

Vodafone Group Plc

FY22 SASB Disclosures



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. On this page, we have provided responses in line with the Telecommunication Services industry-specific criteria. Where appropriate, we have provided additional context for our responses, which can be viewed by clicking the expand button under each response. 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 2022.

Contents

02 | Activity metrics

11 | Product end-of-life management

03 | Environmental footprint of operations

12 | Competitive behaviour and open internet


04 | Data privacy

17 | Managing systemic risks from technology disruptions

09 | Data security

20 | Employee engagement, diversity & inclusion

Activity Metrics

Topic	Code	Accounting Metric	Supporting Disclosures
Activity metrics	TC-TL-000.A	Number of wireless subscribers	 2022 Web Spreadsheet
	TC-TL-000.B	Number of wireline subscribers	
	TC-TL-000.C	Number of broadband subscribers	

Disclosure

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 countries¹ and partner with mobile networks in 48 more.

On 31 March 2022, we had:

- 323 million¹ mobile customers **[TC-TL-000.A]** across 21 markets (FY21: 315 million); and
- 28 million¹ broadband customers **[TC-TL-000.C]** across 17 markets (FY21: 28 million).

We no longer report fixed line voice customers **[TC-TL-000.B]** as society and our customer base increasingly use other communication channels that rely on internet connectivity, such as VoIP or video conferencing.

1. Includes VodafoneZiggo and Safaricom
2. Includes VodafoneZiggo

Activity metrics

TC-TL-000.D

Network traffic

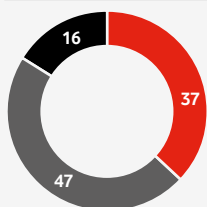
 [2022 Web Spreadsheet](#)

Disclosure

In the year ending 31 March 2022, data traffic volumes across our mobile and fixed network totalled 98,247 Petabytes **[TC-TL-000.D]** (+16% YoY vs. FY21: 84,699 petabytes).

During FY22, 47% of data traffic across our network was driven by the major web platforms such as Google, Facebook, Netflix and Amazon. A further 16% of data traffic on our network was attributed to Content Delivery Networks, which typically host content for other digital content providers such as Disney+, Tik-Tok, Zoom, HBO and DAZN.

Network Data Volume Drivers




- Other
- Content Delivery Networks for apps such as Disney+, Tik-Tok, Zoom, HBO, DAZN, etc.
- Google, Facebook, Netflix and Amazon

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, including all traffic types (i.e. streaming, browsing, gaming, Peer-2-Peer, etc.).

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	 2022 Annual Report, Planet (pages 41-44) and 2022 ESG Addendum

Disclosure

Energy consumption

Our total global energy consumption was 5,926 GWh during FY22 (FY21: 5,997 GWh), equivalent to 21 million GJ [TC-TL-130a.1(1)] (FY21: 21 million GJ). Our base stations and technology centres accounted for 96% of energy consumed, with the balance attributable to retail stores and offices.

Energy sources

During the year, 95% of total energy consumed was provided via the grid [TC-TL-130a.1(2)] (FY21: 95%).

In July 2021, we reached a key milestone in our journey to net zero by 2040, achieving our goal to purchase 100% renewable electricity in all of our European markets. We are working to achieve the same in our African markets by 2025.

As a result of our progress in Europe, 73% of total energy consumed across the Group was from renewable sources during the year [TC-TL-130a.1(3)] (FY21: 53%).

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 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 traffic 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 antennas. 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 (legacy 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 – 100 Wh, 4G – 20 Wh, 5G M-MIMO – 6 Wh.

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

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 1.59 in (FY21: 1.64).

Data privacy

Topic	Code	Accounting Metric	Supporting Disclosures
Data privacy	TC-TL-220a.1	Description of policies and practices relating to behavioural advertising and customer privacy	 2022 Annual Report, Data privacy (pages 47-49)

Disclosure

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 when we obtain and handle customer data, including asking for the consent of the data subject where necessary. 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 the data we collect, as well as 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.
- **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.

Responsible data management

We apply appropriate data management practices to govern the processing of personal data 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 offer several data-based products to our customers without sharing our customers' personal data. For example, our Vodafone Analytics product offers anonymous and aggregated insights which are based on network location data to our public sector and business customers. The product harnesses the power of anonymised geospatial movement data of our customers to give organisations adopting the product a better understanding of how populations move in space and time, all while protecting the privacy of our customers. These insights are used by Vodafone Business customers for transport or retail planning purposes as cities and urban areas become 'smart'. It is important to note that we only use fully anonymised data and only provide aggregated insights generated after multiple processes and extrapolation techniques. Once we have aggregated and anonymised customer-level data, individual customers cannot be identified or targeted with personal advertisements and we never share the actual raw data to ensure the privacy of our customers is respected. Our customer privacy statements are also open and transparent about this use of data and we allow customers to opt-out.

More information on Vodafone Analytics can be found here:




vodafone.co.uk/privacy/vodafone-analytics

In addition to our Locations Insights product, some of our services require that we share customer data by their very nature. For example, when our customers are roaming abroad, we need to share communications metadata with other operators to ensure customers are billed the correct amount.

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. Our European customer data is stored on servers in Europe and any transfers of personal data across national borders are subject to robust data transfers compliance procedures, including use of additional safeguards, such as encryption, anonymisation or pseudonymisation. These processes apply to both internal data transfers (such as with our shared service centres), as well as with suppliers and partners.

Data privacy (continued)

Topic	Code	Accounting Metric	Supporting Disclosures
Data privacy	TC-TL-220a.2	Number of customers whose information is used for secondary purposes	 2022 Annual Report, Data privacy (pages 47-49)

Disclosure

We want to enable our customers to get the most out of our products and services. To provide these services, we need to use our customers' personal information. We are committed to protecting our customers' data, using it for a stated and specific purpose, and we are always open about what customer data we collect, and why we collect it.

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. Our product specific privacy notices include details relating to a particular product. These statements and notices are available to customers online, in the MyVodafone app and in our retail stores.

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. **[TC-TL-220a.2]**

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. We also use customer data to help detect and prevent fraud, as well as keep our networks and services secure. We do not sell data tied to specific individuals to third parties.
- **Marketing and online advertising:** With customer permission, we will use customer data to market our products and services and provide more accurate and tailored 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.
- **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. Ultimately, all third parties that we share customer data with are required to comply with our own Privacy Policies. New suppliers are subject to onboarding supplier security and privacy verification procedures to ensure our standards are met. We do not share customers' personal data otherwise, unless required by law or with the consent of the customer.


Permissions management platform

Our businesses provide our customers with access to their data through online and physical channels. These channels can be used also to request deletion of data that is no longer necessary, or for correction of outdated or incorrect data, or for data portability. Our customer privacy statements and other customer facing documents provide comprehensive information on how these rights can be exercised and how to raise complaints or contact the relevant data protection authority. Our frontline retail and customer support staff are trained to respond to the customers' requests.

Our state-of-art, multi-channel permission management approach was deployed across our channels (MyVodafone app, website, call centres and retail stores) in 2018. This approach allows our customers to control how we use their data for marketing and other purposes at any time and the permissions are synchronised across our channels. For example, customers can:

- Opt-in for processing of special categories of data;
- Choose what data we collect through the MyVodafone app and how it is used;
- Opt-out from marketing across different channels (call, SMS, notifications), or opt-in to the use of their communications metadata for marketing purposes or for receiving third-party marketing messages; and
- Opt-out from the use of anonymised network and location data ('Vodafone Analytics').

Data privacy (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)	 2022 Annual Report, Data privacy (pages 47-49)

Disclosure


We have a strong culture of data privacy and our assurance and monitoring activities are designed to identify potential issues before they materialise. However, during the financial year, Vodafone was fined €2 million (FY21: €20 million) for data privacy issues, primarily relating to telesales and customer authentication practices in Spain. **[TC-TL-220a.3]** In response to the incidents in Spain, we have established a dedicated taskforce that reports directly to the Vodafone Spain Executive Committee. The taskforce also contributed to a new industry code of conduct on telesales published in July 2021.

Fines relating to telesales arose as some of our third-party marketing agencies had conducted direct marketing activities towards people who had opted-out. These activities were in violation of existing supplier agreements. In response to these incidents, 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, the routing of third-party telesales through Vodafone's systems which ensures that calls to opted-out customers are detected and blocked, verification to ensure that commission is only paid for authorised calls, strict enforcement of contractual penalties for non-compliance, and the discontinuation of contracts with several suppliers.

Third parties are increasingly using mobile devices to verify the identity of their customers. For example, banks or websites may issue one time access codes sent via SMS to verify an individual's identity. As a result, there has been an increase in attackers attempting to exploit telecommunication authentication processes for fraudulent purposes. One method involves attackers using social engineering to access customers' telecommunications accounts with the aim of swapping SIMs to new devices or setting up call forwarding. In response to these trends, the Spanish data protection regulator has issued penalties to the main telecommunications companies operating in the country, including Vodafone, for not having stronger levels of authentication processes to prevent such fraudulent activities from occurring. We have been actively collaborating with other local telecommunications operators, the banking sector, law enforcement authorities and the local data protection regulator through a cross-industry taskforce, with the aim of resolving fraudulent customer authentication practices. We have also implemented new technology tools to minimise the risk of further fraudulent activities in Spain, updated our global security policies and are in the process of implementing new tools in our markets.

In addition to the fines in Spain, our businesses in Hungary, Romania, Ireland and Turkey received immaterial fines for data privacy issues. These fines arose as a result of a delayed response to a subject access request, direct marketing towards people who had opted-out of being contacted, and an issue relating to notifying customers about how their personal data was processed. These cases were isolated incidents and we have implemented additional controls, such as stricter access restrictions and increased monitoring in response.

Data privacy (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

Disclosure

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 Board 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 [TC-TL-220a.4].

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](https://www.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.

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 customer 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 (continued)

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 disclose 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.

Country-by-country disclosure

We publish information regarding Law Enforcement Assistance on our website:



vodafone.com/handling-law-enforcement-demands

It is important to emphasise that attempts to compare one country's metrics with those of another are essentially meaningless given there are no consistent points of common reference and there are very wide variations between legal frameworks, record keeping requirements, and reporting regimes. Similarly, it can be difficult to draw accurate conclusions from year-on-year changes in reported metrics within a country, as these can be influenced by a range of factors. These could include amendments to legislation or new laws; developments in agency or authority or accepted industry practices; or changes to the approaches used to log, aggregate and disclose lawful demands.


We have robust processes in place to manage and track each demand and the information collated and published on our website (wherever available and wherever publication is not prohibited) has been overseen by the relevant Disclosure Officer in each market.

Governance

The overall law enforcement assistance programme is overseen by the Group External Affairs Director, a member of the Group Executive Committee.

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

Data security

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)	 2022 Annual Report, Cyber security (pages 49-51)

Disclosure

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 based on a risk assessment considering customers, law enforcement, relevant authorities and our external auditor. The European Union's 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 February 2022, Vodafone Portugal experienced a network outage that was caused by a deliberate cyber attack that was intended to cause disruption. No malware or malicious software was installed, and the attack method would be described as a 'living off the land' attack because it did not use any specialist tools. The attack relied on sophisticated social engineering, and a deep understanding of IT systems and networks. Investigations revealed that no customer data was accessed or compromised. No other Vodafone markets experienced any disruption from this incident.

The outage affected the data network in Portugal. The impact was loss of some voice and data services, some TV services and enterprise and business applications across the country, as well as international connections. Home broadband and linear TV were unaffected by the attack. On detecting the incident, we utilised our global incident management framework and immediately took action to identify, contain further risk and restore services quickly. Mobile data services and interconnections with other operators were resumed within eight hours of the attack, with other services being recovered during the next 48 hours. The Vodafone Portugal CEO immediately and proactively communicated with customers, and the team used widespread online, social media and press information and articles to keep customers aware of our recovery progress. Our cyber security team is continuing the investigation of this incident and working with local law enforcement and security agencies.

During the incident, 4.7 million mobile and one million fixed line customers were impacted, with some customers having both services. While the network outage was significant, it was only classified as a severe network incident for 48 hours. The direct costs of the incident are estimated in the range of €5 million and are financially immaterial in the context of Vodafone Portugal's operations and the wider Vodafone Group.

Data 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	 2022 Annual Report, Cyber security (pages 49-51) and Risk management (pages 59-67)

Disclosure

Our role is to enable connectivity in society. As a provider of critical national infrastructure and connectivity that is relied upon by millions of customers, we prioritise cyber and information security across everything we do. 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 understand 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 and policies to detect, prevent and respond to them. Our cyber security strategy 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 is based on an international standard and includes key security controls which significantly reduce cyber security risk, by preventing, detecting or responding to events and attacks. We have effectiveness targets for the key controls that are monitored and reported to senior management on a monthly basis. Each year, we review the framework in the light of changing threats and create new or enhanced controls to counter these threats. During FY22, we have introduced new controls to strengthen protection against phishing and ransomware, increased requirements for privileged access and authentication, and defined stronger security controls in our agile development lifecycle.

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 do more than just comply with local requirements or certifications; we actively contribute to consultations and debates on laws and regulations. We support level playing fields across regions and seek harmonised regulatory environments that provide strong security and societal benefits at a reasonable cost.

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	 2022 Annual Report, Planet (pages 41-44), 2022 ESG Addendum and EcoRating press release

Disclosure

Aside from carbon emissions, electronic waste is the largest material environmental issue for our business. We consistently seek to manage our own impact in a responsible manner and also support our customers with their efforts.

To begin the shift towards a circular economy of devices, we are taking a life-cycle management approach, which includes extending the lifespan of devices through repair, refurbishment and resale. We estimate that more than 50,000 tonnes of CO₂e could potentially be avoided for every million smartphones Vodafone receives via trade-in that are subsequently refurbished and resold.

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 FY22, we recovered 21 million devices through Consumer-focused product take-back schemes, equivalent to approximately 4,200 metric tonnes. Approximately 96% of these materials were reused or responsibly recycled and this is summarised in the table immediately below.

Product Take-Back Schemes

	Code	2022
Materials recovered through product take-back schemes (metric tonnes)	[TC-TL-440a.1(1)]	4,200
Reused products (%)	[TC-TL-440a.1(2)]	59%
Recycled products (%)	[TC-TL-440a.1(3)]	37%
Landfilled products (%)	[TC-TL-440a.1(4)]	4%

Additional information

Partnerships

In May 2021, we launched a new Eco Rating labelling scheme jointly with other major European operators. This is a pan-industry initiative to help consumers identify and compare the most sustainable mobile phones on the market, whilst also encouraging suppliers to reduce the environmental impact of devices. Eco Rating evaluates the environmental impact of the entire production process, transportation, use and disposal of a handset, resulting in an overall score. The Eco Rating scheme was initially launched in 24 European countries and has since been rolled out in several countries in Latin America and by Vodacom in South Africa. More than 150 mobile phones from 15 manufacturers are now assessed by the Eco Rating initiative, nearly doubling the range of devices rated at launch.


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

 ecoratingdevices.com

This year, we announced a new initiative to extend the life of new mobile phones and encourage customers to trade in or recycle their old devices, in partnership with Recommerce. Starting in European markets from Spring 2022, our customers will be able to access a comprehensive and convenient suite of services, including insurance, support and repairs for their device. We will also launch a new digital platform enabling customers to agree trade-in options for their existing phones. As well as encouraging customers to return their phones, we will begin to offer a wider range of high-quality, competitively priced refurbished smartphones at retail.

We are part of the Circular Electronics Partnership to drive industry action on circularity, bringing together leaders across the value chain from manufacturing, reverse logistics, material recovery, to e-waste management. This year the partnership has extended to 22 members, working to scale solutions across industries.

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)	 2022 Annual Report, Responsible business (page 47-58)

Disclosure

Vodafone has zero tolerance for activities that breach laws concerning competitive behaviour. 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 fines imposed by competition authorities against Vodafone in FY22 [TC-TL-520a.1]. This followed FY21, where there were no cases where Vodafone was found to have been involved in anti-competitive conduct.

During FY22, Vodafone was also successful in several appeals. This included the appeal against the Italian Competition Authority (ICA) infringement decision and fine against Vodafone Italy with respect to the billing cycles case, and the appeal against the ICA bulk SMS infringement decision and fine against Vodafone Italy. Both cases have been appealed by the ICA to the Italian Council of State.

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. Whilst there were no fines imposed by competition authorities against Vodafone in FY22, one new investigation relating to alleged incidents of anti-competitive behaviour was instigated by the competition regulator in Turkey during the year.

In April 2021, the Turkish Competition Authority (TCA) announced the launch of an investigation into a number of companies operating across a range of industries, including e-commerce and digital services. The TCA alleges that the companies had entered into informal arrangements not to hire each other's employees, ultimately suppressing pay and labour standards in Turkey. The number of companies under investigation almost doubled during 2021, and in December 2021, Vodafone was informed that it was also officially part of the TCA's investigation. Vodafone Turkey is vigorously defending itself and submitted a written defence and evidence in support of its case to the TCA in January 2022. In April 2022, the TCA issued its Statement of Objections in this case accusing 16 companies of anticompetitive conduct, including Vodafone Turkey. The investigation is ongoing.

During FY22, there were also a number of developments with regard to competition law matters (investigations and/or litigation) that had originated in previous years.

Romania

During the year, the Romanian courts reduced a fine originally imposed against Vodafone Romania by the Romanian Competition Council in 2011 with respect to the 'Netmaster' case from approximately €28.4 million to €22.8 million. Whilst Vodafone Romania was found guilty of refusing to terminate calls from Netmaster (another Romanian telecommunication services provider) to its network, the fine was reduced following the mitigating circumstance that the tariffs for interconnection of international traffic were not regulated by the Romanian telecoms regulator at the time. Following the original fine in 2011, Vodafone has taken steps to strengthen its competition law compliance programme with the aim of minimising the risk of anti-competitive behaviour. Examples included: enhancing the training programme for high-risk staff to also cover abuse of dominance and ensuring there is a close working relationship between the Legal team and staff of business areas exposed to competition risk.

Competitive behaviour (continued)

Additional Information (continued)

Portugal

Online search advertising (Google Adwords): In July 2020, the Portuguese Competition Authority ('PCA') issued a Statement of Objections to Vodafone and other Portuguese telecommunications operators. The PCA alleged that the operators had entered into an anti-competitive agreement to limit competition in advertising on the Google search engine which, in turn, restricted competition in various retail telecommunications markets. Vodafone Portugal is vigorously defending itself and submitted a written defence and evidence in support of its case to the PCA in October 2020. The investigation is ongoing.

Pay TV advertising (TV adverts): In August 2020, the PCA initiated an investigation on the basis of news in the media regarding the joint commercialisation and implementation of a 30-second advertising spot before Pay TV content by Pay TV operators MEO, NOS, Vodafone Portugal and Accenture. Prior to launching the service, the parties had joint meetings with the PCA to present the project and to address possible competition issues. In December 2021, the PCA issued a Statement of Objections accusing the Pay TV operators of anticompetitive conduct. Vodafone Portugal is vigorously defending itself and submitted a written defence and evidence in support of its case to the PCA in March 2022. The investigation is ongoing.

UK

Phones 4U litigation: In December 2018, the administrators of former UK indirect seller, Phones 4U, sued the three main UK mobile network operators ('MNOs'), including Vodafone UK, and their parent companies. The administrators allege a conspiracy between the MNOs to pull their business from Phones 4U thereby causing its collapse. The first trial on liability is scheduled to start in May 2022. Vodafone is vigorously defending the claim. Further information about this case is provided in the Group's Annual Report for the financial year ended 31 March 2022 on page 203.

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	

Disclosure

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 [TC-TL-520a.2]

Region	Average sustained download speed Mbps	
	5G-preferred mode	4G-preferred mode
Europe	125Mbps (FY21: 101Mbps)	45Mbps (FY21: 44Mbps)
Africa	65Mbps (FY21: n/a)	40Mbps (FY21: 39Mbps)

Fixed networks – Europe [TC-TL-520a.2]

Access Technology	Typical speed tier/ proposition range	Average sustained download speed Mbps
FTTH / Hybrid Fibre Coaxial	100 – 1,000 Mbps	309Mbps (FY21: 285Mbps)
xDSL	38 – 100 Mbps	61Mbps (FY21: 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, Romania and Hungary 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	
<p>Disclosure</p> <p>The principle of net neutrality centres on safeguarding the rights of the end-user on the internet, with end-user in this context meaning both the providers making content available over the internet, and those accessing it. Under the concept of net neutrality, internet service providers should not unjustifiably discriminate against or prioritise certain traffic, and should ensure internet access remains 'open' to end-users, hence it also being known as the open internet principle. Vodafone agrees with and supports these principles.</p> <p>The way in which these principles are applied in practice differs across the markets in which we operate owing to the differing legal requirements, and may be impacted by a number of factors. The application and interpretation of these rules is also subject to change over time. An example in the different approaches can be seen in relation to the concept of zero-rating (described in more detail below).</p> <p>Vodafone always ensures that our services and commercial practices comply with the core principles of net neutrality, and in compliance with the prevailing rules and guidance in the markets in which we operate.</p> <p>At the same time, we are committed to expanding and future-proofing our network infrastructure and developing and supporting innovative services for the benefit of all our customers. The pandemic underscored the importance society places on fast, low latency, reliable and secure connectivity and the services delivered over this, and how this can help overcome the deep digital divides – between people, businesses, and communities – that the pandemic has shone a light on. The development of such a supportive digital ecosystem requires both public and private investment in digital, along with policy reforms that are pro-investment, pro-innovation and supportive of returns.</p> <p>Vodafone is concerned that the fragmented approach to net neutrality globally, and the evolutionary way in which it is applied, does give rise to a degree of regulatory uncertainty, which can in turn act as a brake on the innovation needed. We will therefore continue to work with policy makers and regulators to ensure that the policy environment remains supportive of network deployment, investment and digital connectivity and services whilst at the same time preserving the essence of net neutrality principles.</p>			
<p>Additional Information</p> <p>Zero-Rating</p> <p>The practice of zero-rating is where an internet service provider does not 'charge' an end-user for access to specified content, applications or websites over the internet. In other words, where an end-user accesses zero-rated content, applications or websites, it does not count towards their data allowance.</p> <p>Given the benefits it can bring to end-users, Vodafone does zero-rate certain content and services, but only if the zero-rating complies with the prevailing guidance, regulations and laws in the country it is offered. Vodafone offers zero-rating in two common use cases:</p> <p>Zero-Rated Tariffs</p> <p>In some markets, where many consumers are increasingly choosing unlimited tariffs, the use of zero-rating is becoming less common. However, for those customers choosing tariffs with finite data allowances, zero-rating offers on specific categories of application or use-case can provide more certainty, as they can use the covered applications without worrying about their data allowance.</p> <p>Vodafone has therefore offered tariffs in the EU and UK that include zero-rating since 2015. These offers were always designed with the prevailing net neutrality rules and guidance in mind. For example, to ensure we adhered to the principles of transparency and openness, any partner that met defined objective and transparent criteria was able to have their content zero-rated as part of our offer. Additionally, to ensure we did not restrict the 'openness' of the internet, end-users were only able to access the zero-rated traffic to extent they had a remaining data allowance, meaning they were never in a position where they could only access the 'zero-rated' traffic (i.e. there was never a 'walled garden' internet experience).</p> <p>These offers were reviewed by multiple national regulatory authorities since their launch and, whilst certain adjustments were made over time to ensure compliance with the prevailing guidance, they were deemed compliant under the Net Neutrality framework in the EU.</p> <p>However, in September 2021, the Court of Justice of the European Union ('CJEU') issued three judgements that stated that any price-differentiation practice, including zero-rating, that was not application-agnostic was not considered compliant with the EU's Net Neutrality Regulation. Whilst the detail on how these judgements shall be applied in practice is still under review by the European Body of Regulators ('BEREC'), it is accepted that, in the EU, all operators, including Vodafone, will ultimately be required to phase out zero-rated commercial offers.</p> <p>The CJEU's judgements and any associated guidance issued by BEREC are not directly applicable in the UK. The UK regulator has indicated that Vodafone may continue to offer its zero-rating tariff in the UK on the basis that it was designed to comply with the key principles of net neutrality.</p>			

Competitive behaviour (continued)

Additional Information (continued)

Public Good Zero-Rating

Zero-rating can also be a means to support social good, for example by allowing unrestricted access to content and applications that subscribers rely on. In this sense, zero-rating can be used to enhance data democratisation.

For example, DreamLab is an application that has been developed by the Vodafone Foundation and Imperial College London and has been downloaded over 2 million times. The app helps support cancer and coronavirus research by using the processing power of smartphones to help analyse complex data while the device is charging but going unused (typically overnight). In recognition of the societal benefits that this sort of 'crowd-sourced' scientific research brings, this application was zero-rated by Vodafone.

In addition, Vodafone zero-rated a number of websites, applications and services for the public good during the COVID-19 pandemic – for example, in Ireland we zero-rated certain government-identified health and education resources, in Greece we zero-rated various education websites to facilitate the government's online-learning policy during the pandemic, and in the UK we zero-rated access to health resources. In the Czech Republic, a public good zero-rated pass was introduced, called "Pass for Good", which gave access to health resources, amongst other applications. In Turkey, we also zero-rated remote education and health applications and platforms, on request from public authorities.

In some of our markets, the practice of zero-rating such public good services is something that is even becoming mandatory, where the authorities have determined that the zero-rating of essential state and emergency sites provides social benefits. For example, in South Africa, Vodacom made an undertaking in 2020 to zero-rate specified content on certain Government websites, and is now consulting on new licence conditions that would oblige it to zero-rate mobile content provided by designated Public Benefit Organisations, including gov.za websites.

In light of the recent CJEU judgments on zero-rating, telecommunications operators are now waiting for further guidance on whether this will impact public good zero-rating within the EU. We are actively engaging with our stakeholders and regulators (including BEREC) to emphasise that zero-rating for social benefits is a positive practice.

Content Blocking

As noted above, one of the key principles of net neutrality is that internet service providers should not unjustifiably discriminate against certain traffic, which would include blocking content.

However, operators are permitted to block content under certain circumstances, for example where required under law. This has been of particular relevance to operators in relation to the recent orders issued by the European Union to block content associated with specified Russian media operators. It was confirmed by BEREC that action to block such websites would not be in conflict with the net neutrality principles, and Vodafone has therefore taken action to block the content of these media operators, subject to safeguards required by our internal policies to ensure legality and proportionality of the requirement.

Innovation under Net Neutrality

We are committed to ensuring an internet that is open to all, and where end-users control their experience on the internet.

At the same time, we are seeing substantial changes across the internet value chain, and there is now a significant diversity in terms of the networks, devices, content and types of user. As a result, we are increasingly seeing demand:

- From consumers for different tariff options and packages that best suit their needs;
- From business customers in relation to specific business services, which require guaranteed speeds and quality;
- From content providers, who require their content (such as metaverse or connected mobility applications) to be delivered with a guaranteed quality;
- From connected devices, which also rely on specific quality parameters.

This demand for differentiation will continue to increase, as end-users seek to make use of the opportunities presented by edge computing and 5G network slicing, which allow for differentiation within networks. Therefore, the ability to provide such differentiated services and commercial propositions will encourage operators to invest in their networks and offer innovative services to businesses and customers, which will in turn help bridge the digital divide.

Vodafone strives to ensure that new and existing services and propositions that take advantage of the latest technologies comply with the prevailing rules and guidance on net neutrality. However, whilst existing guidance for example from BEREC, has indicated that use cases based on 5G and edge computing can comply with the net neutrality regulation, there remains a degree of uncertainty, as the regulations were designed before these technologies were in active use. We continue to work with regulators and policymakers to ensure a clear, unambiguous and innovation and investment-friendly interpretation and application of net neutrality principles is applied across our markets.

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)	
<p>Disclosure</p> <p>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. Severity is based on the number of customers affected and whether the number is significant in the context of the overall size of the particular market.</p> <p>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. Severity is based on the number of customers affected and whether the number is significant in the context of the overall size of the particular market.</p> <p>The figures presented below reflect 40 (FY21: 72¹) high-impact and critical incidents identified and resolved during FY22, representing a 44% year-on-year reduction. Vodafone drives a culture of continuous improvement and seeks to identify lessons learned from all service interruptions reported. In fact, March 2022 was our most stable month reported in Europe with no major incidents across mobile and fixed line networks.</p> <p>In FY22 the scope of markets included in our analysis were increased with the addition of Greece, as well as the assets acquired in Germany and Central and Eastern Europe in FY20. To ensure a like-for-like basis of comparison with the prior year, FY21 values have been restated using the same scope as reported in FY22. Further details on the markets within scope is included in the 'Additional Information' section.</p> <p>1. System average interruption frequency [TC-TL-550a.1(1)]</p> <ul style="list-style-type: none"> – Mobile: 0.07 interruptions per customer (FY21: 0.171). In other words, 7% of our in-scope mobile customer base experienced a disruption that was classified as high-impact and critical at some point during the year. – Fixed: 0.07 interruptions per customer (FY21: 0.171). In other words, 7% of our in-scope fixed customer base experienced a disruption that was classified as high-impact and critical at some point during the year. <p>The statistics set out above do not provide any information with respect to the typical duration of each disruption or whether the same customer experienced a disruption more than once during the period.</p> <p>2. Customer average interruption duration [TC-TL-550a.1(2)]</p> <p>The SASB Standards define this metric as the aggregated downtime divided by the total number of customers affected by the interruptions. Given interruptions typically only last for a short period (minutes and hours) and we have such a large customer base, this metric is not meaningful and would be measured in milliseconds.</p> <p>We have therefore calculated an alternative and more meaningful metric based on a weighted average of the disruption time and number of affected customers for each major incident.</p> <ul style="list-style-type: none"> – Mobile: Average disruption duration for affected customers of 5 hours and 43 minutes (FY21: 4 hours and 1 minute¹), representing a 43% year-on-year increase as a direct result of the Portugal cyber-attack in February 2022. By excluding this incident, the average disruption for affected customers reduces to 1 hour 34 minutes, representing a 61% year-on-year improvement. – Fixed: Average disruption duration for affected customers of 5 hours and 8 minutes (FY21: 6 hours and 52 minutes¹), representing a 25% year-on-year reduction. <p>The metric set out above reflects the average disruption duration for affected customers and, as noted in the first part of this question, only part of our customer base experiences disruption in any given year. By multiplying the previous metrics by the percentage of our base that experienced a disruption during the year, we can estimate the average disruption duration for all of our in-scope customers.</p> <ul style="list-style-type: none"> – Mobile: Average disruption duration for entire customer base of 23 minutes throughout the year (FY21: 40 minutes¹), representing a 43% year-on-year reduction. – Fixed: Average disruption duration for entire customer base of 21 minutes throughout the year (FY21: 11 minutes¹), representing a 70% year-on-year reduction. <p>1. To ensure a like-for-like basis of comparison with the prior year, FY21 values have been restated using the same scope as reported in FY22. Further details on the markets within scope is included in the 'Additional Information' section.</p>			

Technology resilience (continued)

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, Albania and Greece.

The number of customer interruptions was calculated by aggregating the number of customers impacted by an interruption to one or more service (Mobile: Voice [2G], Data [3G, 4G] or Fixed: Data and Voice) and for the 40 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

The Standards suggest that the average interruption duration should be calculated by aggregating the total downtime (in hours) and dividing this by the number of customer accounts affected during the period.

As explained above, we do not consider this metric to be meaningful and we have therefore calculated and presented two alternative metrics which we believe provide a more meaningful view of typical disruption duration for affected customers and our entire customer base.

1. Weighted average disruption duration for affected customers; and
2. Weighted average disruption duration for entire customer base.

Disruption in Vodafone Portugal (February 2022)

In February 2022, Vodafone Portugal experienced a network outage that was caused by a deliberate cyber attack that was intended to cause disruption. No malware or malicious software was installed, and the attack method would be described as a 'living off the land' attack because it did not use any specialist tools. The attack relied on sophisticated social engineering, and a deep understanding of IT systems and networks. Investigations revealed that no customer data was accessed or compromised. No other Vodafone markets experienced any disruption from this incident.

More information on this incident can be found in our FY22 Annual Report (page 51) or in the data security disclosures above.

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	 2022 Annual Report, Risk management (pages 59-67)

Disclosure

We define technology failure as network, IT 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 FY22 TCFD Report, we identify a number of 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 and an increase in the likelihood or frequency of technology failure. 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 treatment 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 Business Continuity program and related polices are aligned with the ISO 22301 international standard. In addition, seven markets and our shared services entities also hold equivalent local certifications. We also partner with the Business Continuity Institute ('BCI'), ensuring that our Business Continuity professionals are aware of BCI's Good Practice Guidelines and have access to specific training available through our global learning platform.

Our data centres 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 technology failure occur, we are able to automatically transition to another datacentre to maintain service availability for our customers. We have a continuous process to learn from events such as the Portugal incident described above and to apply necessary improvements across our footprint.


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, data centres, 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)	 2022 ESG Addendum, Headcount tab

Disclosure

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 48 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, 9% 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: Global headcount	TC-SI-330a.2	Employee engagement as a percentage	 2022 Annual Report, People strategy (pages 21-23) and employee experience (page 38)

Disclosure

Our employee engagement index¹ was 73 out of a maximum score of 100 in 2022 **[TC-TL-550a.1(1)]** (FY21: 74). The overall response rate was 80% (FY21: 86%).


Additional Information

Our culture – the 'Spirit of Vodafone' – outlines the beliefs we stand for and the behaviours that enable our strategy and purpose. In May 2020, we introduced a bi-annual employee survey called 'Spirit Beat' to measure culture and its impact. The results demonstrate how Spirit behaviours are being embedded in the employee experience and confirm the positive impact of these behaviours in driving performance.

Following each survey, employees receive personalised and artificial intelligence-driven 'nudges' based on their confidential responses over a 20-week period. These nudges support behaviour change, consolidate new habits, and create a continuous feedback loop, with over two million nudges deployed since May 2020. Based on responses from the latest survey, 68% of colleagues found nudges useful, and analysis has shown that teams with managers who embraced Spirit and took action had a higher Spirit Index (+8) and engagement score (+9) compared to managers who did not.

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.

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)	 2022 Annual Report, Workplace equality (pages 38-39) and Fair pay at Vodafone (page 106)

Disclosure

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

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

Gender Diversity (FY22)	Female	Male
Board	50%	50%
Executive Committee	29%	71%
Senior leadership roles (FY22: 191)	31%	69%
Management and senior leadership roles (FY22: 6,727)	32%	68%
External hires	42%	58%
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 introduced a number of policies and programmes to ensure we are creating an inclusive culture. 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 returner 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.

All of these initiatives aim to support the retention of women in our business as well as enable progression into more senior roles. We also continually support all our leaders to recognise unconscious bias in decision making and build inclusion as a core part of leadership development.

To better understand representation across the organisation and inform our diversity and inclusion programmes, in November 2020 we launched the ‘#CountMeIn’ initiative 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. On this basis we were able to set ethnic diversity targets, which are summarised below.

- **Group:** By 2030, 25% of our global senior leadership team (encompassing 163 of our most senior leaders in Europe & Africa) will come from ethnically diverse backgrounds. This compares to 18% in March 2022.
- **UK:** By 2025, 20% of UK-based senior leadership and management will come from Black, Asian, or other diverse ethnicities, with 4% to be Black. This compares to 15% and 1% respectively in March 2022.
- **South Africa:** By 2030, 75% of South African-based senior leadership and management will come from ethnically diverse backgrounds. This compares to 64% in March 2022.

In addition to the above, 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/ar2022

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.

References to Vodafone are to Vodafone Group Plc and references to Vodafone Group are to Vodafone Group Plc and its subsidiaries unless otherwise stated. Vodafone, the Vodafone Speech Mark Devices, Vodacom and The future is exciting. Ready? are trade marks owned by Vodafone. Other product and company names mentioned herein may be the trade marks of their respective owners.

© Vodafone Group 2023

Designed and produced by Black Sun plc