Vodafone Supplier Policy

Privacy Baseline Requirements

Scope

All Vodafone procurement agreements with Suppliers.

Policy

1. Key Principles

1.1. Vodafone (“we”, or “our”, or “us”) applies the Privacy by Design principle and expects you as a potential Supplier (“you" or "your") to have a similar focus on data privacy. The purpose of this document is to set out the basic requirements, including the technical and organisational requirements required when working with - or processing – Vodafone's customer (“Customers”), employee, or other personal data (referred to as "our personal data"). This document is available in our supplier policy portal, and available to all suppliers entering, or considering entering, into a relationship providing services to any Vodafone Group Company, or VGC. If we do enter into a contract with you, there might be additional requirements agreed with you, based on the particulars of the service and the contract, including, but not limited to a data processing or transfer agreement with specific processing terms based on the type of service you are providing to Vodafone.

1.2. You shall comply with all applicable privacy legislation, and you shall verify your compliance if we ask. These laws may include the GDPR (Regulation (EU) 2016/679 of the EU), the UK GDPR, and any local laws and regulations that might apply to you or to what you do.

1.3. You shall comply with data transfer and/or processing terms substantially similar to Vodafone’s template data processing agreement, and written security requirements (Group Minimum Security Requirements) as updated from time to time, and you shall evidence your compliance if we ask.

1.4. There is no privacy without security. You shall comply with Vodafone's Group Minimum Security Requirements (GMSR). GMSR encompasses all security measures Vodafone applies and requires you to apply throughout our cooperation with you.

1.5. You shall allocate and document the roles and responsibilities within your organisation for personal data use, breaches, and incident response. You shall be able to show us this documentation upon request. In terms of personal data breaches, you shall have clear documentation and practices on what constitutes a personal data breach in your operations and shall be able to align those definitions with ours so that we can properly do a risk analysis of an incident involving Vodafone data. You shall send us the certifications about any related data privacy frameworks you have (E.g. ISO 27701). You shall organise regular trainings and awareness-raising events about data privacy requirements to your employees involved in processing our personal data. Upon request, you shall be able to show us the documentation verifying that these events take place.

1.6. To make sure we understand the flow of our personal data, please provide data flow maps as part of requested RFx submissions. Data flow maps are graphs/diagrams that capture the end-to-end processing activities covering every service under our contract with you. The data flow maps shall depict in a concise way at least:

1.6.1 the geographical locations (i.e. the country) of processing,

1.6.2 the type of storage (e.g. public cloud, own data centre, single-tenancy or multi-tenancy, etc.),
1.6.3 the types of personal data in the flow (e.g. names, e-mail addresses, etc.),
1.6.4 the types of encryptions in transit and at rest (or in use), the systems/tools used to process the data, and how your sub-processors are involved in the processing,
1.6.5 the things you do with the personal data,
1.6.6 The certificates applying to the components depicted.

1.7. When you work with subcontractors and they process our personal data (i.e. they are sub-processors), you shall ensure that they comply with all security and privacy requirements the same way you do. We also ask for a data flow map or summary of your sub-processor relationships.

1.8. Personal data shall only be stored and used for specific purposes and strictly for as long as it is necessary for those purposes. You shall set the shortest retention periods possible per our local market requirements and only use our personal data for the specific purposes and services we specify.

1.9. You shall respond to our privacy-related questions in a timely manner. You shall at least acknowledge receiving our question and allocate a qualified specialist as a single point of contact for the question within 5 working days. We ask you to share the results and findings of the data protection impact assessments (DPIA) and transfer impact assessments (TIA) you completed on the services or tools you provide to us.

1.10. You shall send us yearly transparency reports about information disclosure requests received form government, governmental bodies, agencies (especially law enforcement bodies) and statistics about whether you have complied or not complied with the requests. You shall send us reports about any request as soon as possible if that involves sensitive personal data, or other high risk data categories (e.g. communication content, biometric data).

1.11. You shall let us know without undue delay on any amendment on the scope or purpose of the processing in the context of our agreement as well as if any additional sub-processors get involved in the processing following our initial agreement.

1.12. You shall let us know without undue delay on any significant change in your policies, procedures or infrastructure that might have an impact on the protection of the personal data in scope of our agreement.

2. Technical and Organisational Measures

2.1. You shall substantially agree to and comply with the Group Minimum Security Requirements, and if asked, send us documentation on how you encrypt personal data. We are interested especially in

2.1.1. what encryption methods you use and how,
2.1.2. who manages the encryption keys and how,
2.1.3. what other anonymisation/pseudonymization techniques you use, and
2.1.4. if you apply the principles of confidential computing

2.2. You shall send us documentation on the best practices and techniques you use ensuring that personal data is not used in test environments, error logs, and ticketing/helpdesk scenarios. Where it is not possible to provide the ticketing/helpdesk services without processing personal data, you shall be able to verify that the only pieces of personal data processed are strictly necessary to provide the ticketing/helpdesk services.

2.3. In terms of endpoint hardening on your end, we expect at least the following measures:

2.3.1. Hardened OS for servers (CCS)
2.3.2. BitLocker disk encryption for Laptops, and USB, Bluetooth, CD/DVD blocked
2.3.3. Local admin rights blocked
2.3.4. Antivirus & EDR updates pushed automatically, regular patching and updates of systems and other software
2.3.5. Data classification and protection (AIP) enabled
2.3.6. Restricted internet access while in home office/work from home on VPN
2.3.7. Mobile Security
2.3.8. 2FA enabled for Vodafone internet facing apps
2.3.9. Report Phishing feature on Outlook
2.3.10. Data Loss Prevention (DLP) system in place and DLP (Email and End point) in blocking mode
2.3.11. Enhanced DLP controls for Leavers and data transfer via Peer-to-Peer connection being monitored, where allowed by
2.3.12. the labour code or similar
2.3.13. H2H for secure external file sharing
2.3.14. Quarterly review and reconciliation of roles and responsibilities for access (e.g. admin rights)
2.3.15. Bi-annual review and reconciliation of shared and functional accounts
2.3.16. Network Access Control -ISE
2.3.17. Quarterly vulnerability testing,
2.3.18. Security event logging and alarm system in place that can detect personal data breaches

2.4. Digital Sovereignty is important to us; personal data generated in the EEA (European Economic Area) should not leave the EEA and the deemed adequate countries (from time to time) excepting as is necessary to execute the services to the Customers and as agreed with Vodafone.