Data Processing and Transfer Addendum

Version 1.0, effective 1 July 2026.

1 Introduction

1.1 This Data Processing and Transfer Addendum is entered into between the Nokia entity identified in the Nokia Customer Agreement (the "**Nokia**") and the customer (the "**Customer**"), each a **party** and together the **parties**.

1.2 This Data Processing and Transfer Addendum, including its Schedules, (the "**DPA**") form part of the Nokia Customer Agreement and sets out the terms under which Customer will disclose, and Nokia will process Customer Personal Data when providing the Services under the Nokia Customer Agreement. This DPA contains mandatory provisions required by applicable Data Protection Laws for controllers-processors relationship.

1.3 Except as otherwise indicated, terms not defined herein have the meanings set forth in the Nokia Customer Agreement. The schedules are incorporated into and form part of this DPA.

2 Roles and responsibilities

2.1 Customer is the controller or processor of Customer Personal Data and, subject to Clause 2.2, Nokia is, respectively, the processor or sub-processor. This DPA applies only to Nokia's processing of Customer Personal Data as a processor.

2.2 Nokia and its Affiliates may process personal data as a controller only for Legitimate Business Purposes in accordance with Nokia General Privacy Notice.

2.3 Each party shall comply with applicable Data Protection Laws. Schedule 4 sets forth any applicable jurisdiction-specific requirement. Nothing in this DPA relieves either party of its obligations or liabilities under applicable Data Protection Law.

3 Limitations on Use

3.1 Nokia shall process Customer Personal Data on Customer's behalf, to perform the Services, and in accordance with Customer's documented instructions as set in the applicable Quotation and the Nokia Customer Agreement or as otherwise communicated by Customer. If Customer is a processor, such instructions can be based on the instructions of its controller.

3.2 Customer instructs Nokia to process Customer Personal Data for: (i) delivering and maintaining the Services, and this includes: (a) technically improving the functionality of the Services, such as deducting bugs, fixing errors, and troubleshooting, (b) maintaining the Services, including developing and distributing technical updates; and (c) executing Customer's documented instructions. (ii) securing the Services, including by providing security features and services in accordance with Section 6, taking into account the nature of the Services, (iii) providing Customer-requested support and performing related troubleshooting; and (iv) any other purpose approved by Customer in writing.

3.3 If Nokia is unable to materially comply with this DPA, it will inform promptly notify Customer. Customer may then be entitled to suspend the provision of Customer Personal Data until Nokia complies with this DPA and/or terminate this DPA in accordance with its terms.

4 Cooperation and assistance

4.1 Taking into account the nature of the processing and the information available to Nokia, Nokia shall provide reasonable assistance to Customer, to the extent legally permitted, with: (i) any assessment of the impact of processing Customer Personal Data required under applicable Data Protection Laws; and (ii) investigations, inquiries, or requests from competent regulators or law enforcement authorities relating to Customer Personal Data.

4.2 Customer shall use tools made available by Nokia through the Services to manage files or logs containing Customer Personal Data provided to Nokia.

5 Individual rights

5.1 Upon Customer's written request, Nokia shall provide reasonable assistance, using information reasonably available to Nokia, including through appropriate technical and organisational measures, to enable Customer to respond to requests from individuals to exercise their rights under applicable Data Protection Laws.

5.2 If Nokia receives a request relating to Customer Personal Data from an individual exercising rights under applicable Data Protection Laws, Nokia shall, to the extent legally permitted, promptly forward the request to Customer.

6 Security measures

6.1 Taking into account the nature of the processing and the risks to individuals, Nokia shall implement and maintain appropriate technical and organisational measures to protect Customer Personal Data against unauthorised or unlawful processing and of accidental or unlawful loss, alteration, unauthorised disclosure or destruction, or damage, including the Technical and Organizational Measures set out in Schedule 2.

7 Personal data breach

7.1 Nokia shall notify Customer without undue delay after becoming aware of a Personal Data Breach and shall take reasonable steps to investigate and mitigate its effects. Upon Customer's written request, Nokia shall provide reasonable assistance, using information reasonably available to Nokia, to enable Customer to comply with applicable Personal Data Breach notification obligations.

7.2 The notification shall include, to the extent available, the information required by applicable Data Protection Laws, and may be provided in phases as additional information becomes available.

8 Confidentiality and Production Requests

8.1 Nokia shall ensure that persons authorized to process Customer Personal Data are subject to confidentiality obligations or an appropriate statutory duty of confidentiality.

8.2 If Nokia receives any order, demand, warrant, or other document requesting or purporting to compel the production of Customer Personal Data by any competent authority ("**Production Request**"), Nokia shall, to the extent legally permitted, promptly notify Customer and reasonably cooperate with Customer regarding such request.

9 Sub-processors

9.1 Customer generally authorises Nokia to engage sub-processors to process Customer Personal Data. If Nokia engages a sub-processor, Nokia shall: (i) enter into a contract with such sub-processor containing data protection obligations no less protective than these set out in this DPA; (ii) remain responsible, to the extent required by applicable Data Protection Laws, for the acts and omissions of its sub-processor; and (iii) remain the Customer's sole point of contact, except as otherwise expressly provided.

10 International data transfers

10.1 Where Customer Personal Data is subject to transfer restrictions under applicable Data Protection Laws and is transferred between Customer and Nokia, Schedule 5 applies to such Transfers. The parties may rely on Binding Corporate Rule, Standard Contractual Clauses, adequacy decision, or any other valid Transfer mechanism recognized under applicable Data Protection Laws, as further described in Schedule 5. Such Transfers may be carried out using Binding Corporate Rules, standards Contractual Clauses, adequacy decisions, or any other valid Transfer mechanism recognized under applicable Data Protection Laws.

11 Compliance and audit

11.1 Where required by applicable law, Nokia shall, upon Customer's reasonable written request, provide information reasonably necessary to demonstrate compliance with this DPA.

11.2 Customer may audit Nokia's compliance with this DPA, provided that Customer has first reviewed the information, third-party audit reports, security assessments, and certifications made available by Nokia and such materials are sufficient to demonstrate compliance with applicable Data Protection Laws, subject to at least thirty (30) days' prior written notice (unless a shorter period is required by the applicable law), no more than one audit in any twelve(12)-month period, and during normal business hours in a manner that does not unreasonably disrupt Nokia, its customers, or its sub-processors. Customer shall not appoint a Nokia competitor as auditor, and any third-party auditor must be bound by confidentiality obligations acceptable to Nokia. Nothing in this DPA requires Nokia to permit penetration testing.

11.3 Nokia may satisfy its obligations under section 11.2 by providing third-party audit reports, security assessments, or relevant certifications, including ISO 27001 or equivalent certifications.

11.4 Information obtained through an audit may be used solely to verify compliance with this DPA and shall be treated as Confidential Information.

12 Representations and Warranties

12.1 Each party represents and warrants that it has the authority to enter into and perform this DPA.

12.2 Customer represents and warrants that: (i) it is authorized to provide Customer Personal Data to Nokia for the purposes contemplated by this DPA; (ii) its instructions to Nokia comply with applicable Data Protection Laws; and (iii) it has provided all required notices and obtained all required consents and permissions under applicable Data Protection Laws in connection with Nokia's processing of Customer Personal Data.

12.3 Except as expressly provided in this DPA, each party disclaims all warranties, whether express, implied, statutory, or otherwise, including any implied warranties of merchantability, satisfactory quality, fitness for a particular purpose, and non-infringement, to the extent permitted by applicable law.

13 Liability

13.1 The liability provisions of the Nokia Customer Agreement apply to this DPA, except to the extent prohibited by the applicable Data Protection Laws.

13.2 Notwithstanding the forgoing, Nokia shall not be liable for any Losses arising from Customer's breach of this DPA or applicable Data Protection Laws.

14 Consequences of Termination and Expiry

14.1 Upon termination or expiration of the Nokia Customer Agreement, Nokia shall, and shall ensure its sub-processors shall, cease processing Customer Personal Data and, at Customer's election, return or delete (or anonymise) Customer Personal Data to Customer, except to the extent retention is required by applicable law or the data remains in routine backup or archive systems that are not generally accessible except for disaster recovery, legal compliance, or similar purpose.

15 Non-standard Costs

15.1 Customer shall reimburse Nokia for its reasonable costs and third party expenditure incurred in providing assistance and co-operation requested by Customer under this DPA, including in connection with clauses 4 (impact assessments), 5.1 (individual rights requests), 7 (personal data breaches), 4.1 (communications with supervisory authorities), 11.1 (assistance to demonstrate compliance), 11.2 (Customer audits) and 14 (return of Customer Personal Data).

16 Conflicts

16.1 In the event of a conflict between this DPA and the Nokia Customer Agreement regarding the processing of Customer Personal Data, this DPA prevails.

17 Governing Law and Jurisdiction

17.1 The governing law, dispute resolution, and jurisdiction provisions of the Nokia Customer Agreement apply to this DPA.

18 Variation

18.1 Subject to any change control procedure in the Nokia Customer Agreement, any variation of this DPA must be in writing and signed by the parties' authorized representatives.

19 Schedule 1

19.1 Description of processing

Parties and Roles

Data Exporter

Name, address, and contact details: The name and address of Customer, together with the contact details of its relevant contact person, are set out in the Nokia Customer Agreement and/or collected as part of the customer onboarding process.

Role: Customer acts as a Controller in relation to Customer Personal Data processed by Nokia on Customer's behalf and, where applicable, as a Processor acting on behalf of another Controller.

Data Importer

Name, address, and contact details: The Nokia entity identified in the Nokia Customer Agreement. Contact details for privacy-related inquiries are available here.

Role: Nokia acts as a Processor or Subprocessor, as applicable, in relation to Customer Personal Data processed under the Nokia Customer Agreement.

Activities relevant to the transfer: As described in the Nokia Customer Agreement, and this DPA.

Duration

Customer Personal Data will be processed for the duration of the Nokia Customer Agreement and thereafter as required under the PDA or applicable law.

Categories of Individauls

Customer personnel, users, contractors, suppliers, business contacts, and other individuals whose Personal Data is submitted by or on behalf of the Customer.

Categories of Personal Data

Contact information, account and user data, system and device information, IP addresses, communications data, support and troubleshooting data, and other personal Data submitted by or on behalf of the Customer.

Special Categories of Personal Data

The services are not intended for the processing of special categories of Personal Data unless expressly agreed by the parties.

20 Schedule 2

20.1 Technical and Organizational Measures

These Technical and Organisational Measures ("**TOMs**") form part of the DPA and set out the security measures applicable to Customer Personal Data. In the event of a conflict between these TOMs and the Nokia Customer Agreement (including any Quotation or statement of work) or any attachment, these TOMs prevail. TOMs describe Nokia's current security measures and may be updated from time to time, provided that the overall level of protection for Customer Personal Data is not materially reduced.

Security Policies

Nokia shall maintain and implement information security policies and procedures designed to protect Customer Personal Data, including policies relating to security management, security monitoring and response, network security, physical security, access control and identity management, and business continuity and disaster recovery.

Global Access

Unless otherwise agreed by the parties, Nokia may access Customer Personal Data through its global delivery network where reasonably necessary to provide the Services. Any such access and related Transfers shall be subject to the safeguards and transfer mechanisms set out in Schedule 5 and applicable Data Protection Laws.

Responsibilities

Customer remains responsible for Customer-controlled systems. Each party is responsible for the security measures assigned to it under these TOMs with respect to its personnel, sub-contractors, systems, and equipment used in connection with the Services.

Table 1. Communications regarding the day-to-day obligations.

Control		Responsible Parties	
		Nokia	Customer
5.0	**Asset Management**		
5.1	**Asset Inventory**		
5.1.1	Each Party will maintain an inventory of all media on which Customer Personal Data is stored. Access to the inventories of such media will be restricted to the Parties' personnel authorised in writing to have such access.	X	X
5.2	**Data Handling**		
5.2.2	Customers will identify and classify Customer Personal Data and communicate to Nokia if there if Customer Personal Data enters systems of products managed by Nokia or for which Nokia provides Care Services and identify it to allow for access to it to be appropriately restricted through appropriate access controls.		X
5.3	**Information Classification**		
5.3.1	For each covered statement of work, the Customer shall appropriately inform Nokia of the types of Customer Personal Data that Nokia will process. Customer will notify Nokia when Customer Personal Data is being provided and label it clearly and appropriately.		X
6.0	**Human Resources Security**		
6.1	**Training**		
6.1.1	Confidentiality of personnel: Nokia ensures that all personnel understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities are clearly communicated during the pre-employment and/or induction process.	X	
6.1.2	Nokia requires all Nokia project personnel to complete standard Nokia and any Customer provided data protection training.	X	
	Nokia ensures that all personnel are adequately informed about the security controls of the IT system that relate to their everyday work. Personnel involved in the processing of personal data are also properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.	X	
6.1.3	Each Party will inform its personnel about relevant security procedures and their respective roles.	X	X
6.1.4	Each Party will also inform its personnel of possible consequences of breaching the security rules and procedures.	X	X
7.0	**Physical and Environmental Security**		
7.1	**Physical Security**		
7.1.1	The physical perimeter of Nokia's IT system infrastructure is not accessible by non-authorised personnel.	X	
7.1.2	Each Party will only allow authorised individuals to access facilities where information systems that process Customer Personal Data are located.	X	X
7.1.3	All personnel shall be registered and required to carry appropriate identification badges.	X	X
7.2.1	**Protection from Disruptions**		
7.2.2	Each Party will use a variety of industry standard (e.g., ISO 27001, as applicable) systems to protect against loss of data due to power supply failure or line interference.	X	X
7.2.3	Each Party will use industry standard (e.g., ISO 27001, as applicable) processes to delete Customer Personal Data when it is no longer needed.	X	X
8.0	**Communications and Operations Management**		
8.1	**Network Security Management**		
8.1.1	Each Party will maintain Access Control Lists (ACLs) for network devices.	X	X
8.1.2	Network traffic shall pass through firewalls that are monitored and protected by intrusion detection/prevention systems that allow traffic flowing through the firewalls to be logged. Nokia is not responsible for the protection of Firewalls that are not managed by Nokia or its suppliers.	X	X
8.1.3	Access to network devices for administration shall require a minimum of 128-bit encryption.	X	X
8.1.4	Each Party will enable Anti-spoofing filters.	X	X
8.1.5	Network, application, and server authentication passwords will meet each party's Policies.	X	X
8.1.6	Enable Transport Layer Security (TLS) between the Customer and Nokia email domains.	X	X
8.2	**Virtual Private Networks ("VPN").**		

Control		Responsible Parties	
		Nokia	Customer
8.2.1	When remote connectivity to the Nokia network is required for processing of Customer Personal Data and site to site VPN has been agreed upon, customer shall deploy VPN servers with the following or similar capabilities:		X
8.2.2	Connections will be encrypted using a minimum of 128-bit encryption by each party.	X	X
8.2.3	Customer connections to the Nokia Service Locations will only be established using the Nokia VPN servers.	X	X
8.2.4	Split tunnelling shall be disabled by each party.	X	X
8.2.5	Each Party will delete split tunnelling on their client to VPN remote access servers. With the exception of site to site VPNs, each Party will require the use of two-factor authentication on their client to VPN remote access servers.	X	X
8.3	**Vulnerability Scanning**		
8.3.1	Each Party will require the use of two-factor authentication on their client to VPN remote access servers and this does not apply for site-to-site VPN connections. Vulnerability scanning controls should be used by each party on their own network.	X	X
8.3.2	Each Party will have anti-malware controls to help avoid malicious software gaining unauthorised access to Customer Personal Data, including malicious software originating from public networks.	X	X
8.3.3	**Event Logging**. Each Party will log the use of their respective data-processing systems.	X	X
8.3.4	Log files are activated for each system/application used for the processing of personal data. When feasible they include all types of access to data (view, modification, deletion).	X	
8.4	**Media Handling**		
8.4.1	When transferring Customer Personal Data: Nokia will implement a minimum of 128-bit encryption of data unless restricted by local regulations or agreed to by both Parties.	X	
8.4.2	Where commercially practical and as agreed upon by the Data Protection Representatives, the Customer shall implement means such as masking or de-identification of Customer Personal Data prior to providing access to Nokia. The Customer must identify instances where unmasked/unscrambled production data is used outside of production environments before providing Nokia access. If production data is used for testing, compensating controls shall be agreed to and employed.		X
8.5	**Data Deletion and Disposal**		
8.5.1	Upon completion, project team members will return or destroy any Customer Personal Data that is in his or her possession.	X	
8.5.2	Nokia may retain archival copies of records containing Customer Personal Data as reasonably necessary or as part of normal backup processes to verify Nokia's compliance with this DPA only until such backups are routinely overwritten in accordance with Nokia's standard retention and backup procedures. Nokia will identify such data to Customer at the time such archival copies are withheld and shall mask or otherwise redact the Customer Personal Data in those records. Nokia shall not be obligated retain archival copies of Customer Personal Data bases, or other compilations or stores of Customer Personal Data.	X	
8.5.3	Nokia shall destroy hard copies containing Customer Personal Data via shredder or by depositing in a secure destruction bin when no longer required in the performance of the Services.	X	
8.6	**Third Party Service Delivery Management**		
8.6.1	Execute substantially similar contractual terms relating to privacy and security with subcontractors retained to provide the Services.	X	
8.6.2	Maintain commercially reasonable contractual terms relating to privacy and security with enterprise information technology and communications suppliers who are engaged to provide general services to Nokia and are not engaged specifically to provide the Services (e.g., email and telecommunications providers).	X	
8.7	**Back-up**		
8.7.1	Backup and data restore procedures are defined, documented and clearly linked to roles and responsibilities.	X	X
8.7.2	Backups are given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.	X	X
8.7.3	If Nokia provides hosting services for production databases and offsite tape backups are used, then the backups will be encrypted, at a minimum of 256-bit encryption unless there are contradictory legal requirements, at the Customer's expense.	X	X
8.8	**Data Recovery Procedures**		
8.8.1	Each Party will have specific data recovery procedures in place designed to enable the recovery of Customer Personal Data being maintained in its systems.	X	X
8.8.2	Each party will conduct regular software updates and security patches	X	X

Control		Responsible Parties	
		Nokia	Customer
9	**Access Control**		
9.1	**User Access Management**		
9.1.1	Each Party will maintain and update a record of personnel authorised to access Customer Personal Data via that Party's systems.	X	X
9.1.2	The Customer shall use reasonable commercial efforts to restrict Nokia's access to only that Customer Personal Data required for Nokia to perform its obligations under the Agreement.		X
9.1.3	Each Party will implement user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to all Customer systems, Customer Personal Data and all internal applications used during the course of the project. Designate an appropriate authority (as defined by the engagement) to approve creation of new user ID, or elevated level of access for existing ID.	X	X
9.1.4	Each Party will implement an engagement level access control roster capturing the access details for engagement resources, covering type of access, date access granted, and date access revoked for team members.	X	
9.1.5	Nokia will review the access control roster annually, or as otherwise agreed to by the Parties in writing, to confirm that access levels are still appropriate for individual roles and to confirm that access revocations for personnel who departed from the engagement have been processed correctly.	X	
9.1.6	Each Party will revoke access for personnel departing the engagement within 24 hours of departure, or in compliance with contractual obligations, whichever is sooner.	X	X
9.1.7	Where applicable, each Party will provide access for project personnel and other applicable personnel using the concept of Least Privileged Access, meaning individuals are only granted access to those resources and systems that are required to perform their role.	X	X
9.1.8	When applicable, each Party will logically separate access between environments (e.g., development, testing, and production) so that an individual can be granted access to one environment without being able to access others.	X	X
9.1.9	Each Party will provide each individual accessing a system or application with a unique user ID and password. Prohibit user IDs and passwords from being shared.	X	X
9.1.10	Each Party will provide two-factor authentication to access the Customer's internal network environment from non-Customer/non-Nokia locations. An internal network environment generally means the network environment that what would be available if an individual is sitting within the Customer's offices or data centres.	X	X
9.1.11	To the extent possible, the Customer will enable access methods to control offloading, printing, copying, pasting, or other methods of data extraction of Customer Personal Data (e.g., Citrix/VDI/application layer firewall).		X
9.2	**Password Management**		
9.2.1	Each Party will ensure electronic communications of passwords must be encrypted using a minimum of 168-bit encryption.	X	X
9.2.2	Each Party will require initial user passwords to be changed during the first logon and prohibit user IDs and passwords from being shared.	X	X
9.2.3	Where authentication mechanisms are based on passwords, each Party will require that the passwords are renewed regularly.	X	X
9.2.4	When granting access or assigning user roles, the "need-to-know principle" shall be observed in order to limit the number of users having access to personal data only to those who require it for achieving the processing purposes.	X	
9.3	**Network/Communication security**		
9.3.1	Whenever access is performed through the Internet, communication is encrypted through cryptographic protocols.	X	X
9.3.2.	Traffic to and from the IT system is monitored and controlled through Firewalls and Intrusion Detection Systems. No firewalls or IDS can be installed in Nokia's networks.	X	X
10			
10.1	**Encryption**		
10.1.1	Each party will encrypt transmissions of Customer Personal Data between the parties using a minimum of 128-bit encryption.	X	X
10.1.2	Mobile phones and tablets will be protected via a mandatory PIN, require device encryption, and have restrictions on the amount of email that can be stored on the device.	X	
10.1.3	Full hard disk encryption at a minimum of 256-bit encryption on all laptops in use to deliver Services (i.e., Nokia, rental, Customer, subcontractor workstations).	X	X
11	**Information Security Incident Management**		

Control		Responsible Parties	
		Nokia	Customer
11.1	**Security Incident Reporting**		
11.1.1	Personnel will promptly report to a Nokia centralised management response centre any actual or potential security incident that has resulted, or could be reasonably suspected to have resulted, in the loss, misuse or unauthorised acquisition of any Customer Personal Data. (e.g., a lost or stolen laptop).	X	
11.1.2	Each party will identify any additional security incident notification requirements arising from the Agreement and communicate those requirements to project personnel.	X	X
11.1.3	Each Party will maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the process for recovering data.	X	X
11.1.4	Log files are activated for each system/application used for the processing of personal data. When feasible they include all types of access to data (view, modification, deletion).	X	
11.2	**Business Continuity Management**		
11.2.1	Each Party will maintain emergency and contingency plans for the facilities in which the Parties' information systems that process Customer Personal Data are located.	X	X
12	**Security of data at rest**		
12.1	**Server/Database security**		
12.1.1	Database and applications servers are configured to run using a separate account, with minimum OS privileges to function correctly.	X	X
12.1.2	Database and applications servers only process the personal data that are actually needed to process in order to achieve its processing purposes.	X	X
12.2	**Workstation security:**		
12.2.1	Anti-virus applications and detection signatures is configured on a regular basis.	X	X
12.2.2	Users have a software licensing policy and instruct users to not install unauthorised software applications.	X	X
12.2.3	The system has session time-outs when the user has not been active for a certain time period.	X	X
13	**Compliance**		
13.1	**Compliance with Legal Requirements**		
13.1.1	Nokia will not use Customer Personal Data for any other purpose beyond provision of the contracted services, or as required by applicable law.	X	
13.1.2	For each covered statement of work, identify business, operational, and technical requirements that flow from data privacy laws that Customer is subject to as part of the business process design and/or requirements definition.		X
13.1.3	Comply with controls arising out of applicable data privacy laws as they apply to Nokia as a service provider.	X	

21 Schedule 3

21.1 Definitions

In this DPA:

"**Adequacy Decision**" means a decision, regulation or other legal mechanism recognizing a jurisdiction as providing an adequate level of protection of Personal Data;

"**Affiliate**" means with respect to any entity that Controls, is controlled by, or is under common Control with a party;

"**Confidential Information**" means any non-public information disclosed, by whatever means, by one party to the other that is identified as confidential or reasonably should be understood to be confidential, including the terms of the Nokia Customer Agreement;

"**Control**" means direct or indirect ownership of more than fifty percent (50%) of the voting interest, capital, or similar right of ownership of that person or the legal power to direct or cause the direction of the general management and policies of that person whether through the ownership of voting capital, by contract or otherwise, and "**Controls**" and "**Controlled**" shall be interpreted accordingly;

"**Customer Personal Data**" means personal data for which Customer is a controller or processor that is: (i) supplied by or on behalf of Customer to Nokia (including where Nokia has access to personal data held by Customer or on its behalf), or which Nokia collects or otherwise processes on behalf of Customer; and (ii) processed by Nokia under or in connection with providing the Services or performing an obligation under the Nokia Customer Agreement;

"**Data Protection Laws**" means any law, enactment, regulation or order concerning the processing of data relating to living persons including each to the extent applicable to the activities or obligations of the parties under or pursuant to this DPA;

"**EEA**" means the European Economic Area;

"**European Data Protection Laws**" means the applicable Data Protection Laws of the European Union, including the General Data Protection Regulation 2016/679;

"**Group**" means, a party and its Affiliates;

"**Legitimate Business Purposes**" means Nokia's legitimate internal business purposes, including billing and account management, customer management, training, receiving and using feedback, developing and improving products and services using aggregated data, complying with legal obligations, asserting or defending legal claims, detecting and preventing abuse, fraud, cybercrime, and security threats, internal audit, financial reporting, business planning, and improving and optimizing the Services.

"**Loss**" means any loss, damage, cost, reasonable fee, expense or other liability (including legal and other professional fees) and **Losses** shall be interpreted accordingly;

"**Model Contract**" means any or all model contract language dictated by a particular jurisdiction and determined to provide a sufficient legal basis for restricted Transfers by a competent authority with jurisdiction over the Transfer, including where relevant the EU SCCs, UK SCCs Addendum, Argentine Model Clauses and ADGM Data Transfer Agreement.

"**Nokia P-BCR**" means the Nokia Binding Corporate Rules for Processors, available here, which are approved by the supervisory authority in the (i) EU and (ii) Finland.

"**Nokia Group**" means the Nokia and each member of its Group;

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise processed by the Nokia;

"**Security Measures**" means the Technical and Organizational measures outlined in Schedule 2;

"**Services**" means the services provided under the Nokia Customer Agreement;

"**Supervisory Authority**" means the relevant competent authority responsible for data privacy and protection where the Customer or Nokia is established;

"**Transfer**" means the access by, transfer or delivery to or disclosure of personal data to a person, entity or system located in a country or jurisdiction other than the country or jurisdiction from which the personal data originated.

"**UK SCCs Addendum**" means the international data transfer addendum to the EU Commission standard contractual clauses issued by the UK ICO under section 119A of the Data Protection Act 2018 valid from 21 March 2022 (as amended, superseded or replaced from time to time) incorporating the relevant EU SCCs;

"**UK GDPR**" means the General Data Protection Regulation 2016/679 as incorporated into UK law by virtue of the European Union (Withdrawal) Act 2018; and

"**UK ICO**" means the United Kingdom Information Commissioner's Office.

"**controller**", "**personal data**", "**processor**" and "**processing**" shall have the meaning given to them in Data Protection Laws.

Any reference, express or implied, to an enactment (which includes any legislation in any jurisdiction)

includes, except to the extent that the contrary intention appears: that enactment as amended, extended or applied by or under any other enactment (before, on or after execution of this DPA); any enactment which that enactment re enacts (with or without modification); any subordinate legislation made (before, on or after execution of this DPA) under that enactment, including (where applicable) that enactment as amended, extended or applied, or under any enactment which it re-enacts.

22 Schedule 4

22.1 Jurisdiction Specific Provisions.

The following provisions apply only to Customer Personal Data subject to the applicable Data Protection Laws of the relevant jurisdiction and where Customer is located in that Jurisdiction.

Australia.

(a) If, subject to clause 8, Nokia uses or discloses Customer Personal Data an enforcement activity, Nokia shall maintain a written record of such use or disclosure and, unless prohibited by applicable law, provide a copy of to Customer upon request.

(b) For purposes of this DPA, Nokia is deemed aware of a Personal Data Breach when it has reasonable grounds to suspect that a Personal Data Breach has occurred.

California

If Customer Personal Data is subject to Consumer Privacy Act ("CCPA") Provisions:

(a) Nokia shall provide the level of privacy protection required by the CCPA and notify Customer if it determines it can no longer comply with its obligations under the CCPA.

(b) Customer may, upon prior notice, take reasonable and appropriate steps to verify Nokia's compliance with the CCPA and to stop and remediate unauthorised use of Customer Personal Data. California residents with the same data protection rights under CCPA as provided by Customer.

(c) Nokia shall not (i) sell of share Customer Personal Data; (ii) process Customer Personal Data for any purpose other than providing the Services or otherwise permitted by applicable law; or (ii) combine Customer Personal Data with personal data obtained from other sources expect as permitted by the CCPA.

(d) Where Customer authorizes de-identified, anonymized, or aggregated processing, Nokia shall maintain such data in de-identified, anonymised, or aggregated from and shall not attempt to re-identify it.

United States

Except as provided under the California CCPA provisions above, where Customer Personal Data is subject to applicable U.S. state privacy laws, Nokia shall process such Customer Personal Data solely on Customer's behalf and for the purposes set out in the Nokia Customer Agreement and this DPA. Nokia shall not retain, use or disclose or combine such Customer Personal Data except as permitted by applicable law or the Nokia Customer Agreement.

Indonesia

In the event of a Personal Data Breach, Nokia shall include available information regarding the cause of the breach in its notification to Customer. Where required by applicable law, Nokia may request Customer to acknowledge receipt of such notification.

Israel

(a) Nokia shall not Transfer Customer Personal Data outside Israel except to processors bound by written agreements containing data protection obligations required under applicable Israeli Data Protection Law.

(b) Where Nokia processes restricted data, Nokia shall comply with applicable Israeli security requirements, including: (i) Customer's information security policies to the extent provided by Customer; and (ii) applicable obligations under the Protection of Privacy Regulations (information Security) 2017.

(c) Where required by applicable law, printouts containing restricted data shall bear confidentiality notices.

Qatar

For purposes of this DPA, a Personal Data Breach includes any event where Nokia reasonably believes: (i) its information security program has been breached; or (ii) a risk threatening personal data has arisen.

23 Schedule 5

23.1 International Data Transfers

EEA and Switzerland

Restricted Transfers of Customer Personal Data subject to European and Swiss Data Protection Laws shall be carried out on the basis of the Nokia P-BCRs, available here which are incorporated into this DPA by reference.

Nokia shall use commercially reasonable efforts to maintain authorization of the Nokia P-BCRs and shall

notify Customer of any material change affecting such authorization.

Where the Nokia P-BCRs are unavailable or no longer provide a valid Transfer mechanism under applicable law, Nokia may rely on another valid transfer mechanism recognized under applicable Data Protection Laws

Adopting Countries

Restricted Transfers of Customer Personal Data subject to the Data Protection Laws of a country outside the EEA that has approved the use of the EU Standard Contractual Clauses (each, an "**Adopting Country**"), the applicable module of the EU Standard Contractual Clauses ("**EU SCCs**") is incorporated into and forms part of this DPA. Furthermore, the parties agree that:

(a) Module 2 (Controller-to-Processor) applies where Customer acts as a controller and Nokia acts as a processor.
(b) Module 3 (Processor-to-Processor) applies where Customer acts as a processor and Nokia acts as a sub-processor.
(c) The EU SCCs do not apply to the extent a Transfer is covered by an Adequacy Decision or the Nokia P-BCRs.
(d) For purposes of the EU SCCs, the parties agree that: (i) Clause 7 (Docking Clause) applies; (ii) Clause 9 of the EU SCCs under Option 2, and changes to the list of subprocessors shall be communicated thirty (30) days in advance; (iii) Clause 11 of the EU SCCs, the optional language does not apply; and (iv) Annexes I.A, I.B and II of the EU SCCs shall be deemed completed by Schedules 1 and 2 of this DPA, respectively.
(e) Unless otherwise required under the applicable Data Protection Laws of the Adopting Country: (i) references to the "EU," "Union," "Member State," and EU law shall be interpreted as references to the Adopting Country and its applicable laws; (ii) Clause 17 shall be governed by the laws of the Adopting Country; (iii) Clause 18 disputes shall be resolved by the courts of the Adopting Country; and (iv) Annex I.C shall identify the competent supervisory authority of the Adopting Country.

United Kingdom

Restricted Transfers of Customer Personal Data that are subject to the UK GDPR shall be carried out on the basis of the UK SCCs Addendum, which is incorporated into and form part of this DPA. For the purposes of the UK SCCs Addendum, the parties agree that:

(a) Table 1 of the UK SCCs Addendum, the parties, and their details, and their respective roles shall be as set out in Schedule 1;
(b) Tables 2 and 3 of the UK SCCs Addendum, the applicable module of the EU SCCs shall apply and shall be completed using the information set out in Schedules 1 and 2; and
(c) For the purposes of Table 4 of the UK SCCs Addendum, neither party may terminate the UK SCCs Addendum.

Argentina

Restricted Transfers of Customer Data Protection subject to the Data Protection Laws of Argentina and Transferred to Nokia in a jurisdiction that is not recognized by Argentina as providing adequate protection, the Argentine Model Clauses (Controller to Processor), available at http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm, are incorporated into and from part of this DPA. Schedule 1 shall be deemed to complete the applicable annexes of the Argentine Model Clauses.

Abu Dhabi Global Market Free Zone ("ADGM")

Restricted Transfers of Customer Personal Data subject to Data Protection Laws of ADGM shall be carried out on the basis of the appropriate module of the ADGM Data Transfer Agreement (Controller to Processor or Processor to Processor, as the case may be), hereby incorporated by reference to this DPA, together with Schedule 1.

A signature to the Nokia Customer Agreement shall be considered to also be a signature to the applicable Model Contracts incorporated by reference in this Schedule 5.

Alternative Transfer Mechanism

If, during the term of this DPA:

(a) the EU SCC, the UK Addendum, or any other applicable Model Contract is replaced by a successor Transfer mechanism approved by the relevant competent authority, the replacement Transfer mechanism shall apply and be incorporated into this DPA;
(b) a Model Contract (or its successor) is invalidated or otherwise ceases to provide a lawful transfer mechanism, Customer and Nokia shall cooperate in good faith to implement an alternative transfer mechanism in accordance with applicable Data Protection Law, as soon as reasonably practicable;
(c) a Transfer becomes subject to an Adequacy Decision, the applicable Model Contract shall cease to apply to that Transfers;
(d) a Transfer becomes covered by Binding Corporate Rules, the applicable Model Contract shall cease to apply to that Transfers and the Binding Corporate Rules shall apply instead; or
(e) an Adequacy Decision is invalidated or Binding Corporate Rules authorization is revoked, the applicable Model Contract shall apply to the affected Transfers from the date of such invalidation or revocation.