to be 'offshore' – in most cases, they are closer to our customers and ensure that their local communities keep connected.

We have a fair, open and transparent resourcing process that is equitable for all. Any recruitment of foreign nationals is subject to considerations around local legislation, tax compliance, right to work in the country of employment, and cost of moving talent.

Topic	Code	Accounting Metric	Supporting Disclosures
Employee engagement, diversity & inclusion: Employee engagement	**TC-SI-330a.2**	**Employee engagement as a percentage**	2021 Annual Report, People strategy (pages 21-22 and 36)

Our employee engagement index[1] was 74 in 2021 (max score: 100). The overall response rate was 86%.

[1] The employee engagement index is based on a weighted average index of responses to three questions: satisfaction working at Vodafone, experiencing positive emotions at work, and recommending us as an employer.

Additional Information

Our culture – called the 'Vodafone Spirit' – outlines the beliefs we stand for and the behaviours enabling our strategy and purpose. The Vodafone Spirit is the catalyst for change, underpinning the successful and sustainable delivery of our transformation.

At the start of the financial year, we launched a survey called 'Spirit Beat' to replace our annual employee survey. We use Spirit Beat surveys to measure our culture and its impact. The results show a strong adoption of the Spirit beliefs and behaviours. In the second survey undertaken in January 2021, scores remained relatively consistent in a time of unprecedented change. The scores also outlined strengths and areas of focus to embed our culture further.

Our Spirit Beat surveys are conducted using artificial intelligence and the results are used to encourage the adoption of our Spirit behaviours. Following completion and based on confidential survey responses, all employees receive automated and personalised coaching tips called 'nudges' over a 20-week period, to support behaviour change and the creation of new habits. These personalised nudges create a continuous feedback loop and over 750,000 nudges have been sent to employees so far. Subsequent analysis has shown the value of these nudges: 71% of colleagues found nudges useful, and data shows that teams with managers who embraced the Vodafone Spirit had a higher Spirit Index (+13) and employee engagement score (+15) compared to managers who did not.

Employees (continued)

Topic	Code	Accounting Metric	Supporting Disclosures
Employee engagement, diversity & inclusion: Diversity & inclusion	TC-SI-330a.3	Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees (including a description of policies and programs for fostering equitable employee representation across its global operations)	2021 Annual Report, Workplace equality (pages 36-37) and Fair pay at Vodafone (page 97)

We are committed to developing a diverse and inclusive global workforce that reflects the customers and societies we serve.

We aim to have 40% women in management roles by 2030. We have now reached 32%, and continue to drive progress through our programmes, policies and leadership incentives.

Gender Diversity (FY21)	Female	Male
Board	45%	55%
Executive Committee	29%	71%
Senior leadership roles (FY21: 178)	30%	70%
Management and senior leadership roles (FY21: 6,609)	32%	68%
External hires	43%	57%
Graduates	53%	47%
Overall workforce	40%	60%

Additional Information

Our commitment to diversity and inclusion is reflected across our global policies and principles, such as our Code of Conduct and our Fair Pay principles. Our second Fair Pay principle – 'free from discrimination' – requires that our pay should not be affected by gender, age, disability, gender identity and expression, sexual orientation, race, ethnicity, cultural heritage or belief. We annually compare the average position of our men and women against their market benchmark, grade and function to identify and understand any differences, and take action if necessary.

To improve gender diversity within our organisation, we have a number of programmes in place. These include global parental leave policy, which supports families to share caring responsibilities in the home, flexible working policies, our Domestic Violence and Abuse policy, and our ReConnect programme. Targets regarding women in management have also been embedded as part of broader Environmental, Social, and Governance ('ESG') measures in our Long-Term Incentive Plans for our Executive Committee and Senior Leadership Team.

To better understand representation across our organisation and target diversity and inclusion programmes more effectively, we launched a campaign called #CountMeIn in November 2020, which encourages employees to voluntarily self-declare their diversity demographics. These include race, ethnicity, disability, sexual orientation, gender identity and caring responsibilities, in line with local privacy and legal requirements. Our intention is to use this data to set leadership targets around race and ethnicity, to complement our commitments on gender, by the end of 2021. We are still in the process of collecting robust and complete data for our entire workforce, however 29% of our Executive Committee members are from ethnically diverse backgrounds.

Together we can

Contact details

Investor Relations

ir@vodafone.co.uk
vodafone.com/investor

Media Relations

vodafone.com/media/contact

Sustainability

vodafone.com/sustainability

Online Annual Report

vodafone.com/ar2021

With the exception of the metrics outlined in the 'Subject Matter Information' tab in our ESG Addendum, the information contained within this report has not been independently verified or assured. All the information included in this report has been taken from sources which we deem reliable. While all reasonable care has been taken to ensure the accuracy of the content, Vodafone has not independently verified its accuracy or completeness. Further information on methodologies is included in the 'Scope of Reporting' and 'How we report our KPIs' tabs in our ESG Addendum.

Designed and produced by Black Sun plc