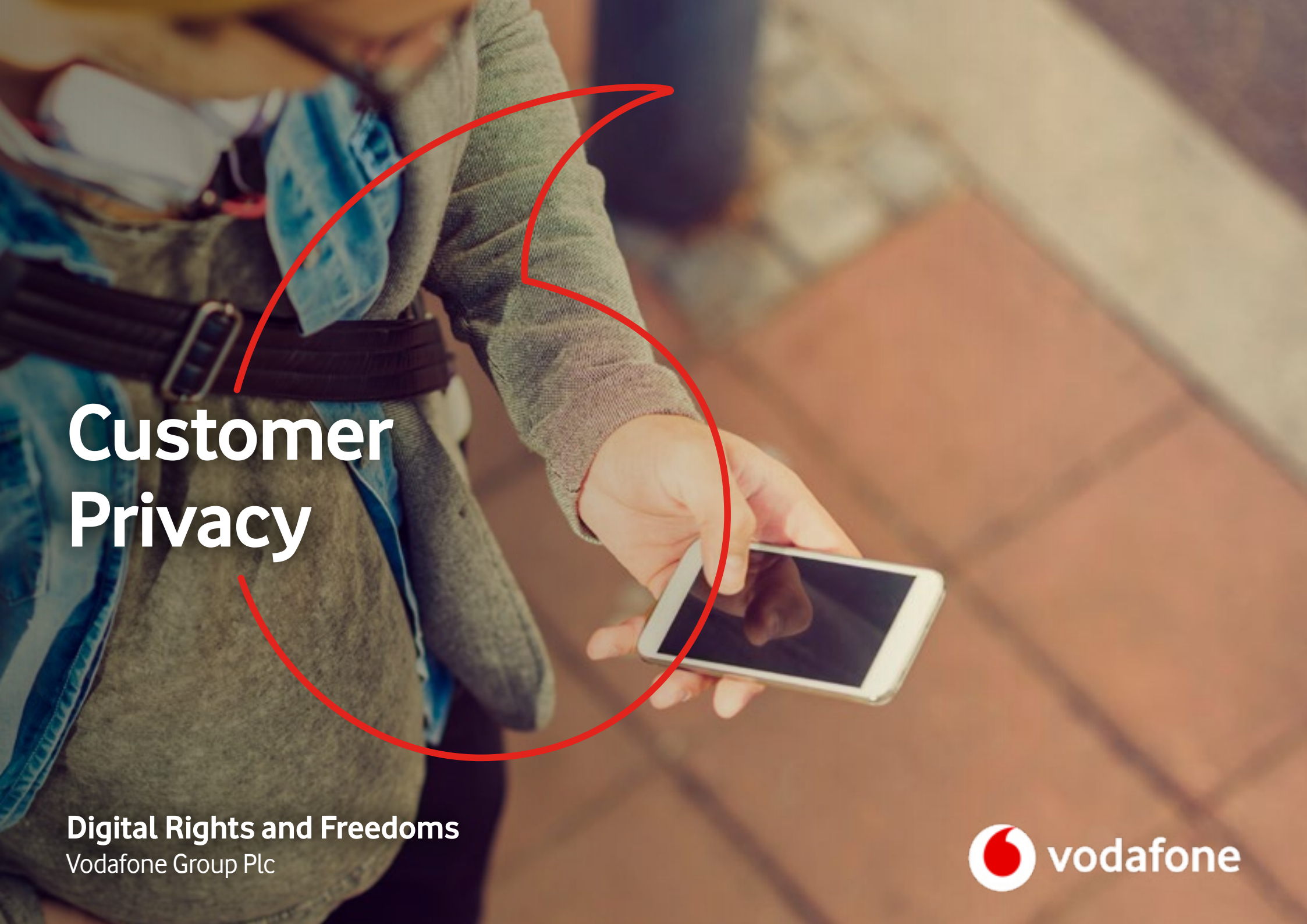

# Customer Privacy

**Digital Rights and Freedoms**
Vodafone Group Plc

vodafone

# Customer Privacy

Respecting our customers' privacy is essential to maintaining their trust in our business. Managing privacy risks effectively – and putting customers in control of their data – is core to our approach.

## Creating the right culture

Our privacy policies and framework govern how we collect, use and manage our customers' information in order to ensure we respect the confidentiality of their personal communications and any choices that they have made regarding the use of their data. The protection of personal data is one of our highest priorities and is central to the Vodafone Code of Conduct that everyone who works for us (or on our behalf) must follow.

*"Privacy is central to earning and sustaining trust in Vodafone and being a responsible and ethical corporate citizen. We always consider the impact our decisions have on the privacy of our customers and employees. Whenever we design products, launch campaigns, sign up vendors, collect information and share such information with our partners and others, we observe and adhere to Vodafone's Privacy Commitments."*

All high-risk policy areas – including the protection of privacy – are covered in Vodafone's annual 'Doing What's Right' internal communications campaign, which raises awareness of the importance of privacy through internal communications, events, online articles and webinars with members of the senior leadership team.

## Privacy policy standards

Vodafone's Privacy Commitments are supported by four privacy policy standards that have been developed to address specific areas of high privacy risk. The policy standards summarised below are overseen by the Group Executive Committee, with implementation and local engagement led by the Group privacy team.

### Privacy Risk Management Standard

This policy standard sets out the resources and privacy risk control processes that must be in place in each of our local markets to ensure compliance with applicable local data protection laws as well as with Vodafone's Privacy Commitments. Those control processes include a privacy risk impact assessment of personal data processing activities – at a functional or organisational level – of new products and services, and of new suppliers. They also require the implementation of a data breach management process and a document management and retention policy. Privacy risks must be logged, and any minimising actions are recorded and monitored for completion. Regular reporting from the local privacy officer to the Group privacy team ensures clarity on how the processes are working at a local level.

### Network Traffic Management Standard

This policy standard sets out the limited purposes for which our businesses can use traffic management technologies in order to help assure the quality of our services. It is clear that there are limitations on the use of such technologies, particularly those that may have consequences from a privacy or net neutrality perspective. The policy standard also addresses the security requirements that must be implemented to protect such technologies from unauthorised access or use.

### Law Enforcement Assistance Policy Standard

This policy standard addresses the balance between our customers' right to privacy and freedom of expression and the statutory requirements to provide law enforcement assistance either through lawful intercept or retention of communications data. Our basic approach is to interpret applicable laws and demands as narrowly as is lawfully possible to guard against unwarranted or over-broad disclosure or assistance. For more information about the implementation of this policy or our approach to working with law enforcement agencies, visit our *Digital Rights and Freedoms Reporting Centre*.

### Permissions Policy Standard

This policy standard defines the customer permissions required in order to process personal data, and for which purpose. It is designed to ensure clarity in balancing internal demands for data analytics against the paramount importance of customer privacy.

# Vodafone's Privacy Commitments

Our privacy policies are supported by our Privacy Commitments, which set out the principles that govern our approach to privacy and how we seek to build customer trust through transparency, empowerment and reassurance.

Our commitment to our customers' privacy goes beyond legal compliance. We are focused on building a culture that respects privacy in order to justify the trust that people place in us:

- **Accountability:** We are accountable for living up to these commitments throughout Vodafone, including when working with our partners and suppliers. We maintain privacy policies and compliance processes that we use to ensure we live up to these principles.
- **Fairness and lawfulness:** We comply with privacy laws and act with integrity and fairness. We work with governments, regulators, policy makers and opinion-formers to help shape better and more meaningful privacy laws and standards.
- **Privacy-by-design:** Respect for privacy is a key component in the design, development and delivery of our products and services.
- **Openness and honesty:** If our actions could affect our customers' privacy, we communicate this clearly. We ensure our actions reflect our words, and we are open to feedback about our actions.
- **Choice and access:** We give people the ability to make simple and meaningful choices about their privacy and allow them – where appropriate – to access, update or delete their personal data.
- **Responsible data management and limited disclosures:** We apply appropriate data management practices to govern the processing of personal data. We limit disclosures of personal data to our partners to what is described in our privacy notices or to what has been authorised by our customers.
- **Balance:** When we are required to balance the right to privacy against other obligations necessary to a free and secure society, we work to minimise privacy impacts.
- **Security safeguards:** We implement appropriate technical and organisational measures to protect personal data against unauthorised access, use, modification or loss.

## Privacy-by-design and by default

We seek to ensure that privacy is built into our products and services by design. We conduct a privacy and legal impact assessment for all new products and services, together with an analysis of any associated data processing activity such as billing. These impact assessments are conducted by the relevant expert teams – at Group and local market level – to ensure compliance with the law and to identify any remedial actions required early in the design process to address potential consequences for customers. For example, the assessment process for enterprise products, services and technologies is overseen by the Vodafone Global Advisory Forum, whose members are relevant internal experts from across the business such as privacy, security, regulatory and business teams.

During 2015-16, we focused on developing a standardised approach to the collection and use of personal data through Vodafone's own branded apps, using the *MyVodafone* app as a case study. The installation process involved the use of clearly worded privacy notices, consent buttons and permissions settings to ensure customers were aware of how their personal data would be used by Vodafone. For example, diagnostic connection data from customer devices is used to help optimise network performance.

## Managing privacy risks

Risk management is central to our approach to privacy. To help us identify and manage emerging risks, we assess the implications of our business strategy, new technologies, customer concerns and relevant industry developments. Our response to the identification of new privacy challenges may include investing in new capabilities or technologies, revising policies or working through associations such as the GSMA to influence others in our industry. We engage regularly with external stakeholders and draw on their expertise to help shape our strategy and respond to their concerns.

The work of the Group privacy team is supported by three areas of activity designed to ensure compliance with all of Vodafone's rules related to risk management, including privacy risks. These are:

1. **The Group's internal audit function**, in which experienced auditors conduct a detailed analysis of a particular aspect of Vodafone's business and make recommendations for action which are communicated to the Group Executive Committee;
2. **Annual policy compliance reviews (PCRs)** conducted for each high-risk policy area, including privacy. For each local market, three specific controls are assessed and the local compliance officer in each country collects specified evidence that demonstrates how those three controls are being implemented; and
3. **Privacy 'deep dives'.** A 'deep dive' analysis is also conducted each year in two or three local markets; this involves an onsite compliance review during which all privacy risk control processes are assessed.

## Managing operational risks

Each privacy officer in our local markets uses our Privacy Risk Management System (explained here) to ensure our Privacy Commitments are delivered at operational level in each country in which we operate. Our Group privacy team has oversight over the privacy officers in each of our local markets. This Privacy Risk Management System provides a common framework for the assessment of – and further improvements to – our privacy programmes across the Group, while allowing the flexibility to respond to local privacy concerns, legal requirements or stakeholder expectations.

Examples of how we ensure each local market manages their customers' data appropriately include:

- maintaining a personal information location register stating where customer data is located, with a robust process to keep this register up to date;
- managing supplier privacy risk, including requiring suppliers who handle our customer data to have privacy clauses in their contracts, have appropriate risk mitigation action plans in place and be recorded within the local privacy risk register; and
- the incorporation of privacy related measures within the new product or service design process ('privacy by design').

During 2017-18, we will update these (and other) requirements to reflect the introduction of the European Commission's General Data Protection Regulations (GDPR). We will also be developing new processes to ensure that we deliver a consistent, repeatable and standard approach to managing and addressing privacy challenges that may arise, either from changes in the law or from new and emerging technologies with implications for customer privacy such as the 'Internet of Things'. The changes to our policies to reflect the GDPR will apply globally, wherever we operate – not just in Europe.

## The European Commission's General Data Protection Regulations (GDPR)

The European Directive on Data Protection 1995 resulted in each member state implementing its own version of data protection law. This has caused complexity in compliance for companies like Vodafone which has a legal presence in multiple European member states. The current Data Protection Directive will be replaced by the GDPR in May 2018. These new regulations are intended to set out one pan-European standard for data protection that will apply equally across the European Union and equally across the different information and communications technologies that are central to the daily lives of hundreds of millions of Europeans.

The GDPR builds on the data protection principles found in the original Directive but includes more prescriptive requirements for evidence of privacy risk management processes, compliance and governance structures. The Regulations also require privacy to be considered within business processing activities by design and by default. The new rules will give supervisory authorities and regulators greater powers to take action for breaches or non-compliance with the requirements, with the most severe penalty being a fine of €20 million or 4% of annual global turnover, whichever is the higher.

Our work in this area is overseen by the Group privacy team. That team will oversee the implementation of the GDPR when the new rules come into force in May 2018 and will then lead the governance process designed to ensure GDPR compliance. We are active participants in a wide range of debates regarding privacy and data protection, including the GDPR and the ePrivacy Directive review. Our response to the consultation on the latter can be found here.