Vodafone Group FAQs on Privacy and Security

1. **Does Vodafone Group publish the number of requests for data it receives from private parties?**

No. We do not publish this information because we do not comply with such requests. Vodafone does not comply with any requests for customer data by third parties unless they are from a law enforcement authority and we are legally obliged to do so. In practice that means that a third party would need to submit their request for data to the applicable agency or authority who would, following lawful procedure, potentially serve a warrant on Vodafone to disclose the data to the agency or authority. You can find out more by reading Vodafone's Global Policy Standard on Law Enforcement Assistance.

2. **Does Vodafone Group notify the relevant authorities without undue delay when a personal data breach occurs?**

Yes. Under our Business Continuity & Incident Management Plan we will notify a personal data breach to the relevant authorities, unless the breach is unlikely to result in a risk to those impacted by it (this could be because of the nature of the incident itself or owing to mitigating measures put in place by our incident response).

Notifying a personal data breach to the relevant authorities is a legal requirement in most of our countries of operation. Even where it is not a legal obligation, under our Business Continuity & Incident Management Plan we take steps to assess whether there are reasons why we should notify the authority regardless.

3. **Does Vodafone Group notify data subjects who might be affected by a data breach?**

Yes, if having taken mitigating measures to contain and mitigate the adverse consequence of a data breach, we decide that a likelihood of a high risk remains to our customers or employees, we will notify them of the data breach. This is in line with the legal requirements of data protection law in many of our countries of operation.

We may also notify our customers or employees if the circumstances imply that this would be to their benefit; for example:

- a media story breaks about a data breach and, even though it presents negligible risk, we wish to reassure our customers/employees of this; or
- a breach poses a low risk but that risk could be easily mitigated by our customers or employees taking a few simple steps (such as resetting their password).

Ultimately we notify our customers or employees of a data breach so that they can take steps to mitigate the risks a data breach might pose. In our notifications we always seek to offer customers support with mitigating those risks – for example by fixing their credit scoring / fraud prevention; advising them to change their passwords; offering a contact line for further queries etc.

4. What kinds of steps does Vodafone Group take to address the impact of a data breach on its users?

Operationally we seek to minimise the impact of a data breach before it takes place by following data protection law principles of only using personal data necessary for the purpose in hand and adopting appropriate technical and organisation measures such as encrypting personal data so that in the event of a breach the likely impact on our customers is minimised.

Should a data breach arise, the steps we take in response will depend on the nature of the breach; whether it stems from a cyber or non-cyber incident, the type, format & location of the data involved and the role of 3rd parties in moving, storing and processing the data. Regardless of the nature of the data breach, our business continuity & incident management plans will seek to understand and contain the breach as a first order priority.

We aim to deter breaches and detect them swiftly, so part of our response would leverage the insights we derive from early detection; looking at what our systems & processes can tell us about who, what, why and when.

The impact of the data breach (whether it's on the confidentiality or integrity of the data), the capability and intent of parties that may have caused the breach (internal or external) and the ways in which the data could likely be used would all feature in our remediation and response plans.

As we remediate we conduct a range of expected and recognised activities; some of these we prefer to keep confidential to disrupt malicious actors. They include forensics, data recovery (from back-up where needed), liaison with law enforcement authorities, data subject impact assessment and thinking beyond the purely technical. These activities are documented and rehearsed and throughout the process we'll be looking at the root cause/s and how to safeguard against the same or associated vulnerabilities across our estate (short-term mitigations) and also wider improvements (longer-term systemic adjustments).

During the response we'll be looking for distraction tactics (masking parallel attacks), deception attempts (false claims) and impact on customers (including the impact of our response). The response we conduct is geared to establish the facts, understand what's happened (including harmful effects), treat our customers with respect and improve where needed.