Council of the European Union
General Secretariat

Brussels, 26 September 2022

WK 12569/2022 INIT

LIMITE

ENFOPOL
IXIM
CT
ISR
JAI

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Commission services
To:	Delegations
Subject:	DRAFT Agreement between the European Union, of the one part, and the Government of the State of Israel, of the other part, on the exchange of Personal Data between the European Union Agency for Law Enforcement Cooperation (Europol) and the authorities of Israel competent for fighting serious crime and terrorism

Delegations will find below the Draft Agreement between the European Union, of the one part, and the Government of the State of Israel, of the other part, on the exchange of Personal Data between the European Union Agency for Law Enforcement Cooperation (Europol) and the authorities of Israel competent for fighting serious crime and terrorism, as provided by Commission services. Delegations are reminded of the sensitive handling of the document.

Draft Agreement

between the European Union, of the one part, and the Government of the State of Israel, of the other part, on the exchange of Personal Data between the European Union Agency for Law Enforcement Cooperation (Europol) and the authorities of Israel competent for fighting serious crime and terrorism

THE EUROPEAN UNION, hereinafter referred to as ‘the Union’,

and

THE GOVERNMENT OF THE STATE OF ISRAEL, hereinafter referred to as 'Israel',

hereinafter jointly referred to as ‘the Contracting Parties’,

(1) CONSIDERING THAT by allowing the exchange of Personal Data between the European Union Agency for Law Enforcement Cooperation (Europol) and the authorities of Israel responsible for fighting serious crime and terrorism, this Agreement will create the framework for an enhanced operational cooperation between the Union and Israel in the field of law enforcement, while safeguarding the human rights and fundamental freedoms of all individuals concerned, including the right to privacy and data protection.

(2) CONSIDERING THAT this Agreement is without prejudice to Mutual Legal Assistance arrangements between Israel and the Member States of the Union allowing for the exchange of Personal Data.

(3) CONSIDERING THAT this Agreement does not impose any requirement on the Competent Authorities to transfer Personal Data and that the sharing of any Personal Data requested under this Agreement remains voluntary.

Have agreed as follows:

Article 1
Objective

The objective of this Agreement is to allow the transfer of Personal Data between the Competent Authorities of Israel and the European Union Agency for Law Enforcement Cooperation (Europol) in order to support and strengthen the action by the authorities of the Member States of the Union and those of Israel, as well as their mutual cooperation, in preventing and combating Criminal Offences, including serious crime and terrorism, while ensuring appropriate safeguards with respect to fundamental rights and freedoms of individuals, including the right to privacy and data protection.

Article 2
Definitions

For the purpose of this Agreement:

(a) 'Contracting Parties' means the European Union, and Israel;

(b) 'Europol' is the European Union Agency for Law Enforcement Cooperation, set up under Regulation (EU) 2016/794[1] or any amendment thereto ('Europol Regulation');

(c) 'Competent Authorities' means, for Israel, the domestic law enforcement authorities that under Israel national law are responsible for preventing and combatting Criminal Offences as listed in Annex II, and for the Union, Europol;

(d) 'Union Bodies' means institutions, bodies, missions, offices and agencies set up by, or on the basis of, the Treaty on European Union ('TEU') and the Treaty on the Functioning of the European Union ('TFEU'), as listed in Annex III;

(e) 'Criminal Offences' are the types of crime listed in Annex I and related Criminal Offences; Criminal Offences are considered related to the types of crime listed in Annex I if they are committed in order to procure the means of perpetrating, or to facilitate, or perpetrate, or to ensure the impunity of those committing such types of crime;

(f) 'Personal Data' means any information relating to a Data Subject;

1 Regulation (EU) 2016/794 means Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA; OJ L135, 24.5.2016, p. 53., OJ 169, 27.6. 2022, p.1-42

(g) 'Data Subject' means an identified or identifiable natural person, an identifiable person being a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(h) 'Genetic Data' means all Personal Data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question;

(i) 'Biometric Data' means Personal Data resulting from specific technical Processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as for instance dactyloscopic data;

(j) 'Processing' means any operation or set of operations which is performed upon Personal Data or sets of 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;

(k) 'Personal Data Breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

(l) 'Supervisory Authority' means one or more domestic independent authorities that is/are, alone or cumulatively, responsible for data protection in accordance with Article 17 of this Agreement, and that has been notified according to Article 27(3);

(m) 'International Organisation' means an organisation and its subordinate bodies governed by public international law, or any other body, which is set up by, or on the basis of, an agreement between two or more countries.

Article 3

Purposes of Processing Personal Data

1. Personal Data requested and received under this Agreement shall be processed only for the purposes of the prevention, investigation, detection or prosecution of Criminal Offences or the execution of criminal penalties, within the limits of Article 4(5) and the respective mandates of the Competent Authorities.

2. The Competent Authorities shall clearly indicate, at the latest at the moment of transferring Personal Data, the specific purpose or purposes for which the data are being transferred. For transfers to Europol, the purpose or purposes for such transfer shall be specified in line with the specific purpose or purposes of Processing set out in Europol's mandate.

Chapter II - Information exchange and data protection

Article 4
General data protection principles

1. Each Contracting Party shall provide for Personal Data exchanged under this Agreement to be:
   (a) processed fairly, lawfully, in line with the transparency requirements in Article 27 (1), and only for the purposes for which they have been transferred in accordance with Article 3;
   (b) adequate, relevant and limited to what is necessary in relation to the purpose or purposes for which they are processed;
   (c) accurate and kept up to date; each Contracting Party shall provide that its Competent Authorities take every reasonable step to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are rectified or erased without undue delay;
   (d) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed;
   (e) processed in a manner that ensures appropriate security of the Personal Data.
2. The transferring Competent Authority, at the moment of transferring Personal Data, may indicate any restriction on access thereto or the use to be made thereof, in general or specific terms, including as regards its onward transfer, erasure or destruction after a certain period of time, or the further Processing of it. Where the need for such restrictions becomes apparent after the information has been provided, the transferring Competent Authority shall inform the receiving authority accordingly.
3. Each Contracting Party shall ensure that the receiving Competent Authority complies with any restriction on access or further use of the Personal Data indicated by the transferring Competent Authority according to paragraph 2.
4. Each Contracting Party shall provide that its Competent Authorities implement appropriate technical and organisational measures in such a way as to be able to

demonstrate that the Processing will comply with this Agreement and the rights of the Data Subjects concerned are protected.

5. Each Contracting Party shall ensure that its Competent Authorities do not transfer Personal Data which have been obtained in manifest violation of human rights recognised by the norms of international law binding on the Contracting Parties. Each Contracting Party shall ensure that the Personal Data received are not used to request, hand down or execute a death penalty or any form of cruel or inhuman treatment.
6. Each Contracting Party shall ensure that a record is kept of all transfers of Personal Data under this Agreement and of the purpose or purposes for those transfers.

Article 5
Special categories of Personal Data and different categories of Data Subjects

1. The transfer and further Processing of Personal Data in respect of victims of a criminal offence, witnesses or other persons who can provide information concerning Criminal Offences, or in respect of persons under the age of 18, shall be prohibited unless it is strictly necessary and proportionate in individual cases for preventing or combating a criminal offence.
2. The transfer and further Processing of Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, Genetic Data, Biometric Data processed for the purposes of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary and proportionate in individual cases for preventing or combatting) a criminal offence, and if those data, except Biometric Data, supplement other Personal Data.
3. The Contracting Parties shall ensure that the Processing of Personal Data under paragraphs 1 and 2 of this Article is subject to appropriate safeguards guarding against the specific risks involved, including restrictions on access, measures for data security within the meaning of Article 16 and limitations on onward transfers under Article 8.

Article 6

Automated Processing of Personal Data

Decisions based solely on automated Processing of the Personal Data exchanged, including profiling, which may produce an adverse legal effect on the Data Subject or significantly affect him or her, shall be prohibited, unless authorised in law for preventing or combating a criminal offence, and safeguards for the rights and freedoms of the Data Subject are provided, including at least the right to obtain human intervention.

Article 7

Geographical limitations to the use of the Personal Data received

1. Subject to paragraphs 2 and 3 of this Article, Israel shall ensure that Personal Data received under this Agreement is used by its Competent Authorities, or other authorities in Israel to which such Personal Data has been transferred pursuant to Article 8, only in the territory to which this Agreement applies pursuant to Article 32(1).

2. By way of derogation, a Competent Authority of Israel which has received Personal Data under this Agreement, or another authority in Israel to which such Personal Data has been transferred pursuant to Article 8, may exceptionally use such Personal Data in the geographic areas that came under the administration of the State of Israel after 5 June 1967, in accordance with the conditions and safeguards set out in this Agreement, and solely for the protection of the civilian population, if the use is:

(a) essential for the prevention of a criminal offence in case of an imminent threat to life; or

(b) necessary for the prevention, investigation, detection, or prosecution of Criminal Offences, and Europol has given its prior authorisation for such use following a corresponding request.

3. Where a Competent Authority of Israel which has received Personal Data under this Agreement, or another authority in Israel to which such Personal Data has been transferred pursuant to Article 8, makes use of such Personal Data by relying on paragraph 2(a), the national contact point for Israel shall inform Europol without undue delay of such use, and provide Europol with an explanation, in the light of the conditions set out in paragraph 2(a), as to why obtaining the prior authorisation by Europol pursuant to paragraph 2(b) was not possible.

Article 8

Onward transfer of the Personal Data received

1. Israel shall ensure that its Competent Authorities only transfer Personal Data received under this Agreement to other authorities in Israel if:
   (a) Europol has given its prior explicit authorisation;
   (b) the purpose or purposes of the onward transfer are the same as the original purpose or purposes of the transfer by Europol or, within the limits of Article 3(1), are directly related to that original purpose or purposes and;
   (c) the onward transfer is subject to the same conditions and safeguards as those applying to the original transfer.

Without prejudice to Article 4(2), no prior authorisation is required when the receiving authority is itself a Competent Authority of Israel.

2. Israel shall ensure that onward transfers of Personal Data received under this Agreement to the authorities of a third country or to an International Organisation are prohibited, unless the following conditions are fulfilled:
   (a) the transfer concerns Personal Data other than that covered by Article 5;
   (b) Europol has given its prior explicit authorisation;
   (c) the purpose or purposes of the onward transfer are the same as the original purpose or purposes of the transfer by Europol, and;
   (d) The onward transfer is subject to the same conditions and safeguards as those applying to the original transfer.
3. Europol may only grant its authorisation under paragraph 2, point b, of this Article for an onward transfer to the authority of a third country or to an International Organisation if and insofar as an adequacy decision, an international agreement providing appropriate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals, a cooperation agreement or any other legal ground for transfers of Personal Data within the meaning of the Europol Regulation, in each case covering the onward transfer, is in place.
4. Europol may share Personal Data received under this Agreement with Union Bodies listed in Annex III and authorities responsible in the EU Member States for preventing and fighting Criminal Offences without the need for prior authorisation by Israel.
5. The European Union shall ensure that onward transfers of Personal Data received by Europol under this Agreement to Union Bodies not listed in Annex III, to the authorities of

third countries or to an International Organisation are prohibited, unless the following conditions are fulfilled:

(a) the transfer concerns Personal Data other than that covered by Article 5;

(b) Israel has given its prior explicit authorisation;

(c) the purpose or purposes of the onward transfer are the same as the original purpose of the transfer by Israel; and

(d) an adequacy decision, an international agreement providing appropriate safeguards with respect to the protection of the right to privacy and fundamental rights and freedoms of individuals or a cooperation agreement within the meaning of the Europol Regulation is in place with that third country or International Organisation, or unless Europol is able to rely on any other legal ground for transfers of Personal Data within the meaning of the Europol Regulation.

Article 9

Assessment of reliability of the source and accuracy of information

1. The Competent Authorities shall indicate as far as possible, at latest at the moment of transferring the information, the reliability of the source of the information on the basis of one or more of the following criteria:

   a) (A) where there is no doubt of the authenticity, trustworthiness and competence of the source, or if the information is supplied by a source who, in the past, has proved to be reliable in all instances

   b) (B) where the information is provided by a source from whom information received has in most instances proved to be reliable

   c) (C) where the information is provided by a source from whom information received has in most instances proved to be unreliable

   d) (X) where the reliability of the source cannot be assessed

2. The Competent Authorities shall indicate as far as possible, at the latest at the moment of transferring the information, the accuracy of the information on the basis of one or more of the following criteria:

   (a) (1) information of which the accuracy is not in doubt at the time of transfer;

(b) (2) information known personally to the source but not known personally to the official passing it on;

(c) (3) information not known personally to the source but corroborated by other information already recorded;

(d) (4) information which is not known personally to the source and cannot be corroborated.

3. Where the receiving Competent Authority, on the basis of information already in its possession, comes to the conclusion that the assessment of information supplied by the transferring Competent Authority or of its source carried out in accordance with paragraphs 1 and 2 needs correction, it shall inform that Competent Authority and shall attempt to agree on an amendment to the assessment. The receiving Competent Authority shall not change the assessment of information received or of its source without such an agreement.

4. If a Competent Authority receives information without an assessment, it shall attempt as far as possible and where possible in agreement with the transferring Competent Authority to assess the reliability of the source or the accuracy of the information on the basis of information already in its possession.

5. If no reliable assessment can be made, the information shall be evaluated in accordance with paragraph 1, point (d)) and paragraph 2, point (d) above.

RIGHTS OF DATA SUBJECTS

Article 10
Right of access

1. The Contracting Parties shall ensure that the Data Subject has the right, at reasonable intervals, to obtain information on whether Personal Data relating to him or her are processed under this Agreement and, when that is the case, access to at least the following information:

(a) the categories of data concerned, the purpose or purposes of the Processing, and where applicable the recipients or categories of recipients to whom the data are disclosed;

(b) an indication of the legal ground for Processing;

(c) the envisaged period for which the Personal Data will be stored, or, if that is not possible, the criteria used to determine that period;

(d) the existence of the right to request from the Competent Authority rectification, erasure or restriction of Processing of the Personal Data concerning the Data Subject;

(e) communication in an intelligible form of the Personal Data undergoing Processing.

(f) The right to lodge a complaint with the Supervisory Authority referred to in Article 17 and its contact details.

2. In cases where the right pursuant to paragraph 1 is exercised, the transferring Contracting Party will be consulted in writing, on a non-binding basis, before a final decision on the request for access is taken.

3. The Contracting Parties may provide for the information in response to any request under paragraph 1 to be delayed, refused or restricted if and as long as such delay, refusal or restriction constitutes a measure that is necessary and proportionate taking into account the fundamental rights and interests of the Data Subject, in order to:

(a) ensure that any criminal investigation and prosecution will not be jeopardised;

(b) protect the rights and freedoms of third parties; or

(c) protect national security, protect public order or prevent crime.

4. The Contracting Parties shall ensure that the Competent Authority having received the request to inform the Data Subject in writing of any delay, refusal or restriction of access and of the reasons for such delay, refusal or restriction of access. Those reasons may be omitted if and as long as this would undermine the purpose of refusal or restriction under paragraph 3. The Competent Authority shall inform the Data Subject of the possibility of lodging a complaint with the respective Supervisory Authority or seeking a judicial remedy.

Article 11

Right to rectification, erasure and restriction

1. The Contracting Parties shall ensure that the Data Subject has the right to have inaccurate Personal Data that concern that Data Subject and have been transferred under this Agreement rectified by the Competent Authorities. Taking into account the purpose or

purposes of the Processing, this includes the right to have incomplete Personal Data transferred under the Agreement completed.

2. Rectification shall include erasure of Personal Data that are no longer necessary for the purpose or purposes for which they are processed.
3. The Contracting Parties may provide for the restriction of Processing rather than the erasure of Personal Data if there are reasonable grounds to believe that such erasure could affect the legitimate interests of the Data Subject.
4. The Competent Authorities shall inform each other of cases referred to in paragraphs 1, 2 and 3. The receiving Competent Authority shall rectify, erase or restrict the Processing in accordance with the action taken by the transferring Competent Authority.
5. The Contracting Parties shall provide for the Competent Authority that has received the request to inform the Data Subject in writing without undue delay, and in any case within three months of receipt of a request in accordance with paragraphs 1 or 2, that data concerning the Data Subject have been rectified, erased or that the Processing has been restricted.
6. The Contracting Parties shall provide for the Competent Authority that has received the request to inform the Data Subject in writing, without undue delay and in any case within three months of receipt of a request in accordance with paragraphs 1 or 2 of any refusal of rectification, erasure or restriction of Processing, of the reasons for such a refusal and of the possibility of lodging a complaint with the respective Supervisory Authority and of seeking a judicial remedy.

Article 12

Notification of a Personal Data breach to the authorities concerned

1. The Contracting Parties shall ensure, in the event of a Personal Data Breach affecting Personal Data transferred under this Agreement, that the respective Competent Authorities notify each other as well as their respective Supervisory Authority of that Personal Data Breach without delay, and take measures to mitigate its possible adverse effects.
2. The notification shall at least:

(a) describe the nature of the Personal Data Breach including, where possible, the categories and number of Data Subjects concerned and the categories and number of Personal Data records concerned;

(b) describe the likely consequences of the Personal Data Breach;

(c) describe the measures taken or proposed to be taken by the Competent Authority to address the Personal Data Breach, including the measures taken to mitigate its possible adverse effects.

3. To the extent that it is not possible to provide all the required information at the same time, it may be provided in phases. Outstanding information shall be provided without undue further delay.

4. The Contracting Parties shall ensure that their respective Competent Authorities document any Personal Data Breaches affecting Personal Data transferred under this Agreement, including the facts relating to the Personal Data Breach, its effects and the remedial action taken, thereby enabling their respective Supervisory Authority to verify compliance with applicable legal requirements.

Article 13

Communication of a Personal Data Breach to the Data Subject

1. The Contracting Parties shall, where a Personal Data Breach as referred to in Article 11 is likely to severely and adversely affect the rights and freedoms of the Data Subject, provide for their respective Competent Authorities to communicate the Personal Data Breach to the Data Subject without undue delay.

2. The communication to the Data Subject pursuant to paragraph 1 shall describe, where possible, the nature of the Personal Data Breach, recommend measures to mitigate the possible adverse effects of the Personal Data Breach, and provide the name and contact details of the contact point where more information can be obtained.

3. The communication to the Data Subject pursuant to paragraph 1 shall not be required if:

(a) the Personal Data concerned by the breach were subject to appropriate technological protection measures that render the data unintelligible to any person who is not authorised to have access to that data;

(b) subsequent measures have been taken which ensure that the rights and freedoms of the Data Subject are no longer likely to be severely affected; or

(c) communication to the Data Subject pursuant to paragraph 1 would involve disproportionate effort, in particular owing to the number of cases involved; in such a case, there shall instead be a public communication or similar measure whereby the Data Subject is informed in an equally effective manner.

4. The communication to the Data Subject pursuant to paragraph 1 may be delayed, restricted or omitted where such communication would be likely to:

(a) obstruct official or legal inquiries, investigations or procedures;

(b) prejudice the prevention, detection, investigation and prosecution of Criminal Offences or the execution of criminal penalties, public or national security;

(c) affect the rights and freedoms of third parties;

where this constitutes a necessary and proportionate measure with due regard for the legitimate interests of the Data Subject concerned.

Article 14

Storage, review, correction and deletion of Personal Data

1. The Contracting Parties shall provide for appropriate time limits to be established for the storage of Personal Data received under this Agreement or for a periodic review of the need for the storage of Personal Data, so that data are stored only as long as is necessary for the purpose or purposes for which they are transferred.
2. In any case, the need for continued storage of Personal Data shall be reviewed no later than three years after the Personal Data has been transferred, and if no justified and documented decision is taken on the continued storage of Personal Data, Personal Data shall be erased automatically after three years.
3. Where a Competent Authority has reason to believe that Personal Data previously transferred by it are incorrect, inaccurate, no longer up to date or should not have been transferred, it shall inform the receiving Competent Authority, which shall correct or delete the Personal Data, and provide notification thereof to the transferring Competent Authority.
4. Where a Competent Authority has reason to believe that Personal Data previously received by it are incorrect, inaccurate, no longer up to date or should not have been transferred, it shall inform the transferring Competent Authority, which shall provide its position on the matter. Where the transferring Competent Authority concludes that the Personal Data are incorrect, inaccurate, no longer up to date or should not have been transferred, it shall inform the receiving Competent Authority, which shall correct or

delete the Personal Data, and provide notification thereof to the transferring Competent Authority.

Article 15

Logging and documentation

1. The Contracting Parties shall provide for the keeping of logs or other documentation of the collection, alteration, access, disclosure including onward transfers, combination and erasure of Personal Data.
2. Logs or documentation referred to in paragraph 1 shall be made available to the respective Supervisory Authority upon request for the purpose of verification of the lawfulness of data Processing, self-monitoring and ensuring proper data integrity and security.

Article 16

Data security

1. The Contracting Parties shall ensure the implementation of technical and organisational measures to protect Personal Data exchanged under this Agreement.

2. In respect of automated data Processing, the Contracting Parties shall ensure the implementation of measures designed to:
   (a) deny unauthorised persons access to Processing equipment used for Processing Personal Data (equipment access control);
   (b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);
   (c) prevent the unauthorised input of Personal Data and the unauthorised inspection, modification or deletion of stored Personal Data (storage control);
   (d) prevent the use of automated Processing systems by unauthorised persons using data- communication equipment (user control);
   (e) ensure that persons authorised to use an automated data Processing system have access only to the Personal Data covered by their access authorisation (data access control);

(f) ensure that it is possible to verify and establish to which bodies Personal Data may be or have been transmitted using data communication equipment (communication control);

(g) ensure that it is possible to verify and establish which Personal Data have been input into automated Processing systems and when and by whom the Personal Data were input (input control);

(h) ensure that it is possible to verify and establish what Personal Data have been accessed by which member of personnel and at what time (access log);

(i) prevent the unauthorised reading, copying, modification or deletion of Personal Data during transfers of Personal Data or during transportation of data media (transport control);

(j) ensure that installed systems may, in the event of interruption, be restored immediately (recovery);

(k) ensure that the functions of the system perform without fault, that the appearance of faults in the functions is immediately reported (reliability) and that stored Personal Data cannot be corrupted by system malfunctions (integrity).

Article 17

Supervisory Authority

1. Each Contracting Party shall ensure that there is an independent public authority responsible for data protection (Supervisory Authority) to ensure compliance with privacy law in order to protect the fundamental rights and freedoms of natural persons in relation to the Processing of Personal Data in accordance with this Agreement.
2. The Contracting Parties shall ensure that each Supervisory Authority:
   (a) acts with complete independence in performing its tasks and exercising its powers; it shall act free from external influence and neither seek nor accept instructions; its members shall have a secure term of office, including safeguards against arbitrary removal;
   (b) has the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers;
   (c) has effective powers of investigation and intervention to exercise oversight over the bodies it supervises, and to engage in legal proceedings;
   (d) has powers to hear complaints from individuals about the use of their Personal Data by the Competent Authorities under its supervision.

Article 18
Judicial redress

1. Each Contracting Party shall ensure that, without prejudice to any other administrative or non-judicial remedy, Data Subject shall have the right to an effective judicial remedy for violations of the rights and safeguards recognized in this Agreement resulting from the Processing of their Personal Data.
2. This shall include the right to compensation for any damage caused to the Data Subject by such Processing as a result of a violation of the Agreement and under the conditions set out in the respective legal frameworks of each Party.

Chapter III - Disputes

Article 19
Settlement of disputes

1.All disputes which may emerge in connection with the interpretation, application or implementation of this Agreement and any matters related thereto shall give rise to consultations and negotiations between representatives of the Contracting Parties with a view to reaching a mutually agreeable solution.

Article 20
Suspension clause

1. In the event of a material breach or of non-fulfilment of obligations stemming from this Agreement, either Contracting Party may suspend this Agreement temporarily in part or in whole by written notification to the other Contracting Party through diplomatic channels. Such written notification shall not be made until after the Contracting Parties have engaged in a reasonable period of consultation without reaching a resolution and suspension shall take effect twenty (20) days from the date of receipt of such notification. Such suspension may be lifted by the suspending Contracting Party upon written notification to the other Contracting Party. The suspension shall be lifted immediately upon receipt of such notification.

2. Notwithstanding any suspension of this Agreement, Personal Data falling within the scope of this Agreement and transferred prior to the suspension of this Agreement shall continue to be processed in accordance with this Agreement.

Article 21

Termination

1. This Agreement may be terminated at any time by either of the Contracting Parties by written notification through diplomatic channels, with three months' notice.
2. Personal Data falling within the scope of this Agreement and transferred prior to the termination of this Agreement shall continue to be processed in accordance with this Agreement at the time of termination.
3. In case of termination of this Agreement, the Contracting Parties shall agree on an implementing instrument for the continued use and storage of the information that has already been communicated between them. If no agreement is reached, either of the two Contracting Parties is entitled to require that the information which it has communicated be destroyed or returned to the transferring Party.

Chapter IV - Final provisions

Article 22

Relation to other international instruments

This Agreement shall not prejudice or otherwise affect or impact the legal provisions with regard to the exchange of information provided by any mutual legal assistance treaty, any other cooperation agreement or arrangement, or working law enforcement relationship for the exchange of information between Israel and any Member State of the Union.

Article 23

Implementing administrative arrangement

The details of cooperation between the Contracting Parties as appropriate to implement this Agreement shall be the subject of an implementing administrative arrangement concluded between Europol and the Competent Authorities of Israel, in accordance with the Europol Regulation.

Article 24

Administrative arrangement on confidentiality

Where necessary under this Agreement, the exchange of EU classified information, shall be regulated by an Administrative Arrangement on Confidentiality concluded between Europol and the Competent Authorities of Israel.

Article 25

National contact point and liaison officers

1. Israel shall designate a national contact point to act as the central point of contact between Europol and Competent Authorities of Israel. The specific tasks of the national contact point shall be listed in the implementing administrative arrangement as referred to in Article 23. The designated national contact point for Israel is indicated in Annex IV.
2. Europol and Israel shall enhance their cooperation as laid down in this Agreement through the deployment of liaison officer(s) by Israel. Europol may deploy one or more liaison officer(s) to Israel.

Article 26

Expenses

1. The Contracting Parties shall ensure that the Competent Authorities bear their own expenses, which arise in the course of the implementation of this Agreement, unless

provided for in this Agreement or stipulated in the implementing administrative arrangement referred to in Article 23.

Article 27

Notification of implementation

1. Each Contracting Party shall provide for its Competent Authorities to make publicly available their contact details as well as a document setting out in an intelligible form information regarding the safeguards for the Processing of Personal Data guaranteed under this Agreement, including information covering at least the items in Article 10(1), subparagraphs (a) and (c), and the means available for the exercise of the rights of Data Subjects. Each Contracting Party shall ensure that a copy of that document is notified to the other Contracting Party.
2. Where not already in place, the Competent Authorities shall adopt rules specifying how compliance with the provisions regarding the Processing of Personal Data transferred under this Agreement will be enforced in practice. A copy of these rules shall be notified to the other Contracting Party and the respective Supervisory Authorities.
3. The Contracting Parties shall notify each other of the Supervisory Authority responsible for overseeing the implementation of, and ensuring compliance with, this Agreement in accordance with Article 17.

Article 28

Entry into force

1. This Agreement shall be approved by the Contracting Parties in accordance with their own procedures.
2. This Agreement shall enter into force on the date of the last written notification by which the Parties have notified each other through diplomatic channels that the procedures referred to in paragraph 1 have been completed.

Article 29

Conditions for Implementation

1. This Agreement shall be implemented as of the first day after the date when all of the following conditions have been fulfilled:

(a) the implementing administrative arrangement as referred to in Article 23 has become applicable; and

(b) the Contracting Parties have notified one another that the obligations laid down in this Agreement have been implemented, including those laid down in Article 27, and such notification has been accepted.

2. The Contracting Parties shall exchange written notifications confirming the fulfilment of the conditions set out in paragraph /1 through diplomatic channels.

Article 30

Amendments and supplements

1. This Agreement may be amended in writing, at any time by mutual consent between the Contracting Parties by written notification exchanged through diplomatic channels. The amendments to this Agreement shall enter into force in accordance with the legal procedure provided for in Article 28 (1) and (2).
2. The Annexes to this Agreement may be updated, as necessary, by exchange of diplomatic notes. Such updates shall enter into force in accordance with the legal procedure provided for in Article 28 (1) and (2).
3. The Contracting Parties shall enter into consultations with respect to the amendment to this Agreement or its Annexes at the request of either Contracting Party.

Article 31

Review and evaluation

1. The Contracting Parties shall jointly review the implementation of this Agreement one year after its entry into force, and at regular intervals thereafter, and additionally if requested by either Contracting Party and jointly decided.
2. The Contracting Parties shall jointly evaluate this Agreement four years after the date of its application.
3. The Contracting Parties shall decide in advance on the modalities of the review of the implementation of the Agreement and shall communicate to each other the composition of their respective teams. The teams shall include relevant experts on data protection and law enforcement. Subject to applicable laws, any participants in a review shall be required

to respect the confidentiality of the discussions and have appropriate security clearances. For the purposes of any review, the Israel and the European Union shall ensure access to relevant documentation, systems and personnel.

Article 32

Territorial applicability

1. In accordance with European Union policy, this Agreement shall not apply to the geographic areas that came under the administration of the State of Israel after 5 June 1967. This provision should not be construed as prejudicing the Contracting Parties' respective principled and long-standing positions regarding the status of these areas. This provision is also without prejudice to the possibility to use Personal Data received under this Agreement pursuant to Article 7 of this Agreement.

2. This Agreement shall apply to the territory of the Union in which and in so far as the Treaty on European Union and the Treaty on the Functioning of the European Union are applicable. By the date of entry into force of this Agreement, the Union shall notify Israel in writing through diplomatic channels of the Member States to whose territories this Agreement applies, and which are bound by this Agreement. Where, after the entry into force of this Agreement, additional Member States chose to be bound by this Agreement, the Union shall notify Israel accordingly. This Agreement shall apply to the territory of each such Member State five days following the date of the notification for that Member State.

This Agreement shall be drawn up in duplicate in Bulgarian, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hebrew, Hungarian, Italian, Irish, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish, each text being equally authentic. In case of divergence of interpretation, the English text shall prevail.

IN WITNESS WHEREOF, the undersigned Plenipotentiaries, duly authorized to this effect, have signed this Agreement.

Done at …, this … day of … , which corresponds to the …in the Hebrew Calendar, in the year …

For the Government of the State of **Israel** For **the EU**

Annex I – Areas of crime

- terrorism,
- organised crime,
- drug trafficking,
- money-laundering activities,
- crime connected with nuclear and radioactive substances,
- immigrant smuggling,
- trafficking in human beings,
- motor vehicle crime,
- murder, grievous bodily injury,
- illicit trade in human organs and tissue,
- kidnapping, illegal restraint and hostage taking,
- racism and xenophobia,
- robbery and aggravated theft,
- illicit trafficking in cultural goods, including antiquities and works of art,
- swindling and fraud,
- crimes against the financial interests of the Union
- insider dealing and financial market manipulation
- racketeering and extortion,
- counterfeiting and product piracy,
- forgery of administrative documents and trafficking therein,
- forgery of money and means of payment,
- computer crime,
- corruption,
- illicit trafficking in arms, ammunition and explosives,
- illicit trafficking in endangered animal species,
- illicit trafficking in endangered plant species and varieties,
- environmental crime, including ship-source pollution,
- illicit trafficking in hormonal substances and other growth promoters,
- sexual abuse and sexual exploitation, including child abuse material and solicitation of children for sexual purposes,
- genocide, crimes against humanity and war crimes.

Annex II – Competent Authorities of Israel and their competences

The Competent Authorities of Israel to which Europol may transfer data are as follows:

Israel National Police

Israel Security Agency

Israel Securities Authority

Israel Tax Authority

Israel Competition Authority

Israel Money Laundering and Terrorism Financing Prohibition Authority

Israel Nature & Parks Authority

Israel Antiquities Authority

Annex III – List of Union Bodies

Common Security and Defence Missions/Operations, limited to law enforcement activities

European Anti-Fraud Office (OLAF)

European Border and Coast Guard Agency (Frontex)

European Union Agency for Criminal Justice Cooperation (Eurojust)

European Union Intellectual Property Office (EUIPO)

European Public Prosecutor's Office (EPPO)

Annex IV – National contact point

The national contact point for Israel to act as the central point of contact between Europol and Competent Authorities of Israel is hereby designated as

Coordination & Operations Division of the Israel National Police

Israel has the duty to inform Europol in case the national contact point for Israel changes.

Annex V- Declaration concerning Contracting Parties

Following the discussions between the European and Israeli sides, it should be clarified for the avoidance of doubt, that upon the entry into force of the Agreement Between the European Union, of the one part, and the Government of the State of Israel, of the other part, on the Exchange of Personal Data Between the European Union Agency for Law Enforcement Cooperation (Europol) and the Authorities of Israel Competent for Fighting Serious Crime and Terrorism (hereinafter, the 'Agreement'), it shall be a legally binding treaty under international law and will be regarded as such by the State of Israel and the Union.

The Agreement shall require ratification for its entry into force, and shall be registered with the UN Secretariat and published by it, upon its entry into force.