PwC SDC Kolkata Data Protection and Privacy Policy*

Document Owner: Risk and Ethics
Classification: Public

Version: 1.3

Released: 24 August 2020

* This policy has also been hosted on Company's external website due to regulatory requirement.

pwc

Document Release Notice	
Document title	PwC SDC Kolkata Data Protection and Privacy Policy
Version draft	V1.3
Date of release	24 August 2020
Document classification	Public
Owner(s)	Risk and Ethics
Author(s)	Arnab Tarafdar
Reviewer(s)	Ujjwal Kumar Bose & Amit Kr Agarwal
Approved by	Subhasis Majumdar

Revision History				
Release No.	**Release Date**	**Change Details (include Section No., if applicable)**	**Amended by**	**Approved by**
1	15 May 2018	First Release	Arnab Tarafdar & Ujjwal Kumar Bose	Subhasis Majumdar
1.1	2 December 2019	Changes in IP Committee Composition	Vikash Agarwal	Subhasis Majumdar
1.2	23 March 2020	Changes in Section 7 – IP Committee contact information	Vikash Agarwal & Amit Kr Agarwal	Subhasis Majumdar
1.3	24 August 2020	Inclusion of clauses of supplement policy	Vikash Agarwal	Subhasis Majumdar

Table of Contents

pwc

1. Purpose and application

As a member of the PwC network, PwC SDC Kolkata will apply the requirements of the PwC network data protection policy through its own local policies. PwC SDC Kolkata will also ensure its local policies reflect the requirements of applicable privacy law. Applicable privacy law includes the GDPR where it applies to a processing activity including EEA personal data.

PwC SDC Kolkata applies the requirements of the PwC network data protection policy in a number of ways, including through this policy. PwC SDC Kolkata has its own Information Security Policy which deals with data protection, primarily in connection with specific functions or business activities. This policy doesn't override data protection requirements in PwC SDC Kolkata's other policies to the extent those requirements are in addition to the requirements of this policy or protect personal data to at least the same standard as this policy. This policy overrides the data protection requirements in PwC SDC Kolkata's other policies to the extent this policy imposes additional requirements or requires a higher standard of protection of personal data.

2. Primary sources of PwC SDC Kolkata's data protection obligations

The primary sources of PwC SDC Kolkata's obligations in connection with data protection are:

- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- the GDPR where it applies to a processing activity including EEA personal data
- PwC Network Standard 10.6 on information protection
- the PwC network data protection policy and this policy
- PwC's intra-network data transfer agreement
- PwC SDC's Information Security Policy

pwc

3. Minimum data protection requirements applying to PwC SDC Kolkata

This policy applies to all employees, contractors, third party staff, temporaries, consultants, secondees and other resources working in the PwC SDC Kolkata. All of these people are expected to be familiar and fully in compliance with these policies.

Data privacy laws (including the GDPR) impose specific legal requirements depending on whether the PwC SDC Kolkata or client entities (PwC firms) have control over the processing activities being undertaken. These requirements may apply to PwC SDC Kolkata when it:

- collects, processes and stores client confidential data;
- processes personal data provided by entities, clients or third parties operating in jurisdictions within the EEA; or
- offers services to individuals or monitors the behaviour of individuals in those jurisdictions; or
- collects, processes and stores personal data of its employees, staff and third parties operating outside the EEA;

This policy sets out minimum requirements that apply to PwC SDC Kolkata when processing personal data or developing global applications that will process personal data.

The minimum requirements differ depending on whether PwC SDC Kolkata is:

- processing the relevant personal data on someone else's instructions (e.g. where PwC SDC Kolkata processes personal data on the instructions of a client or another PwC firm) – see section 6
- processing or procuring processing in any other circumstances – see section 4
- developing a global application that will process personal data - see section 5.

Please note there are modified and additional requirements for processing activities that include EEA personal data.

pwc

4. Minimum data protection requirements

Except to the extent PwC SDC Kolkata processes personal data on someone else's instructions (e.g. on the instructions of a client or another PwC firm), PwC SDC Kolkata's processing or procuring processing of personal data must comply with the minimum requirements in this section 4.

4.1 Data protection by design

When deciding how to process personal data and when processing it, PwC SDC Kolkata must implement technical and organisational measures (e.g. pseudonymisation) designed to implement data protection principles (e.g. data minimisation) effectively and to integrate necessary safeguards into the processing in order to meet the requirements of applicable privacy law[1]. The measures must be appropriate considering (i) the state of the art (ii) the cost of implementation (iii) the nature, scope, context and purposes of the processing and (iv) the risk posed to data subjects.

4.2 Data protection by default

PwC SDC Kolkata must put in place appropriate technical and organisational measures for ensuring that, by default, personal data isn't processed unnecessarily. This applies to the amount of personal data collected, the extent to which it is processed, how long it's stored and who can access it. In particular, PwC SDC Kolkata must ensure that, by default, personal data isn't made available to an indefinite number of people without some action by the data subject.

[1]For processing EEA personal data, the technical and organisational measures must be designed to meet the requirements of the GDPR and protect the rights of data subjects.

pwc

4.3 Lawful collection, processing, transfer and retention of personal data

4.3.1 PwC SDC Kolkata will:

a. **[collection]** collect personal data only for identified and lawful purposes connected with the business of one or more PwC firms.

b. **[processing]** process personal data only where it has a lawful basis for doing so under an applicable privacy law and in a manner that's lawful, fair and compatible with the purpose for which the personal data was collected.

c. **[data minimisation]** collect and process personal data that is adequate, relevant and limited to what is necessary in relation to the purpose for which the personal data is processed

d. **[retention]** retain personal data only:

   i. to the extent and for so long as necessary in connection with the purpose for which PwC SDC Kolkata processes the personal data

   ii. as required by professional standards or Policies

   iii. as required or permitted by law.

Engagement data – All engagement data shall be retained as per the terms and conditions agreed by PwC SDC Kolkata with the respective PwC member firm in the services agreement and/or the applicable statement of work.

Organisational data – All organisation data shall be retained for a minimum period of 8 years.

PwC SDC Kolkata will delete, destroy or permanently anonymise all other personal data it processes.

Legal hold – This must be retained until such time the legal hold is removed. When in doubt or if a conflict occurs (for example, if relevant laws or regulations provide for a shorter retention period than a firm's document retention policies) it is the data owner's responsibility to contact the respective LOS/BU Leader.

When they are no longer needed, all copies of data, including those on backup tapes, must be irreversibly destroyed according to standards and procedures defined by the Information Security team. All users are responsible for timely deletion/purging of

engagement data and emails from designated shared drives and laptops/desktops. The Information Security Team will be informed by respective LOS of specific back-up/retention requirements, if any.

e. **[transfer]**[2] transfer personal data only in accordance with applicable privacy law and, in particular, transfer EEA personal data to a third party only to the extent one of the following applies:

   i. the PwC SDC Kolkata has a lawful basis for doing so and the transfer is to:

      A. a third party controller in the EEA or a white list jurisdiction that has entered into a binding commitment to restrict its processing of the personal data to an agreed purpose and to implement appropriate technical and organisational measures to protect the personal data from unauthorised processing or

      B. a third party controller in neither the EEA nor a white list jurisdiction, if the third party controller has entered into the standard contractual clauses in EU Commission Decision 2004/915/EC or standard data protection clauses adopted by the EU Commission under Article 46(2) of the GDPR or one of the conditions in section 4.3.2 has been met[3] or

      C. a third party processor that has provided sufficient guarantees to implement appropriate technical and organisational measures to enable the PwC firm to meet the requirements of this policy and entered into a binding commitment substantially equivalent to clause 1 of schedule C of PwC's intra-network data transfer agreement and, if the third party processor is in neither the EEA nor a white list jurisdiction, the third party processor has entered into the standard contractual clauses in EU Commission Decision 2010/87/EU or standard data protection clauses adopted by the EU Commission under Article 46(2) of the GDPR or one of the conditions in section 4.3.2 has been met[4]

   ii. the transfer is necessary to comply with a Requirement of Law and the PwC SDC Kolkata transfers only that portion of the personal data that is legally required to be disclosed to comply with the relevant requirement.

4.3.2 The conditions referred to in sections 4.3.1(e)(i)(B) and 4.3(e)(i)(C) for the transfer of EEA personal data to a third-party controller or a third-party processor without the safeguards provided by the EU standard contractual clauses are[5]:

---

[2] *PwC's intra-network data protection agreement and paragraph's M, N and O of PwC Network Standard 10.6 on information protection impose additional requirements in connection with transfers of personal data, including transfers of EEA personal data to another PwC firm. PwC SDC Kolkata must also comply with its transparency and other obligations under this policy in connection with any transfer of EEA personal data.*

[3] *PwC SDC Kolkata should not rely on the conditions in section 4.3.2 for large scale or repetitive transfers.*

[4] *See footnote 3 above*

[5] *See footnote 3 above*

a) the data subject has explicitly consented to the proposed transfer, after being informed about the possible risks for them due to lack of adequate protection and appropriate safeguards or

b) the transfer is necessary for one of the following:

(i) to perform a contract between the data subject and the PwC SDC Kolkata or to implement pre-contractual measures at the data subject's request
(ii) to enter into or perform a contract in the interest of the data subject between the PwC SDC Kolkata and another party
(iii) to protect vital interests of the data subject or others, where the data subject is physically or legally incapable of giving consent.

4.4 Transparency – information to be given to data subjects

PwC SDC Kolkata will give data subjects information about its processing of their personal data in accordance with applicable privacy law and as required by paragraphs M, N and O of PwC Network Standard 10.6 on Information Protection (available at https://www.central.ssp.pwc.com/sites/3u0hktuhcnwfkclqhx3k/SitePages/10.6%20Information%20Protection.aspx). *PwC SDC Kolkata* will provide the relevant information within the timeframes specified in the relevant law.

4.5 Security

PwC SDC Kolkata will implement technical and organisational measures at least consistent with the PwC Network Information Security Policy and Standards to protect personal data against unauthorised or unlawful processing (including unauthorised disclosure, access, loss, alteration, damage and destruction). The measures must be appropriate considering (i) the state of the art (ii) the cost of implementation (iii) the nature, scope, context and purposes of the processing and (iv)the risk posed to data subjects.

PwC SDC Kolkata will restrict access to personal data to personnel with a need to know who are bound to maintain the confidentiality and security of the personal data and process it only on PwC SDC Kolkata's instructions or to comply with a Requirement of Law.

4.6 Accuracy and integrity

PwC SDC Kolkata will take commercially reasonable steps to update, correct, complete or delete (as appropriate) any personal data shown to be out of date, inaccurate or incomplete, to the extent required by applicable privacy laws.

4.7 Rights of data subjects

Where a data subject exercises a right under applicable privacy law, PwC SDC Kolkata will respond by taking any action required by the relevant privacy law, unless the request is obviously unfounded or excessive. PwC SDC Kolkata will take the relevant action within one month of receipt, unless a different time period is set by applicable privacy law.

Upon request by a data subject, PwC SDC Kolkata will provide data subjects with appropriate information on their personal data to confirm that it is accurate and up to date, as well as the right to request correction of their personal data. However, in case of client data, PwC SDC Kolkata will notify the relevant client (i.e. concerned PwC member firm/data controller) about such notice.

4.8 Record keeping

PwC SDC Kolkata will maintain records of its processing operations relating to personal data that document the following:

(a) its name and contact details
(b) the name and contact details of the PwC SDC Kolkata's Information Protection Leader
(c) the purposes for which the relevant personal data is being processed
(d) the categories of data subjects whose personal data is being processed and the categories of personal data being processed
(e) the categories of recipients to whom the personal data has or will be disclosed
(f) where possible, the time limits for retaining different categories of personal data
(g) where possible, a general description of the technical and organisational security measures.

PwC SDC Kolkata will take adequate steps to make the record available to a relevant supervisory authority, as and when found applicable, to the extent required by applicable privacy law subject to necessary internal approval.

pwc

4.9 Breach notification

PwC SDC Kolkata will comply with any applicable privacy law requirement to notify data subjects and/or clients, as the case may be, of a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data PwC SDC Kolkata will also notify the breach to the Network Information Protection Leader, as the case may be, in accordance with reporting guidelines approved by the Network Data Protection Governance Board for this purpose.

4.10 Joint controllers of EEA personal data

4.10.1 PwC firms as joint controllers

If PwC SDC Kolkata is a joint controller of EEA personal data with other PwC firms, PwC SDC Kolkata must have an arrangement with them regarding their respective responsibilities as joint controllers for complying with the requirements of the PwC Network Data Protection policy in connection with the relevant processing, including their respective roles and responsibilities to relevant data subjects.

4.10.2 Third parties as joint controllers

Where PwC SDC Kolkata is a joint controller of EEA personal data with one or more third party controllers, the PwC SDC Kolkata must have an arrangement with the third party controller(s) regarding the respective responsibilities of all of the joint controllers for complying with their obligations under the GDPR in connection with the relevant processing, including their respective roles and responsibilities to relevant data subjects.

4.11 Automated decision making and profiling – only for EEA personal data

Section 4.11 applies only where PwC SDC Kolkata processes EEA personal data.

4.11.1 Unless the decision meets the requirements in sections 4.11.2 and 4.11.3 below, PwC SDC Kolkata must not make a decision about a data subject based solely on automated processing of personal data (including profiling) if the decision has legal or other similarly significant consequences for the data subject.

4.11.2 The decision must be:

(a) necessary to enter into or perform a contract between the PwC SDC Kolkata and the data subject or

(b) authorised by EU or EU Member State law to which the PwC SDC Kolkata is subject or

(c) based on the data subject's explicit consent.

In each case, the PwC SDC Kolkata must have implemented measures to safeguard the data subject's rights, freedoms and legitimate interests, including (at least) the right to express their point of view and contest the decision and to have someone consider the decision on the PwC SDC Kolkata's behalf.

4.11.3 Where the decision is based on special categories of personal data, one of the following must also be satisfied:

(a) the data subject has given explicit consent to processing their personal data for the relevant purpose, unless an EU or EU Member State law provides otherwise

(b) processing is necessary for performing legal obligations or exercising specific rights relating to employment, social security or social protection law

(c) processing is necessary to protect the data subject's vital interests or those of another person, where the data subject is physically or legally incapable of giving consent

(d) processing in the course of the legitimate activities of a not-for-profit body that relates to members, former members or others in regular contact with the body where the personal data isn't disclosed outside the body without the data subject's consent

(e) processing relates to personal data that the data subject has manifestly made public

(f) processing is necessary for establishing, exercising or defending legal claims or whenever courts are acting in their judicial capacity

(g) processing is necessary for reasons of substantial public interest, based in EU or EU Member State law.

4.12 Mandatory DP impact assessment for EEA personal data

Section 4.12 applies only where PwC SDC Kolkata processes EEA personal data.

4.12.1 PwC SDC Kolkata must assess the impact of its proposed processing on the protection of personal data before carrying out any of the following:

(a) systematic and extensive evaluation relating to data subjects based on automated processing (including profiling) which produces legal effects for the data subjects or similarly significantly affects them

(b) large scale processing of special categories of personal data or personal data relating to criminal convictions or offences

(c) large scale, systematic monitoring of a publicly accessible area

(d) other processing of personal data that is likely to result in a high risk to the rights and freedoms of people, particularly where new technologies are used having regard to its nature, scope, context and purpose.

4.12.2 PwC SDC Kolkata must seek the Information Protection Leader's advice in connection with its data protection impact assessment, which must contain (at least):

(a) a systematic description of the proposed processing and its purpose, including any applicable legitimate interest pursued by the controller

(b) an assessment of the necessity and proportionality of the processing in relation to its purpose

(c) an assessment of the risks to the rights and freedoms of data subjects

(d) the measures proposed to address the risks.

4.12.3 If the data protection impact assessment indicates processing would result in a high risk to data subjects in the absence of measures the PwC SDC Kolkata proposes to mitigate risk, before processing begins, the PwC SDC Kolkata must consult the Network Data Protection Leader regarding appropriate consultation with the relevant supervisory authority.

5. Global applications

If PwC SDC Kolkata develops a global application, it must:

a. design the global application to meet any minimum requirements approved for this purpose from time to time by the Network Data Protection Governance Body;

b. on request, provide a PwC firm that may use the global application with a report on

how the global application meets the minimum requirements referred to in paragraph (a) above. The report must be in any form approved for this purpose from time to time by the Network Data Protection Governance Body.

6. Minimum data protection requirements when processing personal data on instructions

The minimum requirements in this section 6 apply to PwC SDC Kolkata to the extent it processes personal data on someone else's instructions (e.g. on a client's instructions or the instructions of another PwC firm). The requirements in the first two sentences of section 4.9 also apply. See section 4 for the minimum requirements that apply to PwC SDC Kolkata for all other processing of personal data.

6.1 Processing on the instructions of another PwC firm

When processing personal data on the instructions of another PwC firm, PwC SDC Kolkata will comply with the relevant obligations under PwC's intra-network data transfer agreement.

6.2 Processing on the instructions of a client or another third party

6.2.1 When processing personal data on the instructions of a client or another third party, the PwC SDC Kolkata must comply with:

(a) its obligations under any relevant agreement with the client or other third party and

(b) to the extent consistent with (a), the other requirements in this section 6.2.

6.2.2 Security

The security requirements in section 4.5 above also apply, to the extent consistent with the terms agreed with the relevant client or other third party.

6.2.3 Lawful collection, processing, transfer and retention

When collecting or processing personal data on the instructions of a client or another third party, PwC SDC Kolkata must:

(a) **[collection, processing and retention]** collect, process and retain the personal data only within the scope of the instructions agreed with the client or other third party or to comply with a Requirement of Law, and ensure anyone acting under the PwC SDC Kolkata's authority does the same

(b) **[contract governing processing arrangements]** when processing EEA personal data, ensure its processing arrangements with the client or other third party are governed by a binding written contract (including electronic form) that meets the requirements of Article 28.3 of the GDPR

(c) **[sub-processors]** not engage another PwC firm or a third party to process the personal data without the client or other third party's prior authorisation (which may be general or specific) and, when the sub-processing includes EEA personal data, ensure its arrangements with the sub-processor are governed by a binding written contract (including electronic form) that imposes the same data protection obligations as are included in the contract referred to in section 6.2.3(b)

(d) **[record of processing activities]** when processing EEA personal data, keep a record of all categories of processing activities carried out on the instructions of a client or other third party, that meets the requirements of Article 30.2 of the GDPR and make the record available to a supervisory authority on request.

7. Information Protection Oversight Committee ('IP Committee')

IP Committee will act as the Information Protection Oversight Body and is aimed at guaranteeing the authorities' manifest support for the Information Protection ('IP') initiatives of the organization.

pwc

7.1 Scope

The IP Committee shall meet at least once a month to review the following:

(a) Review and evaluate current KSDC principles, policies and processes relating to management of data and ensure the same are aligned with the PwC Network's strategy and legal and regulatory requirements;
(b) Provision of regular training, guidance and awareness on information protection and data use matters to other areas of the firm, the staff and contractors;
(c) Informing the leadership of the issues found during the audits (either internal or external audits), and seek their solution;
(d) All non-compliance incidents and investigation reports in consultation with the Incident Response Team (set up in accordance with Incidence Response Plan);
(e) Handling of confidentiality and data protection queries (including those from regulators, clients and individuals);
(f) Advise Line of Service and support functions of emerging critical issues;
(g) Oversee all requirements of Network Information Protection Standard are complied with;
(h) Review of IT, procurement contracts and management of third party vendor contracts to ensure the member firm's compliance with its information protection obligations;
(i) Coordinating with Regional R&Q / Data Protection / IT security leaders on matters of cross-border importance.

7.2 IP Committee composition:

Role	Members	Responsibilities
Information Protection Leader	Subhasis Majumdar	• Overall compliance of Information Protection Standards and related policies as well as scope of IP outlined above;
Office of General Counsel (PwC SDC Legal & Compliance Team)	Ujjwal Kumar Bose	• advise on legal requirement, regulatory obligations and data protection issue; • advise whether to notify PwC Network Firms of breach in applicable cases;
Chief Information Security Officer (CISO)	Amit Gangopadhyay	• advise on the member firm's information security policies and processes, as well as digital threats and responses, where an information security breach is involved; • notify regional CISO and work together with/ notify CSIRT; • determine whether to notify Network Information Security of the breach;

Lead Investigator	Amit Kumar Agarwal	• convene periodic meetings of IP Committee and record actions; • investigate reported matters and report back to IP Committee with recommended actions; • administering IP function; • supporting IP committee as needed;
Chief People Officer	Vivek Mishra	• advise on people related matters • initiate disciplinary actions in applicable cases

8. Queries and Complaints

For help with queries and complains about data privacy and protection, including compliance with local law, regulations and professional standards, reach out to IP Committee through xa_dataprotection@pwc.com.

9. Dictionary

Anonymise	make it impossible to re-identify a data subject from the information, taking into account all means likely reasonably to be used by anyone to re-identify them
Confidential data	data subject to professional secrecy, confidential and/or proprietary data relating specifically to a client's business, and other information identified as subject to professional secrecy, confidential and/or proprietary by a client. This information includes, but is not limited to, business procedures, marketing plans, merger and acquisition data, financial information, the names of the clients in certain cases, and descriptions of the work being performed. This information does not include publicly available information or information in the public domain.
Controller	a natural or legal person or an organisation which alone or jointly with others determines the purposes for which personal data is processed and the manner in which personal data is processed
Data subject	the natural living person to whom personal data relates
Directive	means Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
EEA	the member states of the European Union, Iceland, Liechtenstein, Norway and Switzerland[6]

pwc

EEA personal data	personal data of a data subject in the EEA
Global application	an application developed by PwC IT or using network funds or developed to be used by three or more PwC firms
GDPR	the 'General Data Protection Regulation', Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
Personal data	any information relating to an identified natural living person or to a natural living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, ID number, location data, IP address or other online identifier or to one or more other factors specific to the person's identity. For clarity, personal data includes personal data that is publicly available and excludes personal data that has been anonymised so it is no longer possible to re-identify a data subject from the information, taking into account all means likely reasonably to be used by the controller or anyone else to re-identify them
Privacy law	a law relating to the privacy, confidentiality and/or security of personal data
Processing	means any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
Processor	a natural or legal person or an organisation that processes personal data on behalf of a controller
Profiling	any form of automated processing of personal data evaluating personal aspects relating to a natural person, in particular to analyse or predict the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her
PwC firm	a Member Firm or Relevant Entity
PwC Network Information Security Policy and Standards	means the PwC Network Information Security Policy, the PwC Network Standard related to Information Protection and any other Policies relating to information security or data protection in effect from time to time

PwC's intra-network data transfer agreement	the agreement between PwC firms that provides a framework to facilitate the transfer of confidential information and personal data between them
Special categories of personal data	• personal data revealing someone's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership • genetic data or biometric data processed for the purpose of uniquely identifying someone • data concerning health • data concerning someone's sex life or sexual orientation.
Supervisory authority	any competent public body responsible for monitoring and enforcing compliance with privacy law
Third party	a natural or legal person or an organisation that is not a party to PwC's intra-network data transfer agreement
Transfer	includes disclosure
white list jurisdiction	means a jurisdiction which ensures an adequate level of protection for personal data according to a decision adopted by the European Commission based on Article 25(6) of the Directive or, from 25 May 2018, Article 45(1) of the GDPR[7].

[6] Unlike the other countries referred to in the definition, Switzerland is neither a member of the European Union nor a party to the Agreement on the European Economic Area. Switzerland is included in the definition of EEA for this policy to apply the EU standard of protection to personal data of people in Switzerland.

[7] At the date of approval of Network Data Protection Policy, the jurisdictions approved as offering adequate protection under Article 25(6) of the Directive are: Andorra, Argentina, Canada - for personal data within the scope of the Personal Information Protection and Electronic Documents Act (Statutes of Canada 2000, chapter 5), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay and the U.S. for personal data transferred to organisations in the U.S under the EU-U.S. Privacy Shield. Adequacy decisions adopted by the European Commission based on Article 25(6) of the Directive remain in force under the GDPR until amended, replaced or repealed.

pwc

Thank you