Privacy and security – Our approach

Protecting our customers’ personal information and respecting their privacy are essential to maintain their trust. Managing privacy and security risks effectively and putting customers in control of their data is core to our approach.

People are increasingly concerned about the privacy and security of their personal information as they use communications technology more and more. We aim to make it easier and more intuitive for our customers to understand and take control of how their data is used.

The complexity of technology, cyber threats and the potential for human error can lead to information being lost, deleted or getting into the wrong hands. Our policies and programmes are designed to ensure the privacy and security of customer information across Vodafone. We offer a range of apps and network services that help consumers and enterprise customers enhance their privacy and security.

Governments also have legal powers to demand access to customer communications and data and we manage these challenging issues through the policies and procedures covered in detail in our Law Enforcement Disclosure report.

There is enormous potential to use personal data to create economic and social value for individuals and businesses. To realise this potential, people need to give businesses access to their data and they need to know that it will be used responsibly. We help put our customers in control of their data and how it is used with tools that enable them to manage privacy and permissions for their devices, apps and interactions with Vodafone.

Read on to find out more about our approach. Or go to our Performance section to read about our progress in 2014/15.

In focus: Law Enforcement Disclosure report

The issue of government surveillance has come under increased scrutiny. Our Law Enforcement Disclosure report 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 receive 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 work with key stakeholders on the best way to do this.

Through the Law Enforcement Disclosure report, we:

- explain the principles, policies and processes we follow when responding to law enforcement and intelligence gathering demands from agencies and authorities
- 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 if a government or other public body already discloses such information
- cite the relevant legislation which prevents us from publishing this information in certain countries.


In February 2015, we updated the Legal Annexe to the Law Enforcement Disclosure report to provide, on a country-by-country basis, an overview of three further categories of legal power which may be used by government authorities – this time in the area of censorship. Those categories are: the shutdown of network or communication services; the blocking of access to URLs and IP addresses; and the powers enabling government agencies and authorities to take control of a telecommunication network.

The next full report will be available from mid July 2015.
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.

Creating the right culture

Our privacy and security programmes govern how we collect, use and manage customers’ information – ensuring the confidentiality of their personal communications, respecting their permissions and protecting and securing their information.

We promote a strong internal culture where our employees understand the critical nature of privacy and security risks and know how to manage them. Privacy and security are fundamental to our global Code of Conduct, by which all Vodafone employees are bound, [http://www.vodafone.com/content/index/about/about-us/code-of-conduct.html](http://www.vodafone.com/content/index/about/about-us/code-of-conduct.html).

Our Privacy Commitments set out the principles that govern our approach to privacy and build customer trust through transparency, empowerment and reassurance (see feature below).

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.
Managing privacy and security risks

New technologies such as mHealth, smart working, big data analytics and the Internet of Things offer significant economic and social benefits to people and businesses around the world, see our Transformational solutions section. But their use of personal data raises complex privacy and security risks.

Risk management is central to our approach to privacy and security. To help us identify and manage emerging risks, we assess the implications of our business strategy, new technologies, customer concerns, cyber threats and relevant industry developments.

We conduct regular formal reviews of the most significant privacy and security risks affecting our business at Group and develop strategies to respond to the most critical risks (see table below).

Our response may include investing in new capabilities or technologies, revising policies or working through associations such as the GSMA to influence others in our industry, http://www.gsma.com/. We engage regularly with external stakeholders and draw on their expertise to help shape our strategy and respond to their concerns.

Understanding and responding to privacy and security strategic risks

<table>
<thead>
<tr>
<th>Issue</th>
<th>Risk</th>
<th>Vodafone’s approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud services and hosting</td>
<td>Enterprise and consumer cloud-based services require the movement of data across international borders. Doing so helps us deliver faster services and reduce costs by avoiding duplication of infrastructure. This must be conducted lawfully, legitimately and securely, both within our own organisation and between Vodafone and its suppliers.</td>
<td>As part of our supplier engagement process, cloud service providers are evaluated from a legal and data protection perspective by specialist teams, to understand where data will be stored, what security arrangements for personal information are provided, and what contractual controls apply. Our contracts require all suppliers to advise us of any change in location of data storage and any data security breach.</td>
</tr>
<tr>
<td>Network traffic management</td>
<td>To deliver a high-quality network service, we need to manage the flow of telecommunications traffic across our network. For example, we may need to prioritise an uninterrupted video call over an email that is not so time critical. This requires us to examine some of the information, known as data packets, to identify the type of communication. The actual content, such as the text in a text message, is not inspected. This technique is sometimes referred to as deep packet inspection and can raise concerns about privacy.</td>
<td>We have a policy and a set of specific requirements that govern how we manage telecommunications traffic. Other than for the lawful purpose of managing traffic across our networks, our policy prohibits the use of network technologies that inspect data packets without an in-depth privacy impact assessment. This assessment ensures compliance with the law and allows us to evaluate and avoid or minimise the potential impact on the customer. Use of these technologies must be authorised by a senior executive at Group.</td>
</tr>
<tr>
<td>Advertising, analytics and big data</td>
<td>The vast amount of data generated by our customers has enormous potential value for mobile commerce and programmes with societal benefits, such as analysing traffic to support effective investment in transport infrastructure. The expansion of mobile connectivity into new fields means greater volumes of data. Even when anonymised and aggregated, concerns arise about how the value of big data can be unlocked while protecting individual privacy.</td>
<td>We have policies, guidelines and design principles for applications and services that use personal data. These seek to ensure that we provide customers with clear choices about how their data is used. We also research consumer perceptions and concerns to inform our strategy and help develop techniques that can enhance privacy.</td>
</tr>
</tbody>
</table>
### Privacy and security – Our approach

<table>
<thead>
<tr>
<th>Issue</th>
<th>Risk</th>
<th>Vodafone’s approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law enforcement assistance and human rights</td>
<td>Everywhere 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, their use must be balanced with the respect for civil liberties and freedoms, including individuals’ privacy and freedom of expression.</td>
<td>We closely manage compliance with legal obligations in respect to law enforcement assistance and our relationship with law enforcement authorities, in order to maintain our respect for human rights. We also engage with governments to seek to ensure that legal provisions governing the use of these powers contain adequate protection for human rights. 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, <a href="http://www.vodafone.com/content/sustainabilityreport/2015/index/operating-responsibly/privacy-and-security.html">http://www.vodafone.com/content/sustainabilityreport/2015/index/operating-responsibly/privacy-and-security.html</a>. We also publish statistics on the number of law enforcement demands we receive on a country-by-country basis, where it is legal to do so and the government does not already publish such information. This report will be updated in mid-July 2015. Our 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, <a href="http://www.vodafone.com/content/index/about/about-us/privacy/human_rights.html">http://www.vodafone.com/content/index/about/about-us/privacy/human_rights.html</a>. Vodafone is a founding member of the Telecommunications Industry Dialogue, <a href="https://telecomindustrydialogue.org/">https://telecomindustrydialogue.org/</a>, and a signatory to its Guiding Principles on Freedom of Expression and Privacy, <a href="http://www.vodafone.com/content/dam/sustainability/pdfs/telecom_industry_dialogue_principles.pdf">http://www.vodafone.com/content/dam/sustainability/pdfs/telecom_industry_dialogue_principles.pdf</a>. These 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.</td>
</tr>
</tbody>
</table>
In focus: Taking action on global cyber security

The risk of cyber-attacks is treated by many countries as a priority threat to national security. Cyber threats – from competitors, hacktivists, cyber criminals, terrorists or nation states – pose a significant risk to our business and our customers.

Anticipating and preventing these threats is essential to ensure the security of critical national infrastructure that is supported by our networks and to maintain trust in e-commerce. We analyse and review cyber security threats and develop strategies to respond to the most critical risks.

Vodafone’s Global Security Operations Centre 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. We have a robust business continuity management programme across Vodafone to ensure an effective and timely response to any emergency or crisis involving critical business operations. We align our business continuity management with International Standards, such as ISO 22301, and local legislation.
Respecting privacy, protecting security and putting customers in control of their information is critical to our continued success.

Our investment in security measures is more important than ever. Cyber-attacks are becoming more sophisticated. And wider use of social media is leading to an increase in identity theft and attempts by fraudsters to gain access to confidential information by posing as others online.

Government access to individuals’ private communications has come under increased scrutiny. Our Law Enforcement Disclosure report aims to increase transparency and improve understanding of this issue.

Putting customers in control

We put customer needs at the heart of our approach to privacy. We see huge potential to differentiate our brand by offering products and services designed to support customers in improving their privacy and security.

A new approach to transparency

Personal data belongs to our customers. We are building tools that put them in control by easily view and update the permissions they grant to use their data. We believe the best way to address our customers’ concerns is to make a clear and bold promise to them. We want to make sure that when we talk to our customers about privacy it is not confusing or hidden in legal small print.

To assess and understand customer concerns and awareness of privacy issues, we surveyed 11,000 customers across 11 European markets in 2014/15. This research helped us understand and quantify the commercial benefits of a customer-centric approach to privacy and permissions. We also conducted in-depth conversations with customers about their needs and their desire to manage their information.

Based on this research, we are rolling out improved tools for our customers that will enable them to take control of their personal information so that they can easily see the type of information Vodafone holds about them, find out how this information is used and consent or withdraw their permission for its use. We intend for these tools to be accompanied by a clear promise to our customers which details how we will treat their data, written in terms they can understand.

Several of our products demonstrate the potential of privacy and security as a business opportunity for Vodafone. In 2014/15, we introduced Secure Net in six local markets, http://securenet.vodafone.com/. This service helps protect customers and their families from harmful content, including phishing sites and malware, when using the Vodafone network. A complementary service, Secure Net Companion, offers customers end-to-end protection across our network and when they are using their device over Wi-Fi.

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 (such as smart metering, connected cars and wearable technology). Our approach takes into account recent positions from regulators, such as the US Federal Trade Commission and the European Commission, and translates these positions into requirements for our business. We are also working with organisations like the GSMA to create a standard industry approach, http://www.gsma.com/.
Privacy and security – Performance in 2014/15

Strengthening our programmes

In 2014/15, we continued to address emerging privacy and security 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 openly to protect our customers. We piloted a new customer privacy impact service to ensure that when incidents occur they are managed effectively and that we always put the customer first.

Our internal audit teams conducted in-depth assessments in 2014/15 to test how effectively our global privacy risk management systems are working in the Czech Republic, Germany and Spain. No major non-compliance issues were found. We also undertook an audit of three Vodafone service centres, which provide internal technology and process support for our employees, where some non-compliance issues were identified. We are reviewing the findings and will follow up with these centres.

Our local markets conducted a total of 425 privacy risk impact assessments for new products and services in 2014/15. In addition, we conducted an internal strategic review of our cloud services to ensure a consistent global approach to cloud privacy and security, whether for our internal use or for our customers. As countries around the world move towards requirements for local hosting of essential data, we monitor these developments and ensure that our global platforms and centralised services can comply and compete.

We also assessed compliance with our Global Policy Standard on permissions and audited the permissions we capture from customers to hold and use their data across all our local markets for products and services in areas like marketing, analytics and advertising. This helped us understand how well we are implementing our guidelines on being transparent with customers about choosing which information to share and how it is used. We continue to work with our local privacy teams to ensure our global policy on the permissions required to use customer information is integrated in our processes across the business.

Our acquisition of Cobra Automotive Technologies (now called Vodafone Automotive) brought with it the development of new capabilities in M2M technology for the automotive field. We will publish a white paper in 2015/16 on how we are designing privacy into our connected car proposition, http://m2m.vodafone.com/cs/m2m/discover-m2m/industries/automotive. This will include recommendations for establishing industry standards around privacy for the emerging connected car and usage-based insurance sectors.

Nurturing a culture of privacy and security

Raising awareness of privacy and security issues among employees is critical to our efforts and we use a wide range of tools to communicate effectively on this issue across the business. Our global privacy and security awareness online portals contain policies and guidance, for example on how to work securely at home, in the office and on the move.

Training on the importance of privacy and security is included in our Doing What’s Right e-learning course for all employees, see our Ethics section. In 2014/15, we launched global e-learning modules on privacy and security for employees in high-risk roles around the world, including those who make decisions about product design, respond to government requests or deal with highly confidential information on a daily basis. In the 14 months since its launch, more than 83,000 employees (around 82% of our workforce) have completed the Privacy Basics module.

In December 2014, we ran our fifth annual global Privacy Summit – a week-long series of virtual events, focused on navigating emerging challenges in privacy, including our competitive environment, new technologies and changing legal frameworks governing privacy and data protection around the world. Over 600 people from across Vodafone visited the website to watch videos, read articles and participate in interactive features.

Contributing to policy and debate

In 2014/15, we continued to participate in dialogue and debate about appropriate data regulatory regimes around the world, including the EU General Data Protection Regulation, ePrivacy Directive review, Big Data strategies, Cybersecurity Strategy and the European Commission’s proposal for a Directive on Network and Information Security.

Government surveillance remains a topic of public scrutiny and debate. In 2014/15, we 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 (see table). Our pioneering Law Enforcement Disclosure report was recognised in the 2014 Public Relations Consultants Association (PRCA) Awards for its impact on the dialogue around government surveillance, winning the best international campaign award. We are committed to promoting better transparency, clarity, consistency and due process in government assistance requests. We have engaged in discussions on this topic with governments in markets where we operate, including Australia, Germany, Malta, the Netherlands, Portugal, Spain and the UK.
Ubiquitous connectivity, big data and the Internet of Things have huge implications for our business, the wider industry and society as whole. In 2014/15, we advocated for appropriate privacy protocols and industry standards in these areas that will allow us to effectively manage privacy and security risks, while enabling consumers and businesses to realise the benefits of these global trends.

Vodafone participates in external programmes to strengthen cyber security standards and define minimum standards that industry and nation states should be expected to adhere to. These include government programmes in the EU, US and the Commonwealth and those run by NGOs such as the Internet Security Alliance. Through these external programmes, we promote a Cyber Social Contract between industry and government, working collaboratively to identify effective standards and practices in response to cyber threats. However, minimum universal standards can only go so far. It is critical for Vodafone and other businesses to build on these standards to suit the unique risk profile of their organisations and keep pace with continually evolving threats.

Implementing industry principles on freedom of expression and privacy


We are a signatory to the Industry Dialogue's Guiding Principles on Freedom of Expression and Privacy, http://www.vodafone.com/content/dam/sustainability/pdfs/telecom_industry_dialogue_principles.pdf. These set out a common approach to dealing with privacy and freedom of expression in a principled, coherent and systematic way across the industry. They are closely aligned with Vodafone's own existing Global Policy Standard on Law Enforcement Assistance, http://www.vodafone.com/content/index/about/about-us/privacy/human_rights.html. We continue to work to embed this policy and its guiding principles and drive continuous improvement. The table below sets out Vodafone's status and activities on each of the principles.

Our Law Enforcement Disclosure report provides more detail on our approach to responding to law enforcement demands. The second edition will be published in mid-July 2015.

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

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:

<table>
<thead>
<tr>
<th>Guiding Principle</th>
<th>Vodafone’s alignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>We closely manage and monitor compliance with legal obligations and our relationship with law enforcement authorities to address respect for human rights. Our Privacy Commitments (<a href="http://www.vodafone.com/content/sustainabilityreport/2015/index/operating-responsibly/privacy-and-security.html">http://www.vodafone.com/content/sustainabilityreport/2015/index/operating-responsibly/privacy-and-security.html</a>) and Global Policy Standard on Law Enforcement Assistance (<a href="http://www.vodafone.com/content/index/about/about-us/privacy/human_rights.html">http://www.vodafone.com/content/index/about/about-us/privacy/human_rights.html</a>) with Executive Committee (ExCo) sponsorship, set out the requirements for balancing the potentially conflicting requirements of respecting privacy and assisting law enforcement. These outline that accountability is held at the most senior level. We carried out a global audit of compliance with the policy in 2013/14. It included detailed on-site reviews of the operational management of law enforcement assistance and compliance with our policy standard in certain markets.</td>
</tr>
<tr>
<td>Guiding Principle</td>
<td>Vodafone’s alignment</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| 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:  
- regular formal reviews of the most significant privacy and security risks affecting our business at Group, and strategies to respond to the most critical risks, see earlier  
- 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 and freedom of expression. It assesses and highlights the potential impacts or risks associated with entering new markets. Our human rights impact assessment process for potential new markets identified as high risk was further strengthened in 2013/14  
- 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. We conduct privacy impact assessments, require compliance with the law and evaluate the potential impact on the customer, so that they can be avoided or minimised. Privacy impact assessments for products and services developed by our local markets are also a key part of our Privacy Risk Management System. |
| 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 from law enforcement agencies. Governance controls in our Policy Compliance Review measure how our local markets adhere to the global standard. As part of the 2014 review, the governance controls were tested across all our markets and the majority were found to be compliant. Seven markets strengthened their controls in this area as a result. Only one market had a remedial action outstanding by the end of 2014/15 and that action has since been completed. |
| 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 demand 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. |
| 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 well-being of our employees, [http://www.vodafone.com/content/index/about/about-us/code-of-conduct.html](http://www.vodafone.com/content/index/about/about-us/code-of-conduct.html). 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. |
## Guiding Principle

<table>
<thead>
<tr>
<th>Guiding Principle</th>
<th>Vodafone's alignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Raise awareness and train relevant employees in related policies and processes.</td>
<td>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 earlier. In 2014/15, we rolled out a global e-learning course on Privacy and Human Rights. The course is designed for those who make decisions about government and law enforcement requests, but is available to employees in almost all markets. By the end of March 2015, it had been completed by more than 12,000 employees worldwide. This topic is also incorporated into our general internal privacy awareness campaigns.</td>
</tr>
</tbody>
</table>
| 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, [https://www.telecomindustrydialogue.org/wp-content/uploads/Telco-Industry-Discourse-Annual-Report-2015.pdf](https://www.telecomindustrydialogue.org/wp-content/uploads/Telco-Industry-Discourse-Annual-Report-2015.pdf). In 2014, Vodafone joined the panel of one of the two GNI/Industry Dialogue joint learning forum events, which were attended by a total of approximately 120 participants from industry, academia, government and non-governmental organisations. The forums focused on the theme of Transparency and Human Rights in the Digital Age. Since April 2014, the Industry Dialogue’s quarterly meetings have been extended to include a roundtable discussion with stakeholders including investors, government officials, members of civil society and academia and other companies. During these meetings, Industry Dialogue companies have shared the challenges they face and progress they have made in implementing the Industry Dialogue’s Guiding Principles. Vodafone has shared knowledge and engaged with stakeholders through a number of forums. For example, we participated in the Big Brother Watch Events, Civil Liberties in a digital age, at the three main UK political party conferences in 2014, [http://www.bigbrotherwatch.org.uk/big-brother-watch-party-conferences/](http://www.bigbrotherwatch.org.uk/big-brother-watch-party-conferences/). We provide information through this Group sustainability report, our online Privacy centre ([http://www.vodafone.com/content/index/about/about-us/privacy.html](http://www.vodafone.com/content/index/about/about-us/privacy.html)) and in our Law Enforcement Disclosure report. In February 2015, we updated the Legal Annexe to the Law Enforcement Disclosure report to include a review of three further categories of legal power that may be used by government agencies and authorities to restrict the use of communication networks or to restrict access to certain content or services. The three categories relate to:  
  - shutdown of networks or communication services  
  - blocking of URLs and IP addresses  
  - taking control of a telecommunications network. |
| 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 cover Vodafone’s approach and activities on these issues. During 2014/15, we continued to communicate guidance on the definition and reporting process for major events to our local markets. |
## Guiding Principle

### 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.

Vodafone’s alignment: The Global Policy Standard on Law Enforcement Assistance covers engagement with governments on these issues and we regularly contribute to the dialogue on the development of policies on a national and international level. We seek to ensure that legal provisions governing the use of powers to access information about customers or users of our services contain adequate protection for human rights. We are committed to working for better transparency, clarity, consistency and due diligence processes in government demands for assistance. We have engaged on this topic with governments where we operate including in Australia (our joint venture), Germany, Malta, the Netherlands, Portugal, Spain and the UK. For example, in 2014 Vodafone provided input to the independent review of the UK’s terrorism legislation, [http://www.vodafone.com/content/index/about/about-us/privacy/uk-investigatory-power.html](http://www.vodafone.com/content/index/about/about-us/privacy/uk-investigatory-power.html).

We also contribute to the dialogue on the development of policies at a national and international level through the Telecommunications Industry Dialogue. A number of inputs on these issues are available on the Telecommunications Industry Dialogue website, [https://telecomindustrydialogue.org/content/resources](https://telecomindustrydialogue.org/content/resources).

### 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.

Vodafone’s alignment: During 2014/15, the Industry Dialogue companies have continued to share ideas on how to implement operational-level grievance mechanisms and reviewed examples and guidance from other sectors.

Vodafone has a number of mechanisms whereby grievances can be raised. Employees and contractors in all local markets can use our global external reporting scheme, Speak Up, to report concerns, see our Ethics section. Customers can raise complaints or concerns through established contact channels, which vary in the countries where we operate. They include direct communication with Privacy or Data Protection Officers, or complaints through third-party mechanisms such as rating and certification organisations.

---

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 2015**