

ANNEX 3E

Data Protection and Processing of Personal Information

Article 3E.1 Definitions

For the purposes of this Annex:

“data controller” (also known as data fiduciary in India) means the person who, alone or jointly with others, determines the purposes and means of the processing of personal data;

“data subject” (also known as data principal in India) means an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

“personal data” means any information relating to a data subject transferred from the transferring customs authority to the receiving customs authority in accordance with Annex 3D (Framework for Authentication Process of Origin Declarations);

“personal data breach” means a breach of data security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, the personal data transmitted, stored or otherwise processed;

“process”, “processed” or “processing” means any operation or set of operations which are performed on personal data or on sets of personal data, whether by wholly or partially 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;

“professional secrecy” means the laws and regulations applicable to a customs authority obliging it not to disclose non-public information received in an official capacity;

“receiving customs authority” means the customs authority in India receiving the requested information pursuant to this Agreement;

“receiving Party” means India;

“transferring customs authority” means the customs authority in the United Kingdom sending the requested information pursuant to this Agreement; and

“transferring Party” means the United Kingdom.

Article 3E.2

Scope

1. This Annex shall apply to the transfer of personal data between the customs authorities of the Parties, for general processing, in accordance with paragraphs 6 and 7 of Article 3.16 (Basis of a Claim for Preferential Tariff Treatment) and Annex 3D (Framework for the Authentication Process of Origin Declarations). In accordance with Annex 3D (Framework for the Authentication Process of Origin Declarations), the scope of personal data covered under this Annex shall be limited to data such as unique reference numbers, registered email addresses of exporters and producers, and other information as agreed by the Parties, necessary as part of any transfer of information. For greater certainty, this Annex does not apply to the origin declaration under Article 3.15 (Proof of Origin).
2. The Parties shall ensure that the appropriate safeguards in this Annex are in place for the general processing of personal data and protecting the personal data consistent with the laws, regulations and internal policies and procedures applicable to each Party.
3. The transfer of personal data between the Parties shall be deemed to be a data controller to data controller transfer, for the purposes of the transferring customs authority's legislation.

Article 3E.3

Purpose and Use Limitation

1. Subject to paragraph 2, the transfer of personal data shall solely be for the specified purpose of establishing the authenticity of an origin declaration in accordance with paragraphs 6 and 7 of Article 3.16 (Basis of a Claim for Preferential Tariff Treatment) and Annex 3D (Framework for the Authentication Process of Origin Declarations). The receiving Party shall not further process the relevant personal data in a manner that is incompatible with the purpose for which it was transferred. Compatible processing includes processing pursuant to the terms of the Annex 3D (Framework for the Authentication Process of Origin Declarations), administration and enforcement of determination of origin or of customs matters under this Chapter, and any other authentication instruments that may be agreed between the Parties.
2. The receiving customs authority shall not process the relevant personal data for purposes other than those set out in paragraph 1, unless it has received written approval from the transferring customs authority.

Article 3E.4

Data Accuracy and Minimisation

1. The transferring customs authority shall only transfer personal data that is adequate, relevant and limited to what is necessary in relation to the purpose of

processing. The transferring customs authority shall ensure that, to the best of its knowledge, the personal data it transfers is accurate and up to date.

2. If a customs authority becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other customs authority without undue delay. Each customs authority shall take reasonable steps to ensure that inaccurate personal data is erased, corrected or otherwise rectified as appropriate and in a timely manner, having regard to the purpose of processing.

Article 3E.5 Storage Limitation

The receiving customs authority shall retain the personal data for no longer than necessary and appropriate for the purpose for which it is processed, including any administrative, quasi-judicial or judicial proceedings initiated for the failure to comply with laws and regulations implementing this Chapter. The receiving customs authority shall put in place appropriate technical or organisational measures to ensure compliance with this obligation.

Article 3E.6 Security of Processing

1. The transferring customs authority during the transmission of the personal data and the receiving customs authority upon receipt of the personal data, shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against accidental or unlawful destruction, loss, or alteration, and protection against unauthorised disclosure or access.
2. Subject to paragraph 3, in the event of a personal data breach concerning personal data processed by the transferring customs authority or the receiving customs authority, the customs authority concerned shall notify the other customs authority as soon as possible but no later than 24 hours from the time of discovering the personal data breach. The notification may include appropriate restrictions as to the further transmission of the personal data.
3. In the event of personal data breach, the customs authority concerned may delay or omit the notification when such notification could endanger security of the Party or any form of public security operations.
4. In the event of personal data breach, the customs authority concerned shall use reasonable and appropriate means to remedy the personal data breach, including measures to minimise and mitigate possible adverse effects and prevent such a breach from taking place again.
5. In the event of personal data breach, the customs authority concerned shall document, report, investigate and keep records of the personal data breach, including its effects and any remedial action taken. The other customs authority

may request information on the outcome of the investigation, relating to transfers of personal data under this Annex.

Article 3E.7

Access

1. Each customs authority shall ensure it has appropriate measures in place to respond, without undue delay, to any enquiries and requests it receives from data subjects relating to the processing of their personal data pursuant to this Annex, subject to the restrictions in Article 3E.10 (Restrictions).
2. In particular, upon request by a data subject, the relevant customs authority to the extent applicable shall provide the following:
 - (a) confirmation to the data subject as to whether personal data relating to them is being processed;
 - (b) a copy of the personal data relating to them;
 - (c) confirmation that the personal data held by the receiving customs authority is consistent with the data received from the transferring Party;
 - (d) the information contained in Article 3E.11 (Transparency);
 - (e) information on any onward transfer under Article 3E.13 (Onward Disclosure and Transfer of Personal Data); and
 - (f) information on the right to lodge a complaint with the customs authority.
3. The transferring customs authority shall, at the request of the receiving customs authority, cooperate with the receiving customs authority in responding to enquiries and requests from data subjects under paragraphs 1 and 2.
4. Each customs authority shall provide that the information set out in paragraph 2 is provided free of charge within the time limits set out in Article 3E.12 (Time Limits).
5. If the provision of such information is denied or restricted, the customs authority shall inform the data subject in writing without undue delay, setting out the basis for the denial or restriction.
6. Each customs authority may publish guidance relating to the operation of this Article.

Article 3E.8

Rectification

1. Each customs authority shall ensure that data subjects are able to seek the correction or rectification of their personal data if they assert that it is inaccurate, no longer necessary for the purposes for which it was collected or processed, or

has not been processed in accordance with the applicable legal requirements or requirements of this Annex. Correction or rectification may include supplementation, erasure, blocking, or other measures or methods for addressing inaccuracies or improper processing. On request by a data subject seeking correction or rectification, the customs authority that received the request shall liaise with the other customs authority when considering the request. Upon reaching a decision, the customs authority that received the request shall inform the data subject, without undue delay, whether the data has been corrected or rectified, or whether the request has been denied, and provide reasons for the denial.

2. If the customs authority concludes that personal data it has received under the Agreement is inaccurate, has been improperly processed, or has been kept longer than necessary following a request by a data subject under Article 3E.7 (Access) or through its own investigation or inquiry, it shall take the correction or rectification measures set out in paragraph 1, as appropriate.
3. The transferring customs authority shall, at the request of the receiving customs authority, provide reasonable assistance to the receiving customs authority in taking any appropriate correction or rectification measures pursuant to paragraph 1 or 2.
4. The correction or rectification request by the data subject in a particular case may be subject to reasonable restrictions as set out in Article 3E.10 (Restrictions). If correction or rectification is denied or restricted, the customs authority that received the request shall, without undue delay, inform the data subject in writing as to the basis for the denial or restriction.
5. Each customs authority may publish guidance relating to the operation of this Article.

Article 3E.9 Automated Decisions

If a customs authority uses solely automated decision making, it shall use its best endeavours to have suitable measures in place to inform the relevant data subject about the reasons underlying the automated decision where this has resulted in authenticity not being established under Annex 3D (Framework for the Authentication Process of Origin Declarations).

Article 3E.10 Restrictions

1. Each Party shall provide that the measures set out in Articles 3E.7 (Access) and 3E.8 (Rectification) are subject to the Party's legal obligation not to disclose confidential information pursuant to professional secrecy or other legal obligations.

2. Each Party may restrict disclosure to prevent prejudice or harm to supervisory or enforcement functions of an authority of the Party acting in the exercise of the official authority vested in it.
3. Each Party shall provide that provisions restricting disclosure shall only be relied on, if necessary, provided by law and in accordance with this Annex. Each Party shall provide that reliance continues only for as long as the reason for the restriction on disclosure exists.
4. The receiving customs authority shall ensure that the relevant data subject is informed in writing about the restriction applied, without undue delay, unless doing so would prejudice the reasons for the restriction.

Article 3E.11 Transparency

1. Each Party shall make a transparency notice available to data subjects, describing in a clear and accessible manner, how personal data under this Annex may be processed by its customs authority, in its capacity as a transferring or receiving authority.
2. The transparency notice shall provide information on the purposes of processing, rights available to data subjects and procedures to exercise them, relevant safeguards, and any limitations or conditions applicable to such processing.
3. Each Party shall ensure that the transparency notice is published on an official government website and remains accessible to data subjects along with a copy of this Annex.

Article 3E.12 Time Limits

1. Subject to paragraph 2, each Party shall address and respond to a request from a data subject made in accordance with Article 3E.7 (Access) or Article 3E.8 (Rectification) no later than one month from the date it receives the request.
2. Each Party may further extend the period to respond to a request made pursuant to Article 3E.7 (Access) by up to 60 days, taking into account the complexity and number of requests. Each Party shall notify the relevant data subject of the extended response period within 30 days of the request.

Article 3E.13 Onward Disclosure and Transfer of Personal Data

1. Subject to paragraph 2, the receiving customs authority shall ensure that personal data received pursuant to Annex 3D (Framework for the

Authentication Process of Origin Declarations) is only disclosed and transferred to other national customs enforcement, regulatory or administrative authorities in that Party if:

- (a) it is disclosed and transferred for the purpose set out in paragraph 1 of Article 3E.3 (Purpose and Use Limitation); and
 - (b) the recipient authority undertakes to comply with the safeguards set out in this Annex, including by providing the data subjects with the relevant protections and applicable measures.
2. In exceptional cases, the receiving customs authority may disclose and transfer personal data to other national customs enforcement, regulatory or administrative authorities without the undertakings set out in paragraph 1 provided that the disclosure or transfer of the personal data is for important reasons of public interest or necessary for the establishment, exercise or defence of a legal claim.

Article 3E.14 Administrative Redress

1. Each Party shall ensure that a data subject is entitled to administrative redress where the data subject believes that a request made in accordance with Article 3E.7 (Access) or Article 3E.8 (Rectification) has been improperly denied.
2. Each Party shall provide that a designated authority or person (“reviewer”) reviews and, if appropriate, scrutinises any complaint raised by a data subject with a view to determining whether the processing of that data subject’s personal data by the Party constitutes an infringement of that Party’s laws and regulations or any of the requirements set out in this Annex.
3. Each Party shall provide that the reviewer may, where considered appropriate, inform the relevant data subject about the progress of their complaint. The reviewer shall formally respond to the complaint within 30 days of its receipt, or in exceptional cases, within 45 days.
4. Each Party shall provide that a formal written response setting out its determination and any recommendations relating to the matters raised includes details of the complaint escalation process, including judicial redress pursuant to Article 3E.15 (Judicial Redress), that the relevant data subject may pursue if they are not satisfied with the outcome of the handling by the reviewer.

Article 3E.15 Judicial Redress

1. Each Party shall ensure that if a data subject believes that that Party has failed to comply with the obligations set out in Articles 3E.7 (Access), 3E.8 (Restrictions) or 3E.14 (Administrative Redress), or believes that their personal data has been subject to a personal data breach, that data subject can seek

judicial redress against that Party following that Party's domestic appeal and dispute resolution process as part of the data protection laws and regulations, as appropriate.

2. In the event of a dispute between a data subject and a Party, that Party shall inform the other Party of the dispute. If appropriate, the other Party shall cooperate in resolving the dispute.
3. Paragraphs 1 and 2 are without prejudice to any other judicial redress available with respect to the processing of a data subject's personal data under the law of the Party in which redress is required.

Article 3E.16 Joint Review

The Parties shall conduct periodic joint reviews of the policies and procedures that implement this Annex and their effectiveness through the Working Group on Rules of Origin.

Article 3E.17 Suspension

1. If the transferring Party considers that the receiving Party has materially breached this Annex and has sufficient evidence to support such determination, it may suspend, in whole or in part, the transfer of personal data pursuant to paragraphs 6 and 7 of Article 3.16 (Basis of a Claim for Preferential Tariff Treatment) and Annex 3D (Framework for the Authentication Process of Origin Declarations) by written notification to the receiving Party through the Working Group on Rules of Origin.
2. Such suspension shall be limited to circumstances involving a serious or systemic failure by the receiving Party to comply with its obligations under this Annex. A suspension shall not be initiated in response to isolated or minor breaches that do not constitute a material failure to comply with this Annex, particularly where the receiving Party has taken prompt and appropriate remedial action to contain the breach and prevent its recurrence.
3. The transferring Party may only make a written notification as described in paragraph 1 where it deems the conditions set out in paragraph 2 have been met, and after the Parties have engaged in a reasonable period of consultation through the customs authorities without reaching a resolution.
4. The suspension shall take effect 20 days from the date of notification. Such suspension may be lifted by the transferring Party by written notification to the receiving Party. The suspension shall be lifted immediately on receipt of such notification. Any suspension under this Article shall be subject to a review by the Parties every 90 days.

5. Notwithstanding paragraphs 1 through 3, in the event of a material personal data breach, such as significant cyberattacks, physical security breaches or other serious incidents that compromise the integrity of the system or the personal data, the transferring Party may suspend transfers of personal data with immediate effect, taking into account the nature of the breach and risks to individuals. A suspension shall not be initiated in response to isolated or minor breaches, particularly where the receiving Party has taken prompt and appropriate remedial action to contain the breach and prevent its recurrence.
6. The receiving customs authority shall continue to accept origin declarations as applicable proofs of origin in accordance with Article 3.15 (Proof of Origin) in the event that data transfers to enable the authentication process pursuant to paragraphs 6 and 7 of Article 3.16 (Basis of a Claim for Preferential Tariff Treatment) and Annex 3D (Framework for the Authentication Process of Origin Declarations) are suspended under this Article.
7. Where a personal data breach occurs prior to the receipt by the receiving Party, including during transmission of personal data by the transferring Party, the transferring Party may suspend the transfer of personal data in accordance with paragraph 5. The Parties shall enter into consultations without delay to ensure that appropriate remedial measures are taken by the transferring Party to prevent recurrence. Where continued authentication of origin declarations is likely to be impacted by a suspension, the transferring Party shall, in consultation with and agreeable to the receiving Party, identify and implement suitable alternative mechanisms for data transfer within a reasonable period not exceeding three months. These mechanisms shall be subject to joint review every 90 days, with a view to restoring the normal process of data transfers as soon as practicable. Once the risk underlying the suspension has been addressed to the satisfaction of both Parties, the standard data transfer mechanism shall be reinstated without undue delay.
8. Notwithstanding any suspension of personal data transfers under paragraphs 1, 5 and 7, personal data falling within the scope of this Annex and transferred prior to its suspension shall continue to be processed in accordance with this Annex.

Article 3E.18

Notification

Each Party shall make reasonable efforts to notify the other Party regarding the adoption of laws or regulations that may materially affect the implementation of this Annex, as soon as practicable after such measures are adopted.