PwC Data Protection Addendum

pwc

Table of Contents

Service provider agrees to comply with all of the terms of this Data Protection Schedule ("DPA"), with respect to any and all PwC personal data processed in the course of providing the Services.

1. Definitions

1.1 The following terms used in this DPA have the meanings below:

Agreement	means the agreement that is signed between the Controller and the Service Provider.
Controller	means the PwC Network Firm or Firms on whose behalf Service Provider processes personal data under the agreement.
Data protection laws	means a) all statutes, statutory instruments, regulations, by-laws, ordinances or subordinate legislation, including but not limited to the General Data Protection Regulation (GDPR) b) the common law and law of equity c) the Middle East laws and regulations d) any binding court order or judgement e) any guidance, policy or standard which, in each case, is enforceable by law or f) any direction or order that is legally binding and issued by a supervisory authority, insofar as applicable to a party and relating to the protection or security of personal data
Data subject	means the natural living person that is the subject of PwC personal data
EEA	means the member states of the European Union, Iceland, Liechtenstein, Norway and Switzerland.
European Commission Model Contractual Clauses	means the standard contractual clauses approved by the European Commission for transfers of personal data to processors established in third countries in decision 2010/87/EU or its superseding instrument
DIFC Standard Contractual Clauses	means the standard contractual clauses as referred to in the DIFC data protection law No.5 of 2020 (as may be amended)
KSA PDPL Standard Contractual Clauses	means the standard contractual clauses provided by the SDAIA in accordance with the Personal Data Protection Law issued pursuant to Royal Decree No. (M/19) dated 16/09/2021 G and amended pursuant to Royal Decree No. (M/148) dated 27/03/2023.
ADGM Standard Contractual Clauses	Means the standard contractual clauses as referred to in the ADGM Data Protection Regulations 2021 (as may be amended)
Business days	means working days of the country where Service Provider is located
Good industry practice	means the exercise of at least the skill, care, prudence and efficiency which would reasonably be expected for a leading provider of services the same as or similar to the services provided under this agreement

Personal data	means any information, including information in electronic form, relating to a living person who can be identified (a) from those data or (b) from those data and the use of additional information, taking into account all means reasonably likely to be used by anyone to identify the person directly or indirectly and includes, without limitation, first and last names, ID numbers, including government-issued identifiers, personal dates such as birth dates, email addresses, location data, internet protocol address or other online identifiers and information concerning race, ethnicity or mental or physical health. For clarity, personal data includes personal data that is publicly available and excludes personal data that has been anonymised so it's no longer possible to re-identify a data subject from the information, taking into account all means likely reasonably to be used by Service Provider or anyone else to re-identify them
Personnel	means any individual involved in the delivery of the services who is an employee, agent, partner, member or officer of Service Provider, including contingent workers
Processing	means any operation or set of operations performed on personal data, whether or not by automated means, such as accessing, collection, downloading, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction
PwC personal data	means any personal data submitted by PwC or other PwC Network Firms to Service Provider or that is otherwise processed by Service Provider on behalf of PwC or other PwC Network Firms in the course of providing the services
PwC Network Firm	means the PwC contracting entity as set out in the Agreement
Services	means the services as set out in the Agreement
Service Provider	means the Party that will provide Services to the Controller under the Agreement
Sub- processor	means anyone engaged by Service Provider to perform processing that Service Provider performs on behalf of PwC or any PwC Network Firm
Supervisory authority	means any person or body having regulatory, supervisory, administrative or governmental authority over all or any part of Service Provider or the PwC Network. For avoidance of doubt, this includes successors to any person or body that would be considered to be a supervisory authority at the date of this agreement

2. Obligation to comply with Data protection laws

2.1 Each party must comply with obligations of Data protection laws that apply to it, including the Middle East data protection laws, and to the Services and to the terms of this DPA. The Parties agree that, for the personal Data, PwC shall be the Data Controller and the Service Provider shall be the Data Processor.

3. Scope of processing and controller's obligations

3.1 For the execution of Services, Controller undertakes to limit the personal data provided to Service Provider to what is necessary for the provision of the Services. For avoidance of doubt, the obligations of this DPA apply to all personal data submitted by PwC or any PwC Network Firm to Service Provider, or otherwise processed by Service Provider on behalf of PwC or any PwC Network Firm, as part of the Services.

4. Service provider's obligations

4.1 The Service Provider shall be liable to comply with the terms of this DPA and will ensure that its personnel, staff, employees, partner or any other person working for or on behalf of the Service Provider will comply with this DPA as per the applicable Middle East data protection laws.

4.2 Service Provider must process PwC personal data solely (i) as necessary to provide the Services that are the subject matter of this Agreement on behalf of PwC or PwC Network Firms or (ii) as necessary and as required by laws applying to Service Provider. Service Provider must not process PwC's personal data for any other reason without PwC's prior written authorization unless the law requiring such Processing prohibits Supplier from notifying PwC, in which case it shall notify PwC as soon as that law permits it to do so. Controller's instructions to Service Provider regarding the processing of PwC's personal data are set forth in this DPA Any additional or modified instructions must be mutually agreed in writing.

4.3 Service Provider must immediately notify PwC of any change to the Services which will prevent Service Provider from complying with the obligations of this DPA or Data protection laws. PwC may, upon notice, take reasonable and appropriate steps to stop and remediate any unauthorized Processing of Protected Personal Data.

4.4 Service Provider must immediately notify PwC (unless legally prohibited) of any communication relating to PwC personal data from any law enforcement, supervisory authority or other government agency. Service Provider must cooperate fully with PwC in relation to such communications and where legally permitted must delay disclosure of PwC personal data to enable PwC to investigate and determine its response.

4.5 Service Provider must inform PwC immediately in writing if, in its opinion, an instruction under clause 4.20 infringes any data protection law (such as EEA, UK, DIFC, ADGM, Jordan,Bahrain, Oman, KSA, Qatar and QFC).

4.6 Service Provider must restrict access to PwC personal data within Service Provider's organisation to personnel who require access to PwC personal data to perform the Services and who are under binding obligations to maintain the confidentiality and security of the information.

4.7 Service Provider must comply with the data security measures described in Service Provider Information Security Controls (e-link) for as long as it has PwC personal data in its possession or control. Service Provider must apply and maintain technical and organisational measures over and above those in Service Provider Information Security Requirements (e-link) to ensure a level of security appropriate to the risks. In determining such additional measures, Service Provider must take into account the nature and volume of personal data processed, the risks for data subjects including the risks presented by unauthorised processing, the state of current technology and the costs of implementation. Service Provider is obligated to apply the following measures where appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident; and

d) a process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational security measures.

4.8 If Service Provider and/or sub-processor processes PwC personal data originating in a jurisdiction that imposes restrictions over transferring personal data (such as EEA, UK, DIFC, ADGM, Bahrain, Oman, KSA, Qatar and QFC) or in any country, territory or sector in circumstances that do not provide an adequate level of protection for personal data according to

the laws of the aforementioned jurisdictions, Service Provider must comply with all of the data importer obligations as set out in the laws of the aforementioned jurisdictions (including without limitation the EU Model Contractual Clauses; the DIFC Standard Contractual Clauses, ADGM Standard Contractual Clauses and KSA PDPL Standard Contractual Clauses where and when applicable) or their superseding instruments, including the third party beneficiary rights afforded to data subjects by those laws . All such obligations are fully incorporated into this Agreement by this reference.

4.9 Service Provider may not engage sub-processors in connection with the Services without PwC's prior written consent. Using sub-processors does not release Service Provider from its obligations under this DPA and Service Provider remains primarily and fully liable for any failure of its sub-processors to comply with the obligations of this DPA.

4.10 Service Provider must notify PwC of all sub-processors engaged at the effective date of this agreement and must thereafter notify PwC at least 30 days before appointing a new subprocessor. Such notice shall (a) be sent to mer_me_data_protection_management@pwc.com; and (b) shall provide PwC with the information necessary to enable it to adequately assess such proposed new Sub-Processor (including, at a minimum, its name, location, and a description of the anticipated Processing activities) and exercise its right to object. PwC may raise reasonable objections to a new sub-processor in which case the parties will negotiate to reach a mutually acceptable solution. If a mutually acceptable solution is not reached within thirty calendar days of PwC raising the objection, PwC reserves the right to terminate the Services without penalty in accordance with the termination provisions of the agreement.

4.11 Subject to clause 4.9, the Service Provider must bind each sub-processor to a written commitment substantially equivalent to this DPA.

4.12 The commitment referenced in clause 4.11 must include, if the sub-processor processes PwC personal data originating in a jurisdiction that imposes restrictions over transferring personal data (such as EEA, UK, DIFC, ADGM, Bahrain, Oman, KSA, Qatar and QFC) or in any country, territory or sector in circumstances that do not provide an adequate level of protection for personal data according to the laws of the aforementioned jurisdictions , all of the data importer obligations as set out in the aforementioned laws (including without limitation the EU Model Contractual Clauses; the DIFC Standard Contractual Clauses,ADGM Standard Contractual Clauses and KSA PDPL Standard Contractual Clauses where and when applicable) or their superseding instruments including the third party beneficiary rights afforded to data subjects by those clauses.

4.13 If the Services do not provide PwC with the ability to extract, delete, update or correct personal data, Service Provider must, on PwC request and as far as possible, assist PwC in addressing the legal rights of data subjects, including, without limitation, the right to receive a copy of personal data and to have personal data corrected, updated or deleted.

4.14 Service Provider must provide information, on PwC's request, to enable PwC to comply with Data protection laws where the requested information is in Service Provider's possession or under its control. This includes assisting PwC in complying with the requirements outlined in the relevant Data protection laws, notably ensuring adherence to data subject rights, notification of data breaches to both data subjects and relevant authorities, and conducting data protection impact assessments.

4.15 Service Provider must inform PwC in writing at mer_me_data_protection_management@pwc.com within 3 business days of receiving a request from a Data Subject relating to personal data and without responding to the request.

4.16 Service Provider must inform PwC without undue delay and in any event not later than forty eight (48) hours after becoming aware of accidental, unauthorised or unlawful destruction, loss, alteration or disclosure of or access to PwC personal data (including any PwC personal data processed by a sub-processor). Service Provider must additionally inform PwC of the following as soon as known to Service Provider:
a) the nature and surrounding circumstances of the incident, including when the incident occurred or is estimated to have occurred
b) the type of PwC personal data and the number of data subjects affected and the categories and approximate number of personal data records concerned
c) how the incident is being investigated.including the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4.17 Service Provider must take immediate measures to contain any incident described in clause 4.16 and address its underlying causes. Service Provider must provide reasonable information about remediation on PwC request.

4.18 Subject to clause 4.19, on completion or termination of the Services, whichever happens first, Service Provider must (i) follow any instructions of PwC regarding return of PwC personal data and (ii) within a reasonable timeframe, irretrievably delete, and cause subprocessors to irretrievably delete, all copies of PwC personal data remaining in Service Provider's (or its sub-processors') possession or control. Service Provider must provide confirmation of deletion on PwC's written request.

4.19 Clause 4.18 does not apply to PwC personal data which Service Provider is required to retain to comply with law. In that case, the Service Provider warrants that it will guarantee the confidentiality of the personal data transferred and will not process the personal data anymore.

4.20 On PwC's request, and subject to suitable confidentiality obligations, Service Provider must provide to PwC information demonstrating Service Provider's or any sub-processor's compliance with this DPA, in the form of a SOC 2 Type II, SSAE 16 SOC 1 Type II or international equivalent (ISAE 3402 or ASAE 3402) as amended or replaced from time to time. and allow for and contribute to audits, including inspections, conducted by PwC or another auditor mandated by the data controller. The Data Controler may exercise the rights in this clause not more than once annually unless Service Provider reports an incident under clause 4.16, in which case PwC may exercise the rights in this clause as it deems necessary in order to satisfy itself that any risks arising from the incident have been resolved

5. PwC Network Firms

5.1 PwC Network Firms that are authorised users or recipients of the Services shall be third party beneficiaries of the terms of this DPA.

6. Indemnification

6.1 Service Provider agrees to indemnify and keep indemnified PwC, PwC Network Firms and their respective data subjects, partners, members, officers, directors, employees, contractors, agents, representatives, successor and assigns ("Indemnitees") from and against all judgments, awards, settlements, liabilities, damages, claims, costs, expenses, including reasonable attorney's fees, and any penalties and fines awarded against any of the Indemnitees, to the extent arising out of or relating to Service Provider's breach of this DPA or data protection laws.

7. Service provider affiliates

7.1 Service Provider shall procure that each of its affiliates (or entity which has signed a participation agreement with PwC or any PwC Network Firm) complies with the terms of this DPA if processing PwC personal data.

8. Interpretation

8.1 Any phrase following the terms “include”, “including”, “in particular” or similar expression is illustrative and does not limit the sense of the words preceding those terms.

9. Survival

9.1 Except for clause 6 (indemnification) which endures beyond termination or expiration of the agreement without limit in time, all obligations of this DPA endure beyond termination or expiration of the agreement for as long as Service Provider has PwC personal data in its possession or control.

10. Precedence

10.1 In case of conflict, ambiguity or discrepancy among the terms of the documents that form the agreement, then to the maximum extent that the conflicting or inconsistent terms can be interpreted so that they are consistent with and supplemental to one another, such reading of the terms shall prevail so as to give effect to all terms. If the preceding sentence does not resolve interpretive questions, the order of precedence shall be: firstly, the Middle East applicable data protection law, secondly, this DPA and lastly, the terms of the agreement.

11. Amendment

11.1 No amendment to this DPA is effective unless it is in writing and signed by both parties. This DPA may be modified without the consent of any third party.