Version 16 (As Accepted)

Global Cross Border Enforcement Cooperation Arrangement

	Preamble	**2-3**
1	**Definitions**	**4**
2	**Purpose**	**4**
3	**Aims**	**5**
4	**Nature of the Arrangement**	**5**
5	**Reciprocity**	**6**
6	**Confidentiality**	**6**
7	**Respecting privacy and data protection principles**	**7**
8	**Coordination principles**	**7**
9	**Resolving Problems**	**8**
10	**Allocation of costs**	**8**
11	**Return of evidence**	**8**
12	**Eligibility**	**8**
13	**Role of the Executive Committee**	**9**
14	**Withdrawal**	**9**
15	**Commencement**	**9**
SCHEDULE ONE		**10**

PREAMBLE

Recalling that the resolution of the Warsaw Conference mandated an extension to the work of the International Enforcement Coordination Working Group to develop a common approach to cross-border case handling and enforcement coordination, to be expressed in a multilateral framework document addressing the sharing of enforcement-related information, including how such information is to be treated by recipients thereof.

Acknowledging that a global phenomenon needs a global response and that it is in the interests of privacy enforcement authorities[1], individuals, governments and businesses that effective strategies and tools be developed to avoid duplication, use scarce resources more efficiently, and enhance effectiveness in relation to enforcement in circumstances where the privacy and data protection effects transcend jurisdictional boundaries.

Mindful that cases are increasingly demonstrating how increased transborder data flows and the practices of private and public sector organisations relating to these transborder flows can quickly and adversely affect the privacy and the protection of the personal data of vast numbers of individuals across the world and that therefore increased transborder data flows should be accompanied by increased cross-border information sharing and enforcement cooperation between privacy enforcement authorities with such information sharing and enforcement cooperation being essential elements to ensure privacy and data protection compliance, serving an important public interest.

Reflecting on the fact that a number of privacy enforcement authorities have concurrently investigated several of the same practices or breaches.

Recalling the provisions of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108'), specifically those under Chapter IV on mutual assistance.

Recalling the 2007 OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy which recommends Member Countries cooperate across borders in the enforcement of laws protecting privacy and data protection, and taking the appropriate steps to:

- improve their domestic frameworks for privacy law enforcement to better enable cross-border cooperation, in a way consistent with national laws;

- provide mutual assistance to one another in the enforcement of laws protecting privacy, including through notification, complaint referral, investigative assistance and information sharing, subject to appropriate safeguards; and

- engage relevant stakeholders in discussions and activities aimed at furthering co-operation in the enforcement of laws protecting privacy.

Recalling the Resolutions of previous International Conferences of Data Protection and Privacy Commissioners (ICDPPC) and the Montreux Declaration which encouraged privacy enforcement

[1] For the avoidance of doubt and for the purposes of this document, the term 'privacy enforcement authorities' also includes data protection authorities.

authorities to further develop, amongst other things, their efforts to support international enforcement cooperation and to work with international organisations to strengthen data protection worldwide.

Building on significant progress which has been made in recent years at a global and regional level to enhance arrangements for, inter alia, cross-border enforcement cooperation.

Recognising that cross border enforcement cooperation can manifest itself in various ways. It can happen at different levels (national, regional, international), be of different types (coordinated or uncoordinated), and cover several activities (sharing best practice, internet sweeps, co-ordinated investigations, or joint enforcement actions leading to penalties/sanctions). However it manifests itself, key to its success is creating a culture of proactive and appropriate information sharing which may include information which is non-confidential or confidential and may or may not include personal data; and coordinating enforcement activities appropriately.

Encouraging all privacy enforcement authorities to use and develop further existing enforcement related mechanisms and cooperation platforms and help maximise the effectiveness of cross border enforcement cooperation.

Concluding that to effectively respond to data protection and privacy violations that affect multiple jurisdictions a multi-lateral approach is required and therefore appropriate mechanisms to facilitate the information sharing of confidential enforcement related material, and coordination of enforcement amongst privacy enforcement authorities to tackle said violations is much needed.

Therefore, privacy enforcement authorities are strongly encouraged to become Participants to this Arrangement and commit to following its provisions, particularly on confidentiality and data protection, when engaging in cross border enforcement activities.

1. DEFINITIONS

The following definitions will apply in this Arrangement:

'enforcement cooperation' – is a general term referring to privacy enforcement authorities working together to enforce privacy and data protection law.

'enforcement coordination' – refers to a specific type of enforcement cooperation in which two or more data protection or privacy enforcement authorities link their enforcement activities in relation to the enforcement of violations of privacy or data protection law in their respective jurisdictions.

'**Privacy and Data Protection Law'** means the laws of a jurisdiction, the enforcement of which has the effect of protecting personal data.

'Privacy Enforcement Authority' (hereafter 'PEA')[2] means any public body that has as one of its responsibilities the enforcement of a privacy and/or data protection law, and that has powers to conduct investigations or take enforcement action.

'**Request for assistance'** is a request from a Participant to one or more other Participants to cooperate/coordinate enforcing a privacy and data protection law and may include:

i. A referral of a matter related to the enforcement of a privacy and data protection law;
ii. A request for cooperation on the enforcement of a privacy and data protection law;
iii. A request for cooperation on the investigation of an alleged breach of a privacy and data protection law; and
iv. A transfer of a complaint alleging a breach of a privacy and data protection law.

'**Participant**' means a PEA that signs this Arrangement.

'Committee' means the Executive Committee of the International Conference of Data Protection and Privacy Commissioners.

Complainant – means any individual that has lodged, with the PEA, a complaint about an alleged violation of privacy and/or data protection law.

2. PURPOSE

The purpose of this Arrangement is to foster data protection compliance by organisations processing personal data across borders. It encourages and facilitates all PEAs' cooperation with each other by sharing information, particularly confidential enforcement-related information about potential or on-going investigations, and where appropriate, the Arrangement also coordinates PEAs' enforcement activities to ensure that their scarce resources can be used as efficiently and effectively as possible.

[2] For the avoidance of doubt and for the purposes of this document, the term 'privacy enforcement authorities' also includes data protection authorities.

3. AIMS

This Arrangement aims to achieve its objective by:

(i) Setting out key provisions to address the sharing of enforcement-related information, including how such information is to be treated by recipients thereof.
(ii) Promoting a common understanding and approach to cross-border enforcement cooperation at a global level;
(iii) Encouraging Participants to engage in cross-border cooperation by sharing enforcement related material and, where appropriate, coordinating their knowledge, expertise and experience that may assist other Participants to address matters of mutual interest;
(iv) Encouraging Participants to use and assist in the development of secure electronic information sharing platforms to exchange enforcement related information, particularly confidential information about on-going or potential enforcement activities.

4. NATURE OF THE ARRANGEMENT

This Arrangement sets forth the Participants' commitment with regard to international cross-border privacy enforcement cooperation, particularly on reciprocity, confidentiality, data protection, and coordination.

This Arrangement is NOT intended to:

(i) replace existing national and regional conditions or mechanisms for sharing information, or to interfere with similar arrangements by other networks:
(ii) create legally binding obligations, or affect existing obligations under other arrangements or international or domestic law;
(iii) prevent a Participant from cooperating with other Participants or non-participating PEAs, pursuant to other (binding or non-legally binding) laws, agreements, treaties, or arrangements.
(iv) create obligations or expectations of cooperation that would exceed a Participant's scope of authority and jurisdiction; or
(v) compel Participants to cooperate on enforcement activities including providing non-confidential or confidential information which may or may not contain personal data.

5. RECIPROCITY PRINCIPLE

All Participants will use their best efforts to cooperate with and provide assistance to other Participants in relation to cross border enforcement activity. This includes responding to requests for assistance as soon as practicable.

Participants should indicate in writing, when providing enforcement related material and data pursuant to this Arrangement, that such material is being provided pursuant to the terms of this Arrangement. Participants receiving requests for assistance should acknowledge receipt of such requests as soon as possible, and preferably within two weeks of receipt.

Prior to requesting assistance from another Participant, the sending Participant should perform an internal preliminary check to ensure that the request is consistent with the scope and purpose of this Arrangement and does not impose an excessive burden on the request participants.

A Participant may limit its cooperation in relation to cross border enforcement at its sole discretion. The following is a non-exhaustive list of such circumstances:

(i) The matter is not within the Participant's scope of authority or their jurisdiction.
(ii) The matter is not an act or practice of a kind that the Participant is authorized to investigate or enforce against in its domestic legislation.
(iii) There are resource constraints.
(iv) The matter is inconsistent with other priorities or legal obligations.
(v) There is an absence of mutual interest in the matter in question.
(vi) The matter is outside the scope of this Arrangement.
(vii) Another body is a more appropriate body to handle the matter.
(viii) Any other circumstances that renders a Participant unable to cooperate

If a Participant refuses or limits its cooperation then it should notify the reasons for refusal or limitation in writing to the Participant(s) requesting assistance where feasible four weeks of receiving the request for assistance.

6. CONFIDENTIALITY PRINCIPLE

6.1 Participants will, without prejudice to section 6.2, treat all information received from other Participants pursuant to this Arrangement as confidential by:

(i) treating any information received or requests for assistance pursuant to this Arrangement - which includes that another Participant is considering, has launched, or is engaged in, an enforcement investigation - as confidential , and, where necessary, making additional arrangements to comply with the domestic legal requirements of the sending Participants ;
(ii) not further disclosing information obtained from other Participants to any third parties, including other domestic authorities or other Participants, without the prior written consent of the Participant that has shared the information pursuant to this Arrangement;
(iii) limiting the use of this information to those purposes for which it was originally shared;
(iv) ensuring that, where a Participant receives an application from a third party (such as an individual, judicial body or other law enforcement agency) for the disclosure of confidential information received from another Participant pursuant to this Arrangement, the Participant that has received the application should:
    a. oppose, or strive to minimise, to the fullest extent possible any such application;
    b. maintain the confidentiality of any such information;
    c. notify the Participant that supplied the information forthwith and seek to obtain that Participant's consent for the disclosure of the information in question;
    d. inform the Participant who shared the information and has refused consent for its disclosure, if there are domestic laws that nevertheless oblige the disclosure of the information.
(v) upon withdrawal from this Arrangement, maintaining the confidentiality of any confidential information shared with it by another Participant pursuant to this Arrangement, or with mutual agreement with other Participants, return, destroy or delete the information.
(vi) ensuring that all appropriate technical and organizational measures are taken so that any information provided to it under this Arrangement is kept secure . This includes returning or

handling the information, (as far as possible to be consistent with national law) in accordance with the consent of the Participant that provided it.

6.2 Where domestic legal obligations may prevent a Participant from respecting any of the points in 6.1(i) – (vi), this Participant will inform the sending Participant(s) prior to the exchange of information.

7. RESPECTING PRIVACY AND DATA PROTECTION PRINCIPLES

Depending on Participants or the enforcement activity in question, it may be necessary to exchange personal data. However, in accordance with recognised privacy and data protection principles, the exchange of such personal data should be limited to what is necessary for effective privacy and data protection enforcement. All Participants to this Arrangement who either disclose or receive personal data will use their best efforts to respect the data protection safeguards of each other. However, it is recognised that these best efforts alone will not always be sufficient to enable the exchange of personal data.

In that case, if the Participant disclosing the personal data requires specific data protection safeguards, they should either:

- request the other Participants to provide assurance that they will comply with the requirements outlined in Schedule One; or,

make other arrangements between those who disclose and receive personal data to ensure that each Participant's privacy and data protection requirements are fully observed. Participants should notify the Committee if they are committing to the requirements set out in Schedule One or notify the Committee of other arrangements as referenced above. In principle, this notification should be done when submitting a notice of intent to participate in accordance with section 13, or, in any case before receiving personal data from another Participant under this Arrangement. A list of Participants, including their initial and updated notifications regarding Schedule One and/or other arrangements as described above, will be made available to all Participants.

8. COORDINATION PRINCIPLES

All Participants will use their best efforts to coordinate their cross border enforcement activities. The following principles have been established to help achieve the coordination of cross-border enforcement of privacy and data protection laws.

(i) Identifying Possible Coordinated Activities

a. PEAs should identify possible issues or incidents for coordinated action and actively seek opportunities to coordinate cross-border actions where feasible and beneficial.

(ii) Assessing Possible Participation

a. PEAs should carefully assess participation in coordinated enforcement on a case-by-case basis and clearly communicate their decision to other authorities.

(iii) Participating in Coordinated Actions

a. PEAs participating in a coordinated enforcement action should act in a manner that positively contributes to a constructive outcome and keep other authorities properly informed.

(iv) Facilitating Coordination

a. PEAs should prepare in advance to participate in coordinated actions.

(v) Leading Coordinated Action

a. PEAs leading a coordinated action should make practical arrangements that simplify cooperation and support these principles.

For further explanation of these principles, Participants can refer to the International Enforcement Coordination Framework

9. RESOLVING PROBLEMS

Any dispute between Participants in relation to this Arrangement should ideally be resolved by discussions between their designated contacts and, failing resolution in a reasonable time, by discussion between the heads of the Participants.

10. ALLOCATION OF COSTS

Each Participant bears their own costs of cooperation in accordance with this Arrangement.

Participants may agree to share or transfer costs of particular cooperation.

11. RETURN OF EVIDENCE

The Participants will return any materials that are no longer required if, at the time they are shared, the Requested Participant makes a written request that such materials be returned. If no request for return of the materials is made, then the Requesting Participant may dispose of the materials using methods prescribed by the Requested Participant, or if no such methods have been prescribed, by other secure methods, as soon as practicable after the materials are no longer required.

12. ELIGIBILITY CRITERIA

Any PEA may submit a notice of intent to the Committee indicating that they intend to participate in this Arrangement:

i. As a Member, if they are an accredited member of the International Conference of Data Protection and Privacy Commissioners (the Conference) and, as such, fulfil the membership requirements of Paragraph 5.1 of the Rules and Procedures of the Conference, including the requirement of appropriate autonomy and independence; or

ii. As a Partner if, although not an accredited member of the Conference, they are:

a. from a Member State signatory to the Convention for the Protection of Individuals with Regard to Automatic Processing (Convention 108); or

b. a member of the Global Privacy Enforcement Network (GPEN); or

c. a Participant in the APEC Cross-border Privacy Enforcement Arrangement (CPEA); or
d. a member of the Article 29 Working Party.

The Committee will keep an updated list of all PEAs that have committed to participate in the Arrangement and of all Participants that have committed to respect Schedule One. The list should be easily available to all Participants.

13 ROLE OF THE INTERNATIONAL CONFERENCE EXECUTIVE COMMITTEE

The Committee will:

a. Receive notices of intent to participate in or withdraw participation in this Arrangement;
b. Receive notices of commitment to Schedule One or such other arrangements as referenced in clause seven above;
c. Review such notices in order to verify that a PEA is eligible to sign this Arrangement;
d. Review the operation of the Arrangement three years after its commencement and submit its findings to the International Conference;
e. Publicise this Arrangement;
f. Recommend to the International Conference, upon due consideration of evidence, that a Participant to this Arrangement should have their participation suspended. Or, in the most serious cases of breach of the requirements set out in this Arrangement and thus breaching the trust that this Arrangement establishes between Participants, recommend to the International Conference that the Participant should be excluded from the Arrangement.

14. WITHDRAWAL FROM THE ARRANGEMENT

A Participant may withdraw participation in this Arrangement by giving one month's written notice to the Committee.

A Participant shall, as soon as reasonably practicable after notifying the Committee of its intention to withdraw participation in this Arrangement, take all reasonable steps to make its withdrawal from participation known to other Participants. This should include posting such information on the Participant's website whilst still participating in the Arrangement and for a reasonable period after ceasing to participate.

A Participant that is actively involved in a cross-border enforcement activity pursuant to this Arrangement should endeavour to satisfy its obligations in relation to such an activity before withdrawing from participation.

Regardless of withdrawal from the Arrangement, any information received pursuant to this Arrangement remains subject to the confidentiality principle under clause six and data protection principles referred to under clause seven and Schedule One of this Arrangement where relevant.

15. COMMENCEMENT

The Committee will accept notices of intent from the date of the 37th Conference and the Arrangement will commence once there are at least two Participants.

PEAs will become Participants once notified by the Committee of their acceptance.

SCHEDULE ONE

(1) Pursuant to clause seven of this Arrangement, the commitments in this Schedule may be appropriate to enable the exchange of personal data.

This Schedule does not, however, preclude circumstances where privacy and data protection laws of a Participant require further safeguards to be agreed between Participants in advance of any sharing of personal data.

As a minimum, provided both the Participants are in a position to enter into them, Participants exchanging personal data and committed to this Schedule will:

(i) restrict the sharing of personal data to only those circumstances where it is strictly necessary, and in any event, only share personal data that is relevant and not excessive in relation to the specific purposes for which it is shared; in any case personal data should not be exchanged in a massive, structural or repetitive way;

(ii) ensure that that personal data shared between Participants will not be subsequently used for purposes which are incompatible with the original purpose for which the data were shared;

(iii) ensure that personal data shared between Participants is accurate and, where necessary, kept up to date;

(iv) not make a request for assistance to another Participant on behalf of a complainant without the complainant's express consent;

(v) inform data subjects about (a) the purpose of the sharing (b) the possible storage or further processing of their personal data by the receiving Participant, (c) the identity of the receiving Participant, (d) the categories of data concerned, (e) the existence of the right of access and rectification and (f) any other information insofar as this is necessary to ensure a fair processing. This right can be limited if necessary for the protection of the data subject or of the rights and freedoms of others;

(vi) ensure that, data subjects have the right to access their personal data, to rectify them where they are shown to be inaccurate and to object to the exchange, storage or further processing of personal data relating to them. These rights can be limited if necessary for the protection of the data subject or of the rights and freedoms of others; the right to object can be further limited either where exercising this right would endanger the integrity of the enforcement action between Participants or where such a right interferes with other domestic legal obligations; ensure that where sensitive personal data are being shared and further processed, additional safeguards are put in place, such as the requirement that the data subjects give their explicit consent.

(vii) adopt, when receiving personal data, all technical and organizational security measures that are appropriate to the risks presented by the exchange, further use or storage of such data. Participants must also ensure that security measures are also adopted by an organization acting as data processor on their behalf and such processors must not use or store personal data except on instructions from that receiving Participant;

(viii) ensure that any entity to which the receiving participant makes an onward transfer of personal data is also subject to the above safeguards.

(ix) ensure that, where a Participant receives an application from a third party (such as an individual, judicial body or other law enforcement agency) for the disclosure of personal data received from another Participant pursuant to this Arrangement, the Participant that has received the application should:

a. oppose, or strive to minimise, to the fullest extent possible any such application.
b. notify the Participant that supplied the information forthwith and seek to obtain that Participant's consent for the disclosure of the information in question.
c. inform the Participant who shared the information and has refused consent for its disclosure, if there are domestic laws that nevertheless oblige the disclosure of the information.

(x) ensure mechanisms for supervising compliance with these safeguards and providing appropriate redress to data subjects in case of non-compliance;

(2) In this Schedule, 'sensitive personal data' means

a. Data which affect the complainant's most intimate sphere; or
b. Data likely to give rise, in case of misuse, to:
i. Unlawful or arbitrary discrimination; or
ii. A serious risk to the data subject.

In particular, those personal information which can reveal aspects such as racial or ethnic origin, political opinions, or religious or philosophical beliefs as well as those data relating to health or sex life, will be considered sensitive data. The applicable national legislation may lay down other categories of sensitive data where the conditions referred to in the previous paragraph are met.