



Supplier Data Processing Requirements

Date: 08/25/2023
Approved by: VP, Chief Privacy Officer

SUPPLIER DATA PROCESSING REQUIREMENTS

1 HERE'S THE DEAL.

T-Mobile's Supplier Data Processing Requirements ("**DPR**") defines the mandatory data privacy requirements for Suppliers that Process T-Mobile's Personal Data in connection with the Supplier's performance under the terms of its agreements with T-Mobile (e.g., Contracts and Amendments, Main Agreement, Statement of Work, Scope of Work, Purchase/Change Order, etc.).¹ As defined below, "Process" includes any access Supplier has or is granted to T-Mobile's Personal Data.

Strict adherence to the DPR is necessary to ensure Supplier's compliance with: (1) applicable federal and state privacy laws², and (2) T-Mobile's privacy policies.

The requirements described in this DPR are in addition to any supplemental data processing and security terms in Supplier's contract with T-Mobile. Additional engagement-specific requirements may be required depending on the services or products provided. Such additional requirements will be set forth in a written agreement between Supplier and T-Mobile. If the requirements described in this DPR conflict with the requirements in an existing contract between Supplier and T-Mobile, the requirements described in this DPR take precedence, unless the contract expressly supersedes specific DPR requirements. This DPR forms an integral part of Supplier's obligations under its contract with T-Mobile, along with the parties' Main Agreement, Amendments, SOWs, POs, the T-Mobile Supplier Code of Conduct, T-Mobile's Third-Party Information Security Policy, all other applicable T-Mobile policies, and all Applicable Laws (collectively, these constitute T-Mobile and Supplier's "**Agreement**").

2 WHAT'S IN SCOPE?

The requirements in this DPR apply to all T-Mobile Suppliers who Process **Personal Data**.

3 DATA PROCESSING REQUIREMENTS.

3.1 Limitation of Processing. Supplier will handle Personal Data in compliance with this DPR, the data processing and security terms in Supplier's Agreement with T-Mobile, and Applicable Laws.

Supplier may only Process Personal Data for the following limited and specified purposes, and solely to the extent necessary: (a) to provide services or deliverables and to fulfill a SOW in accordance with the purpose for Processing as set forth in the SOW, (b) to deploy, maintain, or repair the equipment and/or systems designated in a SOW, or (c) otherwise to perform its business purposes and obligations as documented under the Agreement ("Business Purposes"). **Supplier may not Process Personal Data for any other purpose not expressly specified in the Agreement**, including marketing to or contacting persons identifiable from such Personal Data (alone or in combination with other data), customizing, training, or otherwise improving any artificial intelligence ("AI") model, data mining, data analytics, or distribution of the information to any third parties, including subcontractors. Supplier will not retain, use, or disclose the Personal Data that it collects pursuant to this DPR outside the direct business relationship between T-Mobile and the Supplier or for any commercial purpose other than the specific Business Purposes identified in the Agreement. Supplier will not combine Personal Data it obtains from, or on behalf of, T-Mobile with personal data it receives from, or on behalf of, a third-party, or personal data it collects from its own

¹ Capitalized terms are defined in Section 4 of this DPR.

² The DPR's legal requirements are aggregated from individual state laws (e.g., California Consumer Privacy Act, as amended, Virginia Consumer Data Protection Act, Colorado Privacy Act, Connecticut Data Privacy Act, etc.). These requirements will be updated as necessary to incorporate new laws as they become effective to ensure ongoing legal compliance.

interactions with T-Mobile customers or other individuals. All Personal Data, and data, information, analyses, and models developed based on the Personal Data (including derivative data, De-Identified Data, or aggregated data), will be Confidential Information. Supplier agrees that except as strictly necessary to perform under the terms of Supplier's Agreement, Supplier will have no rights, licenses, or permissions to use, store, or retain Personal Data or Confidential Information, or to create derivative, de-identified, or aggregate data from the Personal Data or Confidential Information. The nature of the Processing, the type of Personal Data subject to Processing, and the duration of Processing are stated in the SOW.

3.2 No Third-Party Sales or Sharing of Personal Data. Except as expressly permitted by T-Mobile in writing, neither Supplier nor any of its subcontractors may sell, rent, release, transfer, share, disclose, disseminate, or otherwise make available in any form or for any reason, Personal Data to any third-party.

3.3 Data Return and Deletion. Promptly, (i) upon the termination or expiration of the Agreement, or (ii) at T-Mobile's request, Supplier will return all Personal Data and De-Identified Data Processed by Supplier or Supplier's Personnel or subcontractors in a form and format acceptable to T-Mobile and delete all Personal Data and De-Identified Data including copies (unless this requirement conflicts with Applicable Law or T-Mobile provides written authorization to retain De-Identified Data). Any retained Personal Data will remain under the protections of this DPR until its deletion.

3.4 Individual Requests and Supplier Assistance. Supplier and its subcontractors will, through appropriate technical and organizational measures, assist T-Mobile in fulfilling its obligations to respond to individual requests, including requests to access, modify, delete, or correct Personal Data, as described in T-Mobile's Privacy Notice located at <https://www.t-mobile.com/privacy-center/privacy-notices/t-mobile-privacy-notice.html>. Supplier's assistance may include the provision of all necessary Personal Data in Supplier's or its subcontractor's possession obtained or created in the performance of Supplier's Agreement with T-Mobile, the correction of inaccurate Personal Data, and/or the enablement of T-Mobile to do the same.

Supplier will immediately notify T-Mobile in writing (via email to privacy@t-mobile.com) regarding: (a) any inquiry or request received by Supplier or its subcontractors from a consumer regarding services provided under the Agreement relating to, among other things, accessing, modifying, deleting, or correcting Personal Data, or (b) any consumer complaint received by Supplier or its subcontractors relating to Personal Data. Supplier will not reply to any such inquiry other than to direct the individual to T-Mobile, and Supplier will promptly comply and fully cooperate with all directions from T-Mobile with respect to any such inquiry or complaint.

3.5 Third Party Legal Process or Requests. If Supplier receives a legal demand or other request for release of Personal Data, Supplier will give prompt, written notice to T-Mobile (via email to VendorNotifications@T-Mobile.com). Prior to providing any Personal Data, Supplier will give T-Mobile the opportunity to seek a protective order or other appropriate relief at T-Mobile's sole cost and expense. Supplier agrees that it will not release Personal Data to any government, entity, or individual except when legally required. If T-Mobile does not seek a protective order or other appropriate relief, Supplier will coordinate and cooperate with T-Mobile with respect to the production and delivery of Personal Data to ensure compliance with all governing laws and T-Mobile policies. If Applicable Law prohibits Supplier from providing notice to T-Mobile of a legal demand for Personal Data, Supplier will abide by all federal and state law governing release of such Personal Data.

Unless prohibited by an Applicable Law or court order, Supplier will promptly notify T-Mobile in writing (via email to VendorNotifications@T-Mobile.com) of any request by a foreign government, entity, or person for access to Personal Data or information regarding legal process or electronic surveillance activities related to T-Mobile end users.

3.6 De-Identified Data. Supplier represents and warrants that it: (a) will not re-identify or attempt to re-identify any De-identified Data with any Personal Data, or otherwise perform functions that would associate De-identified Data with any individual, (b) has implemented reasonable measures, including technical and business Safeguards that prohibit the re-identification of De-Identified Data and prevent inadvertent or unauthorized release of De-Identified Data, (c) has publicly committed (e.g., in privacy notices) to maintain and use the De-Identified Data only in de-identified form, and (d) will contractually commit any of Supplier's Personnel or subcontractors with access to De-Identified Data to do the same.

De-Identified Data is Confidential Information, but except as addressed in Section 3.3 and this Section 3.6, De-Identified Data is not subject to the requirements regarding Personal Data set forth in this DPR.

3.7 Engaging Subcontractors. Supplier will not permit the Processing of Personal Data by a subcontractor without T-Mobile's prior written consent. Supplier will submit all requests to use a subcontractor to VendorNotifications@T-Mobile.com and include the proposed subcontractor's: (i) full entity name, (ii) address, (iii) point of contact name and email address, and (iv) scope of Services to be performed and Deliverables to be provided. Supplier's requests for approval do not constitute T-Mobile's consent. T-Mobile will notify Supplier of its decision and any conditions or restrictions by reply email to Supplier's request. Prior to any Processing of Personal Data by a subcontractor, Supplier and subcontractor will have entered into a written agreement that is at least as restrictive as T-Mobile's Privacy and cybersecurity requirements, including this DPR, T-Mobile's Third-Party Information Security Policy, and all other relevant data protection and security terms of Supplier's Agreement with T-Mobile. Supplier is responsible for the subcontractor with respect to the Processing of Personal Data under the Agreement and will reasonably assess the subcontractor's compliance abilities and determine that the subcontractor can meet all of Supplier's obligations for T-Mobile Personal Data throughout the duration of the engagement.

3.8 Duty of Confidentiality. Supplier, subcontractors, and each person Processing Personal Data is subject to a duty of confidentiality with respect to the data.

3.9 Notices and Disclosures. If Supplier obtains Personal Data directly from individuals on behalf of T-Mobile in performance of the Agreement, Supplier will, if applicable: (a) obtain consent and/or authorization to share or receive Personal Data from each individual as required by Applicable Laws, (b) promptly notify T-Mobile of any withdrawal of such consent or authorization, and (c) provide all notices and disclosures as required by Applicable Laws.

3.10 Data Rights and AI. To the extent the services or deliverables provided under Supplier's Agreement includes the Processing of data for machine learning, algorithmic calculations, or other forms of AI or AI tools to be used by T-Mobile, Supplier warrants that: (i) it has legal rights and any required consents to use such data for these purposes; and ii) Supplier's AI Processing and AI tools have been evaluated and, to the extent possible, corrected to eliminate or minimize risks of discriminatory bias.

3.11 Compliance. Without limiting any of T-Mobile's existing audit rights under the Agreement, and as mandated by certain state laws, Supplier will allow T-Mobile to take reasonable and appropriate steps to ensure that Supplier uses the Personal Data it received from or on behalf of T-Mobile in compliance with the Agreement and Applicable Laws, including: (a) consenting to any legally permitted or mandated audits by T-Mobile regarding Supplier's Processing of Personal Data, and (b) making available to T-Mobile all information necessary to demonstrate compliance with this DPR, the Agreement and Applicable Laws. Supplier will allow T-Mobile, upon notice, to take reasonable steps to stop and remediate any unauthorized use of Personal Data. Supplier will provide any information and assistance necessary for T-Mobile to conduct privacy risk assessments as required by Applicable Laws.

3.12 Certification. By entering into any agreement with T-Mobile pursuant to which Supplier will Process Personal Data, Supplier certifies that, as required by the California Consumer Privacy Act or any other Applicable Law requiring a similar attestation: (a) Supplier understands the Personal Data use and sharing limitations in this DPR, (b) Supplier is acting as a Service Provider (or analogous term, such as Processor), Contractor, or Third Party to T-Mobile under this DPR and the Agreement and (c) Supplier will comply with all requirements regarding the Processing of Personal Data set out in this DPR, the Agreement, and under Applicable Law, including by providing the same level of privacy protection as required of businesses by the CCPA.

4 DEFINITIONS.

For purposes of the DPR, the following definitions apply. Capitalized terms not otherwise defined in this DPR have the meaning set out in Supplier's Main Agreement with T-Mobile or Applicable Law. Lists of examples following "including," "such as," "e.g.," "for example" or the like used throughout this DPR are interpreted to include "without limitation" or "but not limited to" unless qualified by words such as "only" or "solely." Where Applicable Law requires a different definition of these terms, the definition provided by Applicable Law will govern.

"Agreement" means, collectively, the parties' Main Agreement, Amendments, SOWs, POs, this DPR, the T-Mobile Supplier Code of Conduct, T-Mobile's Third-Party Information Security Policy, all other applicable T-Mobile Policies, and all Applicable Laws.

“Applicable Law” means all international, federal, state and local laws, ordinances, codes, rules, regulations, and orders in effect that are applicable to the parties and to performance under the Supplier’s Agreement with T-Mobile including the California Consumer Privacy Act, as amended.

“Confidential Information” means the terms of this Agreement, any Order, and all non-public information or materials, disclosed before or after the Effective Date, that are marked as confidential, orally described as confidential, or should reasonably be understood to be confidential, including information about T-Mobile’s network, technical, financial, and customer information, but excluding anything that: (a) was rightfully known to the receiving party prior to the Effective Date without any confidentiality obligation, (b) is or becomes publicly known through no wrongful act of the receiving party, (c) was rightfully received from a third party without any confidentiality obligation to that third party, (d) was free of confidentiality restrictions by agreement of the disclosing party; or (e) was independently developed by the receiving party without using any of the other party’s information; provided, however, Personal Data – even if derived from the sources listed in (a) through (e) above – will remain Confidential Information and the terms in the Agreement governing Confidential Information will apply.

“De-Identified Data” means data obtained from T-Mobile, on T-Mobile’s behalf, or generated by T-Mobile customers, consumers, or employees that cannot reasonably be used to infer information about, or otherwise be associated with or linked to any individual person, household, device, or T-Mobile account. Data that is readable only with a key or other technical measure is not De-Identified Data if Supplier has access to the associated key or measure. If De-Identified Data is Confidential Information, then the terms in the Agreement governing Confidential Information shall apply.

“Personal Data” means any data obtained by Supplier from T-Mobile, on T-Mobile’s behalf, or generated by a T-Mobile customer, consumer, or employee: (a) that is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with an identified or identifiable individual, household, device, or T-Mobile account, (b) that is ‘personal information’, ‘personal data’, or analogous variations of such terms under Applicable Law related to privacy, data security, or protection of information about individuals, or (c) linked to, associated with, or combined with data identified in subsections (a) or (b), including identification numbers, location data, online identifiers, any one or more factors specific to a person’s physical, physiological, genetic, mental, economic, cultural, national or social identity, a person’s name, signature, address, telephone number, email address, employee identification number, Social Security number, driver’s license number, other government-issued identification number, financial information (including account numbers, credit or debit card number, credit report information, income information, password, PIN, account credentials, etc.), biometric data, medical or health data, answers to security questions, or any other personal or account authentication information.

“Personnel” means employees, subcontractors, independent contractors, agents, and other representatives.

“Process” or “Processing” or derivatives means any operation or set of operations performed on data or on sets of data, including by automated or manual means, such as collection, accessing, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure, destruction, including any new data created or resulting from this process or processing.

“Safeguards” means administrative, technical and/or physical measures to identify, assess and protect against any reasonably foreseeable anticipated or actual threats or hazards (whether internal or external) to the security or integrity of information (including threats of loss, theft, unauthorized access, use, disclosure or other unauthorized processing of information or any failure of security controls protecting Confidential Information), whether contained in tangible or intangible records.

“SOW(s)” means, as applicable, any of the following, a: (a) Statement of Work; (b) Master Statement of Work; (c) Order for Software; (d) Order for Cloud Services; (e) Project Amendment; (f) a Purchase Order; (g) Change Order, or (h) any other written agreement signed by the parties’ authorized representatives to procure Services or Deliverables under the Supplier’s Agreement with T-Mobile.

“Supplier” means for purposes of this DPR any entity that Processes T-Mobile’s Personal Data in connection with that entity’s performance under the terms of its Agreement with T-Mobile. For purposes of this DPR, “Supplier” includes Service Provider, Contractor, or Third Party as those terms are defined in the California Consumer Privacy Act, as amended, and Processor as that term is defined in Applicable Laws, as context requires.



5 CONTINUOUS ASSESSMENT; NOTICE OF NON-COMPLIANCE.

Supplier must continuously reassess its compliance with this DPR and promptly notify T-Mobile at VendorNotifications@T-Mobile.com following Supplier's determination that it cannot or will no longer be able to meet its obligations under this DPR, Supplier's Agreement with T-Mobile, or Applicable Laws.

6 MORE INFO

Additional T-Mobile Supplier policies, including the T-Mobile Third Party Information Security Policy and Supplier Code of Conduct, can be found online at <https://www.t-mobile.com/our-story/working-together/suppliers/supplier-code-of-conduct>.