Privacy and security – Our approach

The way we handle privacy and security is a vital part of our responsibility to our customers and essential to the success of our business.

Privacy and security are often viewed by organisations merely as compliance or risk management responsibilities, but we see significant opportunities for Vodafone to differentiate what we offer and strengthen our reputation through our efforts in these areas.

Our customers trust us with their personal information and their privacy. Protecting that information and respecting their privacy is fundamental to maintaining that trust. Our privacy and security programmes govern how we collect, use and manage customers' information – from ensuring the confidentiality of their personal communications and respecting their permissions and preferences, to protecting and securing their information.

Personal data also has enormous potential to create economic and social value, both for the individuals concerned and for the businesses who serve them. In order to ensure this opportunity is executed well, we are using technology to make it easier and more intuitive for customers to take control of how their data is used.

Understanding customers' concerns about how communications technology can impact privacy and security

We understand that customers may be concerned about the privacy and security of their personal information as they use communications technology more often and for different purposes. We help customers manage a wide range of privacy and security risks that may impact them when using mobile and other devices.

The confidentiality of customers' personal and private communications is a fundamentally important requirement for any communications company as the company will manage a great deal of sensitive information including customers' personal communications, their location and how they use the internet. The complexity of technology, threats from hackers and the potential for human error can lead to information being lost or deleted or getting into the wrong hands.

Law Enforcement Disclosure report

The issue of government surveillance has come under increased scrutiny. For the first time, we have published a Law Enforcement Disclosure report which details Vodafone's approach to responding to government demands for access to customer information, along with a breakdown of the legal powers governments hold. We also publish statistics on the number of law enforcement demands we received on a country-by-country basis, where it is legal to do so and the government does not already publish such information.

Vodafone is one of the first communications operators in the world to provide this kind of country-by-country analysis of law enforcement demands, based on data gathered from our local licensed communications operators. We have committed to update the information disclosed in this report annually. We expect the contents and focus of the report to evolve over time and we will be working with key stakeholders on the best way to do this.

The report is intended to:

- explain the principles, policies and processes we follow when responding to demands from agencies and authorities that we are required to assist with their law enforcement and intelligence-gathering activities
- explain the nature of some of the most important legal powers invoked by agencies and authorities in our countries of operation
- disclose the aggregate number of demands we received over the last year in each of our countries of operation unless prohibited from doing so or unless a government or other public body already discloses such information
- cite the relevant legislation which prevents us from publishing this information in certain countries.

Read our Law Enforcement Disclosure report on page 58.

Privacy and security – Our approach

As more services use mobile and communications related data for an ever-expanding range of uses, customers need to be able to understand and be able to control how information about them is used. Smartphones, tablets, e-readers, apps and new technologies using the 'internet of things' (such as connected cars, smart grids and mHealth) offer many economic and social benefits, but also raise some complex privacy issues. For example, mHealth services may enable physicians to monitor patients round the clock by having remote access to their health devices and data, but by doing so sensitive health data may need to be transmitted across communications networks, hosted in the cloud, and processed by a range of applications used by medical staff.

Governments also have legal powers to demand access to customer communications and data. See our new Law Enforcement Disclosure report on page 58 for more information.

Creating the right culture

Everyone at Vodafone must have a clear understanding of how important protecting and respecting our customers' information is to our business. We continue to create a strong internal culture where our employees understand the critical nature of privacy and security risks and know how to manage them. This focus helps us to retain the trust of our customers and the respect of our colleagues, stakeholders and peers.

We have set out our commitment to privacy and security at the highest level in our global Code of Conduct, which all Vodafone employees are bound by. Our Privacy Commitments, which are part of our Code of Conduct, set out the principles that govern our approach to privacy (see feature below).

These Privacy Commitments encapsulate three key elements of building customer trust:

- Transparency: Being more open about what we do (Commitment 2: Openness and Honesty)
- Empowerment: Using our technology to empower our customers and give them control over their personal information (Commitment 3: Choice)
- Reassurance: Making sure that we do what we promise to and that we are doing what's right (Commitment 7: Accountability).

We can only ensure our customers' privacy if we first ensure the security of their information and communications. Information security is an essential part of our business. Our Key Principles on Information Security (see feature below) set out how we securely create, use, store or dispose of all information we manage, so that it cannot be lost, stolen or manipulated, or used without Vodafone's authorisation. We expect our employees to know how to protect customer information and to challenge others who fail to do so. Our global awareness and transformation strategy, Protect and Secure, is further deepening our security culture at Vodafone, raising employee awareness of security risks and what they can do to mitigate them.

In focus: Privacy Commitments

1. **Respect:** We value privacy because of its value to people. It's about more than legal compliance – it's about building a culture that respects privacy and justifies the trust placed in us.
2. **Openness and honesty:** We communicate clearly about actions we take that may impact privacy, we ensure our actions reflect our words, and we are open to feedback about our actions.
3. **Choice:** We give people the ability to make simple and meaningful choices about their privacy.
4. **Privacy-by-design:** Respect for privacy is a key component in the design, development and delivery of our products and services.
5. **Balance:** When we are required to balance the right to privacy against other obligations necessary to a free and secure society, we work to minimise privacy impacts.
6. **Laws and standards:** We comply with privacy laws, and we will work with governments, regulators, policy makers and opinion formers for better and more meaningful privacy laws and standards.
7. **Accountability:** We are accountable for living up to these principles throughout our corporate family, including when working with our partners and suppliers.

In focus: Key Principles on Information Security

Customer information is one of the greatest assets we are entrusted with and must be protected appropriately. We handle vast amounts of customer information in a variety of forms – written, spoken, electronic and on paper – on a daily basis. It is vital that we secure and manage this information and can ensure its:

- **Confidentiality:** Customer information must not be disclosed to, or accessed by, unauthorised people
- **Integrity:** Customer information and software must be accurate, complete and authentic so that it can be relied upon
- **Availability:** Customer information must be available when needed – including to our customers – and information systems and networks must function when required.

Privacy and security – Our approach

Recognising opportunities, not just obligations

Not managing the privacy and security of our customer's data appropriately can pose risks to our customers and our business. However, we also see the potential to differentiate our brand by managing these risks well and by offering products and services designed to support customers in improving control over their data.

These include free apps such as Vodafone Protect that keep consumers safer online by enabling them to lock and wipe their mobile remotely if it is lost or stolen, and Vodafone Guardian that helps parents keep children safer when using their mobile phones. We also support our enterprise customers with products such as Vodafone Device Manager and Profile Manager, which enable employees to have separate work and personal areas on a single device, and our innovative Vodafone Locate tracking service which has privacy controls inbuilt.

We are developing tools that will enable our customers to set permissions and preferences for all their devices, apps and interactions with Vodafone in a single tool, to make it easier for them to see and control their settings.

Understanding and responding to risks

Risk management is at the heart of Vodafone's approach to privacy and security. Identifying emerging issues and risks – as well as opportunities (see Performance) – is essential to help us understand and manage those risks. We do this by examining the implications of our business strategy, new technologies and business models, areas of concern for customers and industry developments within our own and related markets.

Many of the latest developments in the ICT sector raise privacy and security issues, concerns and opportunities. These include 'big data' analytics (see below), connected cars, smart cities, smart metering (see Low carbon solutions), mHealth, Mobile payments and Smart working.

We conduct regular formal reviews of the most significant privacy and security risks affecting our business at Group level. Based on these reviews, we develop strategies to respond to the most critical risks (see below), which may include developing new internal policies, investing in new capabilities, technologies and programmes, or influencing the positions of our industry peers and partners, through associations such as the GSMA.

To help shape our strategy on privacy and security and ensure robust responses to stakeholder concerns, we regularly engage with external stakeholders and draw on their expertise.

In focus: Vodafone Germany's Ombudswoman for Data Protection – Ms Renate Schmidt

Vodafone Germany's dedicated Data Ombudswoman acts as a trusted advisor to the business on the rights and interests of Vodafone Germany's customers regarding privacy and data protection. Former federal minister Renate Schmidt, appointed in 2008, brings a wealth of knowledge and experience to the role. Her guidance and insight is also sought more widely for input on the Vodafone global privacy programme and specific privacy initiatives.

Managing strategic risks

Based on our strategic risk review, some of the most critical privacy and security risks we face include:

Cloud services and hosting

As we deliver better services faster, expand our cloud-based services to enterprises and customers and reduce costs by avoiding duplication of infrastructure in different markets, we increasingly need to move data across international borders.

We must ensure that the movement of customer data across borders is conducted lawfully, legitimately and securely, both within our own organisation and between Vodafone and its suppliers.

We operate a global information governance system that enables us to track the flow of customer data and ensure we apply appropriate governance and legal processes. We have robust, standardised security processes within our own operations (see below) and employ specialist teams to evaluate the governance and controls of our suppliers.

As cloud-based solutions become increasingly widespread, we must continue to optimise the benefits of this technology, while effectively managing the risks. We are developing new tools to ensure the systematic management of all cloud capabilities and conformance to security and data management requirements.

Traffic management

To deliver the quality of service customers expect, we need to manage the flow of communications traffic across our network. For example, we may need to prioritise an uninterrupted video call over an email (which is not so time critical). To do this, we need to examine some of the information, or data packets, attached to the communication, in order to know what type of communication it is, although the actual 'content' of a communication (such as the text in a text message) is not inspected. This type of technique is sometimes referred to as deep packet inspection.

Privacy and security – Our approach

Knowing more about these data packets – and thus about the nature of our customers' communications – naturally raises privacy concerns. We have clear, specified governance and policy requirements around the use and deployment of these types of techniques. Other than for the lawful purpose of managing traffic across our networks, our policy prohibits any application of network technologies involving the inspection of data packets until they have been subjected to an in-depth privacy impact assessment. As well as ensuring any use of deep packet inspection complies with the law, this assessment evaluates the potential impact on the customer and enables us to identify and develop solutions to avoid or minimise any impacts. Any use of these technologies must be authorised by a senior executive at Group level.

Advertising, analytics and 'big data'

The vast amount of data generated by our customers on mobile devices, services and networks has enormous potential value for mobile commerce, as well as for programmes with societal benefits, such as analysing trends in public health. The expansion of mobile connectivity into new fields, such as connected cars, smart metering and mHealth, means ever greater volumes of data are being generated. Even when this information is anonymised and aggregated, concerns arise about how the value of such 'big data' can be unlocked while protecting individual privacy.

Our internal policies, guidelines and design principles for applications and services that make use of personal data help us to ensure that we provide customers with transparent information and clear choices about how their data is used. We also research consumer perceptions and concerns to inform our strategy and explore and develop techniques that can enhance privacy (see our Performance section).

Law enforcement assistance and human rights

In every country where Vodafone operates, governments retain law enforcement powers that can limit privacy and freedom of expression. These include legal powers that require telecommunications operators to provide information about customers or users or to put in place the technical means to enable information to be obtained for law enforcement purposes, such as lawful interception. Governments also retain powers to limit network access, block access to certain sites and resources or even switch off entire networks or services.

These powers have many legitimate purposes, including fighting crime and terrorism, and protecting public safety. However, use of these powers must be balanced with the respect for civil liberties and freedoms, including individuals' privacy and freedom of expression. We closely manage and monitor compliance with these legal obligations and our relationship with law enforcement authorities to ensure human rights are respected. We also engage with governments to seek to ensure that legal provisions governing use of these powers contain adequate protection for human rights.

In focus: Privacy-by-design

We are committed to building privacy considerations into our products and services from the outset, and using our influence to shape the technologies of our partners and peers.

Our series of privacy design principles guide product development teams in shaping and designing products. For instance, our Visible Privacy Design Principles provide a framework to make sure we give users control over how they manage their privacy and how their data is collected, used and shared.

We provide privacy resources and guidance to third party developers, which are published on our Developer portal. We also work with industry organisations and application developers to create guidelines and policies, such as the GSMA's Mobile Application Privacy Guidelines, to ensure our partners and suppliers build privacy into the products and services they design.

Vodafone's Global Policy Standard on Law Enforcement Assistance sets out our principles and standards on assisting law enforcement, including processes to ensure our actions are accountable at the most senior level.

We are a founding member of the Telecommunications Industry Dialogue on Freedom of Expression and Privacy, a group of global telecoms companies working together and in collaboration with the Global Network Initiative to address issues of privacy and freedom of expression. We are a signatory to the Industry Dialogue's Guiding Principles on Freedom of Expression and Privacy, which define a common approach to dealing with demands from governments that may affect privacy and freedom of expression in a principled, coherent and systematic way across the industry.

Our Law Enforcement Disclosure report details our approach to responding to law enforcement demands for access to customer information, along with a breakdown of the legal powers governments hold. We also publish statistics on the number of law enforcement demands we received on a country-by-country basis, where it is legal to do so and the government does not already publish such information.

Managing operational risks

Our network of privacy officers across the Group use our comprehensive Privacy Risk Management System (see box below) to help us live up to our Privacy Commitments in our day-to-day operations, while ensuring that we are prepared to respond to new privacy and security concerns and risks as they emerge. This system provides the flexibility to respond to local privacy concerns, legal requirements or stakeholder expectations, while providing a common framework to build and measure the maturity of our programme and implement improvements across all key areas of our business operations.

Privacy and security – Our approach

Our privacy programme is underpinned by extensive information and network security practices and technologies designed to secure the infrastructure and systems on which our business' and our customers' privacy is based. These include:

- Advanced security monitoring systems to detect and respond to cyber security issues in real time (see feature below)
- Physical controls including appropriate vetting of people to manage against misuse of access or privileges by our own staff, contractors or third parties
- Significant investment in security technologies.

The robust information security policies, processes and procedures supporting these controls are regularly audited and tested.

Our approach is based on the principles outlined in ISO 27001, the international standard for information security management systems. Our core data centres in Germany, India, Ireland and Italy are certified to this standard. We require our external suppliers and partners to meet defined minimum security standards and we conduct risk assessments and due diligence exercises to provide assurance that these are being met in practice.

In focus: Taking action on global cyber security

Cyber security threats pose a significant risk to our business, infrastructure and customers' information. Remaining vigilant in anticipating attacks, defending against them and planning for the future, are essential elements of our strategic risk management. The threats are posed by a range of agents, from nation states and commercial competitors through to 'hacktivists', cyber criminals and terrorists.

Risk management is at the centre of our approach. We analyse and review the most significant security risks affecting the business at Group level and based on this we develop strategies to respond to the most critical risks and determine future investment.

Vodafone's Global Security Operations Centre (GSOC) is designed to detect attacks as they happen and minimise their impact. This centralised security centre monitors our IT systems 24 hours a day, seven days a week, to enable us to respond to cyber threats in real time and provide the highest level of protection. We identify and deal with tens of millions of IT security attacks every month, to protect the information of over 400 million customers and ensure the best network performance.

We recognise that some attacks may be successful and may result in data being compromised. The management of these incidents when they happen is as critical as their prevention. As a result we piloted a new customer privacy impact service this year to ensure that we always put the customer first when incidents occur.

In focus: Vodafone Privacy Risk Management System

- **Supplier review:** Process to review suppliers, such as outsourced call centres and companies that provide hosting platforms and customer data and ensure measures are in place to protect privacy
- **Product and service review:** Processes for taking privacy into account when developing products and services (such as privacy-by-design in mobile applications)
- **Incident management:** Process for managing incidents, such as data security incidents and losses of data
- **Disclosure:** Processes for governing all disclosures of personal information, such as in response to legally mandated government requests and assisting law enforcement authorities
- **Data management and retention:** Processes for managing the lifecycle of data, including destruction and retention of data
- **Privacy impact assessment:** Processes for identifying, prioritising and conducting privacy impact assessments, such as for specific business units, technologies or products
- **Personal information location register:** A register of personal information assets, enabling the effective management of all personal information
- **Critical privacy risk management:** Processes for ensuring that strategies and policies developed to address critical privacy risks are effectively implemented
- **Review and reporting:** Processes to ensure that all the above are reviewed and reported to executive management, with identified improvements included in business plans.

Operational risk management is as much about prevention as it is about detection and treatment. We continue to run a series of coordinated global awareness and engagement programmes designed to ensure our staff understand the vital importance of privacy to our customers, including the role that individual employees have in protecting the security of customers' information.

Our Group Privacy and Security Governance Forum ensures coordination and alignment between our Group-level privacy and security functions, to provide end-to-end protection of customer information throughout its lifecycle within Vodafone's business.

Privacy and security – Performance in 2013/14

Ensuring privacy and security and putting customers in control of their information is critical. Gaining our customers' trust is essential to unlock the potential benefits of using customer data to help grow our business in areas such as mobile commerce and analytics.

At the same time, our continued investment in security measures is becoming more critical as the threat of targeted cyber attacks to businesses and their customers' information increases, as have social engineering attacks as a result of wider use of social media.

Government access to individuals' private communications has come under increased scrutiny. Our policy on law enforcement assistance has been in place since 2010 and we published our Law Enforcement Disclosure report to increase transparency and improve understanding on this issue.

Putting customers in control

Research tells us customers are increasingly concerned that their information is being misused or sold to third parties. The most strongly stated concern is a lack of control and transparency[1]. In 2013/14, we continued our programme of research to improve our understanding of what our customers expect from us in relation to privacy and how we can meet their expectations. We surveyed over 6,500 consumers, 1,500 opinion formers and 150 stakeholders, such as politicians and regulators, across Europe, Africa and Asia to understand their views, attitudes and expectations.

Our research revealed that stakeholders believe companies are abusing their position by taking advantage of consumer ignorance and apathy and that many existing initiatives are seen by stakeholders as companies putting their own interests ahead of consumers. However, consumers conveyed a sense that as the scale of information use changes, they will increasingly trust and use companies that are willing to offer them greater control through tools that are easy to use.

In the UK, a survey of over 1,600 consumers on their attitudes to receiving targeted offers and their views on apps and services that use their data found that customers are comfortable with internet companies, social media and some smartphone apps using their information to target personalised offers and adverts, but are concerned that companies are using their data for more than was initially agreed. While they see value in location services, or services which take into account their gender and age, they dislike sharing information about calling patterns and are more likely to share data in exchange for services which they perceive as valuable.

Our research feeds into our business strategy and is particularly important in shaping our efforts to provide customers with effective tools to manage their personal data. In 2013/14, we developed new tools and capabilities to empower our customers to take more control over their personal information and provide greater transparency. We ran focus groups across five European markets to help us refine these tools to better meet the needs of our customers, and they will be rolled out during 2014/15.

The tools will enable our customers to set their permissions and indicate their preferences across all touch points, including smartphone apps, tablets, online and in store. Bringing all the different choices and information together into a single tool will improve customers' experiences by increasing visibility about how their information is used and shared and putting them in control. It will also help us prepare for the European reform of data protection law by building our technical capability to comply with the anticipated new regulation regarding the way permission to use information is sought from customers.

In addition, we have been investigating how to build privacy management capabilities into our machine-to-machine (M2M) platform and embed privacy features into the next generation of M2M technology (also known as the 'internet of things'). This is forming the foundation of many of the most important developments in our industry, including smart metering, connected cars and wearable technology.

Recognising opportunities, not just obligations

Privacy and security can pose risks to our customers and our business, but we also see potential to differentiate our brand not just by managing these risks but by offering products and services designed to support customers in improving their privacy and security.

In 2013/14, we launched and expanded a number of products that demonstrate the potential of privacy and security as a business opportunity:

- **Secure Call:** Vodafone has developed a high-level security app, in partnership with Secusmart, called Secure Call, which uses government-level encryption to help companies of all sizes protect the confidentiality and privacy of their voice calls
- **Secure SIM Data:** Vodafone is the first telecommunications company to introduce a SIM card-based, end-to-end encryption solution for the mobile workplace. Developed in collaboration with Giesecke & Devrient, a leading provider of SIM cards and mobile security solutions, Secure SIM Data encrypts and signs e-mails, documents, data media and VPN connections, offering companies and other organisations enhanced security in their mobile data communications

Privacy and security – Performance in 2013/14

- **Secure Family:** Vodafone has introduced a new service which helps parents manage their children's access to the internet by, for example, blocking access to certain websites, allocating 'quiet times' when children cannot access the internet at all and alerting parents when children download new apps. This product was carefully designed to prevent it being misused to covertly monitor the online activities of another person. It has launched in Italy and will be introduced in other markets during 2014.

We also continued to explore the economic potential of the vast amount of data that flows across our networks. In March 2014, we publicly outlined the key actions that support Vodafone's overall strategy on big data and analytics at the Cebit industry trade conference. Our privacy and permissions programme (outlined above) is central to this strategy. We believe that putting our customers in control of their personal data is not only essential to ensuring that Vodafone is trusted by our customers, but that we are trusted and respected by potential partners in big data and analytics.

Strengthening our programmes

In 2013/14, we introduced a series of new metrics to measure the maturity of our privacy approach across the Group, extending beyond compliance controls in our Privacy Risk Management Framework (see Our approach section) to include employee engagement activities, new research carried out and external engagement with stakeholders. We also introduced a new requirement for local markets to report any major events in 'real time' as part of our commitment to implement the Guiding Principles of the Telecommunications' Industry Dialogue on Freedom of Expression and Privacy (see below).

We continued to focus on developing the competence and professional skills of privacy professionals within the business. In 2013/14, we launched the Vodafone Privacy Learning Centre for our privacy community, and we sponsored 10 privacy officers from our local markets to become Certified Information Privacy Managers through the International Association of Privacy Professionals (IAPP), an internationally recognised qualification in privacy management.

In 2013/14 we focused on strengthening our programme in a number of key areas:

- **Law enforcement and privacy** – We carried out a global audit of compliance with our Law Enforcement Assistance Policy, which included detailed on-site reviews of operational management of law enforcement assistance and compliance with our policy standard, in certain markets. We also reviewed the powers governments have across our markets to order the disclosure of information about our customers, block access to services or prevent the publication of statistics on the number of orders we are subjected to. This review fed into our new Law Enforcement Disclosure report
- **Big data and analytics** – We conducted privacy impact assessments for big data and analytics projects in various countries and issued further guidelines to our local markets on how to increase transparency and provide customers with meaningful choices about how their data is used. We engaged with privacy NGOs to explain our approach and seek their input on innovative ways to build consumer confidence in data analytics applications. We also worked with our local privacy teams to ensure our global policy on the permissions and transparency required to use customer information, adopted in 2013, is integrated in our processes across the business
- **Connected car** – Working closely with Vodafone's machine-to-machine (M2M) team, we conducted an extensive privacy impact assessment which helped to shape the development and design of our connected car platform, Vodafone Vehicle Connect, and usage-based insurance proposition. We will publish a white paper in 2014 on how we designed privacy into our connected car proposition, including recommendations for establishing industry standards around privacy for the emerging connected car and usage-based insurance sectors.

In focus: Recognition for privacy leadership

Vodafone's Chief Technology Security Officer in India, Burgess Cooper, received the 2013 Privacy Leader of the Year Award from the Data Security Council of India (DSCI), a not-for-profit organisation that develops and promotes security and privacy best practice. The DSCI stated that:

"Positioning privacy as a brand differentiator and having ensured that a few operating circles [telecoms regions] of Vodafone India are already certified against the BS10012 standard, Mr Burgess Cooper stands out as a leader in the privacy domain."

Find out more about the DSCI Excellence Awards 2013 on their website at www.dsci.in/taxonomypage/863

Our efforts to ensure the privacy of our customers' information would be meaningless without our measures to ensure the security of that information. In 2013/14, we continued to strengthen our information security controls and systems and emphasise the link between privacy and security functions at Group and local level. Senior Technology Security Heads improve oversight and mitigation of information security risks, reporting directly to the Chief Technology Security Officers in each local market and working closely with their local Head of Corporate Security.

In 2013/14, we continued to proactively address emerging threats and vulnerabilities through ongoing monitoring and compliance programmes. Remediation plans have been put in place to address deficiencies identified through these programmes. We also recognise that if things do go wrong, we need to act quickly and transparently to protect our customers.

Privacy and security – Performance in 2013/14

We piloted a new customer privacy impact service to ensure that we always put the customer first when incidents occur (see feature below).

In focus: Responding quickly and transparently to protect our customers

In September 2013, Vodafone Germany suffered a highly sophisticated and illegal intrusion into one of its servers in Germany, which resulted in the theft of a limited amount of our German customers' data. In order to ensure that we had the best advice and information about the potential impact of this theft on our customers, we initiated a new rapid investigation service using a specialist independent security consultancy. Within eight hours of the details of the incident being obtained, we had received a report detailing the potential impact on our customers, including the risks of identity theft or fraud, and had received independent advice on the steps we could take to protect our customers. Our communications to our customers referenced this independent advice and we offered our customers free use of an identity theft service to minimise any risk of harm to them.

Creating a cultural shift

Creating awareness of privacy and security across Vodafone is vital to ensure that we provide the best experience for our customers and our global employee awareness campaign, Doing What's Right, was extended across all markets in 2013/14.

We have launched a global security awareness online portal accessible to all employees, containing guidance, policies and procedures on how to work securely at home, in the office and on the move, building on our global security awareness strategy, Protect and Secure.

A series of e-learning courses were developed in 2013/14 and are being rolled out globally in 2014/15, including a course on security and three modules on privacy – Privacy Basics, Privacy-by-Design and Privacy and Human Rights.

In 2013/14, we provided tailored training for all employees in high risk roles, including those who deal with highly confidential information on a daily basis, with particular attention to employees working in call centres and retail stores, and senior leaders.

Our Secure World Award, launched in 2013, gives our security teams from across the Group the opportunity to share inspirational stories on how we are protecting and securing our business, customers and the wider community. The winner of the 2013 award was Vodafone UK, which worked with our distribution partner to establish a new system to prevent the delivery of fraudulent orders, saving Vodafone £1.6 million.

In 2013, we ran a year-long Privacy Dialogue to raise awareness and help people across the business live up to the Vodafone Privacy Commitments (see Our approach). Using internal communications tools and social media, this featured a series of activities to bring privacy to life including a global competition inviting employees to respond and vote on a series of dilemmas, illustrating the importance of our commitment to choice, and a campaign that highlighted examples of how important good design is to solving problems, linking to our commitment to Privacy-by-Design.

We also held our fourth annual global Privacy Summit, a week-long series of events in London, Dusseldorf, Johannesburg and Mumbai with workshops and external speakers. The theme of the Summit this year was 'Seizing the Opportunity', emphasising the importance of our privacy programme to the long-term commercial success of the business. Over 500 people from across Vodafone participated in person or online.

In focus: Training employees on security in Turkey

Vodafone Turkey launched a new training app in 2013/14 that uses a game to raise employee awareness and understanding of information security practices.

Many security breaches are the result of human error. By training our people on security best practice, we can prevent these breaches and protect our customers and our business. With this in mind, Vodafone Turkey developed and launched a training app that can be accessed on any tablet device, which aims to promote and engage employees in our Five Simple Steps on information security.

Contributing to policy and debate

In 2013/14, we continued to participate in dialogue and debate about the proposed EU Data Protection Regulation and the EU's Cyber Security Strategy and the Commission's proposal for a Directive on Network and Information Security.

Following intense public scrutiny, government surveillance has been a topic of much debate. We have a well established policy on assisting law enforcement authorities and throughout 2013/14, we have engaged extensively on this issue with stakeholders in government and across civil society and the media, including through our participation in the Telecommunications' Industry Dialogue on Freedom of Expression and Privacy.

We participated in the first joint learning forum of the Telecommunications' Industry Dialogue on Freedom of Expression and Privacy and the Global Network Initiative in December 2013. We also took part in workshops in London and Brussels, as part of the Center for Democracy & Technology's project, examining Systematic Government Access to Private-Sector Data, which aims to improve understanding of the

Privacy and security – Performance in 2013/14

nature and scope of government legal powers to order access to data held by private sector organisations. Our inaugural Law Enforcement Disclosure report, and accompanying legal annex, represents Vodafone's latest contribution to this complex and controversial area.

Another emerging issue is the increasing concern about the risks and challenges to consumer privacy from the growth and popularity of mobile apps. Regulators around the world have issued a range of new guidelines to tackle the 'application' of society. As one of the founder companies behind the GSMA's Mobile Privacy Initiative in 2010, Vodafone has played a leading role in articulating appropriate standards and accountability mechanisms for mobile app deployment, including Vodafone's Mobile Application Privacy Principles and the GSMA's Privacy design guidelines for mobile applications.

In 2013/14, we worked with the Mobile Entertainment Forum, an industry association for companies seeking to monetise their products and services using mobile technology, to create a tool to help mobile app developers implement privacy-by-design requirements. The AppPrivacy tool is available to developers free of charge and includes an automated privacy policy generator that creates a short, simple, user-friendly statement explaining how the app uses personal data.

Vodafone also participates in external programmes to strengthen cyber security standards and define minimum standards that industry and nation states should be expected to adhere to, including government programmes in the EU and US and those run by NGOs such as the Internet Security Alliance.

Implementing industry principles on freedom of expression and privacy

Vodafone is a founding member of the Telecommunications' Industry Dialogue on Freedom of Expression and Privacy, which was launched in March 2013, alongside a collaboration with the Global Network Initiative (GNI) to advance freedom of expression and privacy rights in the telecoms industry. Find out more about the work of the Industry Dialogue during its first year here.

In March 2013, we adopted the Guiding Principles on Freedom of Expression and Privacy, which set out a common approach to dealing with privacy and freedom of expression in a principled, coherent and systematic way across the industry.

The Guiding Principles are closely aligned with Vodafone's own existing Global Law Enforcement Assistance Policy Standard. We continue to work to embed this and the table below sets out Vodafone's status and activities on each of the principles.

Our Law Enforcement Disclosure report on page 58 also provides more detail on our approach to responding to law enforcement demands.

See next page for Vodafone's alignment with the Industry Dialogue Guiding Principles on Freedom of Expression and Privacy.

Privacy and security – Performance in 2013/14

Vodafone's alignment with the Industry Dialogue Guiding Principles on Freedom of Expression and Privacy

Guiding Principle	Vodafone's alignment
Telecommunications companies should, to the fullest extent that does not place them in violation of domestic laws and regulations, including licence requirements and legal restrictions on disclosure:	
1. Create relevant policies, with Board oversight or equivalent, outlining commitment to prevent, assess, and mitigate to the best of their ability the risks to freedom of expression and privacy associated with designing, selling, and operating telecommunications technology and telecommunications services.	Our Privacy Commitments (see Our approach section) and Global Policy Standard on Law Enforcement Assistance, with Executive Committee sponsorship, set out the requirements for balancing the potentially conflicting requirements of respecting privacy and assisting law enforcement. During 2013/14, we carried out a global audit of compliance with the policy, which included detailed on-site reviews of operational management of law enforcement assistance and compliance with our policy standard, in certain markets.
2. Conduct regular human rights impact assessments and use due diligence processes, as appropriate to the company, to identify, mitigate and manage risks to freedom of expression and privacy – whether in relation to particular technologies, products, services, or countries – in accordance with the Guiding Principles for the Implementation of the UN 'Protect, Respect and Remedy' framework.	A range of due diligence processes are in place. These include: • The Strategic Privacy Risk Register (see Our approach section), which is at the centre of a formal review process used regularly to assess the most significant privacy risks affecting our business • A due diligence process undertaken before entering new markets, acquiring businesses or establishing new partnerships. This process incorporates human rights issues such as corruption, respect for privacy, internet freedom, freedom of expression and workers' rights, to assess and highlight the potential impacts or risks associated with entering new markets. In 2013/14, we further strengthened our human rights impact assessment process for potential new markets identified as high risk • Our Global Advisory Forum brings together a cross-functional group of experts from across Vodafone Group to provide input on potential new products, services and technologies, ensuring that privacy and freedom of expression are taken into account at the earliest stage of the design process.
3. Create operational processes and routines to evaluate and handle government requests that may have an impact on freedom of expression and privacy.	Our Global Policy Standard on Law Enforcement Assistance includes guidance for evaluating and, where necessary, escalating demands and requests from law enforcement agencies.
4. Adopt, where feasible, strategies to anticipate, respond and minimise the potential impact on freedom of expression and privacy in the event that a government demand or request is received that is unlawful or where governments are believed to be misusing products or technology for illegitimate purposes.	The Global Policy Standard on Law Enforcement Assistance provides requirements on challenging law enforcement where we have reasonable grounds to believe the request is not legally mandated or is unlawful. It requires operating companies to bring together the right people to consider the possible impacts and actions and use their judgement.

Privacy and security – Performance in 2013/14

Guiding Principle	Vodafone's alignment
5. Always seek to ensure the safety and liberty of company personnel who may be placed at risk.	Vodafone's Code of Conduct includes a high-level commitment to protect the health, safety and wellbeing of our employees, and the Global Policy Standard on Law Enforcement Assistance requires potential personal risk to individuals to be considered in any decision to challenge law enforcement demands.
6. Raise awareness and train relevant employees in related policies and processes.	Our Global Policy Standard on Law Enforcement Assistance includes a requirement on training and awareness and we continually raise awareness as part of our wider privacy communications campaigns (see above). A series of e-learning courses were developed in 2013/14 including a module on Privacy and Human Rights. This is being rolled out globally in 2014/15.
7. Share knowledge and insights, where relevant, with all relevant and interested stakeholders to improve understanding of the applicable legal framework and the effectiveness of these principles in practice, and to provide support for the implementation and further development of the principles.	We regularly share knowledge and engage with stakeholders on these issues, for example through the stakeholder engagement activities of the Telecommunications Industry Dialogue. This included a GNI/Industry Dialogue joint learning forum involving approximately 100 participants from companies, government and non-governmental organisations held in Brussels in November 2013. We also provide information through this Group Sustainability Report, our online Privacy Centre and in our new Law Enforcement Disclosure report.
8. Report externally on an annual basis, and whenever circumstances make it relevant, on their progress in implementing the principles, and on major events occurring in this regard.	The Law Enforcement Disclosure report and this Privacy and security section of our Group Sustainability Report covers Vodafone's approach and activities on these issues. During 2013/14, we developed and communicated to our operating companies, guidance on the definition and reporting process for major events. This process will continue to be rolled out during 2014.
9. Help to inform the development of policy and regulations to support freedom of expression and privacy including, alone or in cooperation with other entities, using its leverage to seek to mitigate potential negative impacts from policies or regulations.	The Global Policy Standard on Law Enforcement Assistance covers engagement with government on these issues and we regularly contribute to dialogue on the development of policies on a national and international level.
10. Examine, as a group, options for implementing relevant grievance mechanisms, as outlined in Principle 31 of the UN Guiding Principles for Business and Human Rights.	During 2013/14, the Industry Dialogue companies have shared ideas of how to implement operational-level grievance mechanisms and reviewed examples and guidance from other sectors.

EY
Building a better working world

Vodafone's alignment with the Industry Dialogue Guiding Principles on Freedom of Expression and Privacy in this section is included within EY's assurance of Vodafone's Sustainability Report.

For more details see our Assurance Statement.

June 2014

Notes:

1. The Data Dialogue report from UK Think Tank DEMOS