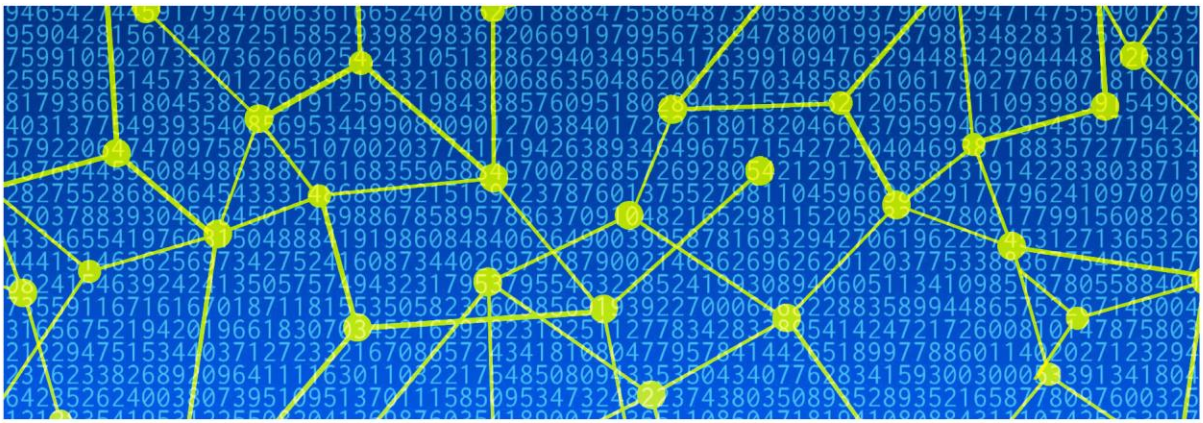

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 1/2020

EDPS Opinion on the negotiating mandate to conclude an international agreement on the exchange of personal data between Europol and New Zealand law enforcement authorities

31 January 2020

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 '[w]ith respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3) 'for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.

Under Article 42(1) of Regulation 2018/1725, the Commission shall 'following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the EDPS where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data'.

This Opinion relates to the EDPS' mission to advise the EU institutions on coherently and consistently applying the EU data protection principles, including when negotiating agreements in the law enforcement sector. It builds on the general obligation that international agreements must comply with the provisions of TFEU and the respect for fundamental rights that stands at the core of EU law. In particular, compliance with Articles 7 and 8 of the Charter of Fundamental Rights of the EU and Article 16 TFEU must be ensured.

Executive Summary

On 30 October 2019, the European Commission adopted a Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and New Zealand on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the New Zealand authorities competent for fighting serious crime and terrorism. The objective of the envisaged Agreement is to provide the legal basis for the transfer of personal data between Europol and the competent authorities of New Zealand respectively, in order to support and strengthen their actions and mutual cooperation in preventing and combatting serious transnational crime and terrorism, while ensuring appropriate safeguards with respect to the protection of privacy, personal data and other fundamental rights and freedoms of individuals.

Transfers of personal data gathered in the context of criminal investigations and further processed by Europol to produce criminal intelligence are liable to have a significant impact on the lives of the individuals concerned. For that reason, the international agreement must ensure that the limitations to the rights to privacy and data protection in relation to the fight against serious crime and terrorism apply only in so far as is strictly necessary.

The EDPS notes that New Zealand has a well-established national data protection legislation and an independent data protection authority, competent to supervise also the law enforcement authorities. Moreover, he appreciates the fact that Commission has incorporated into the proposed negotiating mandate with New Zealand a number of the specific recommendations already expressed by the EDPS in his Opinion 2/2018 on eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries.

Hence, the aim of the recommendations in this Opinion is to clarify and, where necessary, further develop the safeguards and controls with respect to protection of personal data, taking into consideration the specific context of New Zealand. To this end, the EDPS recommends that:

- the Council Decision authorising opening of negotiations pursuant to Article 218 TFEU should contain a reference not only to the procedural legal basis but also to the relevant substantive legal basis, which should include Article 16 TFEU;

- in line with the principle of purpose limitation, the envisaged Agreement should explicitly lay down the list of the criminal offences regarding which personal data could be exchanged;

- in view of the practical implementation of the principle of storage limitation, the future Agreement should specifically provide for periodic review of the need for storage of the transferred personal data;

- given the importance of the right to information for the exercise of the other data protection rights, the Agreement should include clear and detailed rules regarding the information that should be provided to the data subjects.

Finally, the EDPS expects to be consulted at later stages of the finalisation of the draft Agreement in accordance with Article 42 of Regulation (EU) 2018/1725. He remains available for further advice during the negotiations.

TABLE OF CONTENTS

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[1],

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC[2], in particular Article 42(1),

Having regard to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[3],

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKGROUND

1. 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[4], (hereafter "Europol Regulation"), lays down specific rules regarding transfers of data by Europol outside of the EU. Article 25(1) thereof lists a number of legal grounds based on which Europol could lawfully transfer data to authorities of third countries. One possibility would be an adequacy decision of the Commission in accordance with Article 36 of Directive (EU) 2016/680 finding that the third country to which Europol transfers data ensures an adequate level of protection. Since there is no such adequacy decision at the moment, the other alternative for Europol to regularly transfer data to a third country would be the conclusion of a binding international agreement between the EU and the receiving third country adducing adequate safeguards with respect to the protection of privacy and other fundamental rights and freedoms of individuals.

2. At the moment, there is no legal basis for the regular and structured exchange of personal data between Europol and New Zealand law enforcement authorities. Europol and New Zealand Police have signed a working arrangement in April 2019. This arrangement provides a framework for structured strategic-level cooperation, including a secure line allowing direct secure communication, and New Zealand has deployed a liaison officer at Europol. However, it does not provide a legal basis for the exchange of personal data.

3. The Commission considers it necessary to add New Zealand as a priority country to start negotiations with in the short-term in the light of the political strategy outlined in the European

Agenda on Security[5], the Council Conclusions on EU External Action on Counter-terrorism[6], the Global Strategy[7] and the operational needs of law enforcement authorities across the EU. It underlines that the potential benefits of closer cooperation were also demonstrated by the follow up to the Christchurch attack of March 2019. New Zealand formally requested the initiative on 23 August 2019.

4. On 30 October 2019, the European Commission adopted a Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and New Zealand on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the New Zealand authorities competent for fighting serious crime and terrorism[8] (hereinafter "the Recommendation"). The Annex to the Recommendation (hereinafter "the Annex") lays down the Council's negotiating directives to the Commission, i.e. the objectives the latter should aim to achieve on behalf of the EU in the course of the negotiations.

5. The objective of the envisaged Agreement is to provide the legal basis for the transfer of personal data between Europol and the competent authorities of New Zealand respectively, in order to support and strengthen the action by the competent authorities of this country and Member States as well as their mutual cooperation in preventing and combatting serious transnational crime and terrorism, while ensuring appropriate safeguards with respect to the protection of privacy, personal data and fundamental rights and freedoms of individuals[9].

6. Pursuant to Article 42(1) of Regulation 2018/1725, the Commission has to consult the EDPS following the adoption of a proposal for a recommendation to the Council pursuant to Article 218 TFEU, where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data.

7. Furthermore, Recital 35 of the Europol Regulation provides that "where appropriate and in accordance with Regulation [2018/1725] the Commission should be able to consult the EDPS before and during the negotiation of an international agreement between the EU and a third country to allow the exchange of data between Europol and the authorities of this third country".

8. The EDPS welcomes that he has been consulted on the Recommendation by the European Commission and expects that a reference to this Opinion will be included in the preamble of the Council Decision. The present Opinion is without prejudice to any additional comments that the EDPS could make on the basis of further available information at a later stage.

2. GENERAL COMMENTS

9. Transfers of personal data gathered in the context of criminal investigations and further processed by Europol to produce criminal intelligence envisaged under the Agreement are liable to have a significant impact on the lives of the individuals concerned, as they will potentially be used in prosecution cases in the receiving country under its national law.

10. As transfers of personal data to third countries constitute an interference with individuals' rights to privacy and data protection guaranteed by Articles 7 and 8 of the Charter, requirements of **necessity and proportionality** of the envisaged processing need to be assessed in accordance with Article 52(1) of the Charter[10]. As a result, the international agreement must ensure that the limitations to rights to privacy and data protection in relation to the fight against serious crime and terrorism apply only in so far as is strictly necessary[11].

11. While the Europol Regulation provides for an autonomous data protection regime specific to Europol, its Recital 40 clarifies that it should remain *"consistent with other relevant data protection instruments applicable in the area of police cooperation in the Union" [...] in particular, Directive (EU) 2016/680 [...]"*. In this regard, Recital 68 of Directive (EU) 2016/680 lists among the various factors, which should be taken into account in the context of assessing of transfers of personal data to law enforcement authorities in third countries, their "*international commitments*" as well as *"any relevant Commission adequacy decision adopted in accordance with Article 45 of Regulation (EU) 2016/679"*.

12. To this end, the EDPS notes that New Zealand has national data protection legislation, the Privacy Act, and an independent data protection authority, the Privacy Commissioner, competent to supervise both private and public bodies, including law enforcement authorities, since 1993[12]. Furthermore, the Commission has adopted in December 2012 a Decision on the adequate protection of personal data by New Zealand pursuant to Directive 95/46/EC[13]. New Zealand is an observer to the Council of Europe Committee of Convention 108[14]. In addition, the Office of the Privacy Commissioner of New Zealand has served until recently as Secretariat of the International Conference of the Data Protection and Privacy Commissioners (ICDPPC), now renamed to Global Privacy Assembly (GPA).

13. The EDPS has already had the opportunity to comment on the exchange of personal data between Europol and the law enforcement authorities of eight third countries on the basis of Article 25(1)(b) of Europol Regulation[15]. The EDPS welcomes that the Commission has incorporated a number of the recommendations from the 2018 Opinion into the proposed negotiating mandate with New Zealand, including: introducing an exhaustive list of the competent authorities in New Zealand to which Europol may transfer personal data with a short description of their competences (directive 3(d) of the Annex)[16]; allowing onward transfers of information by New Zealand authorities only for the original purposes of the transfer by Europol (directive 3(i) of the Annex)[17]; obliging the competent authorities of New Zealand to respect the restrictions by Europol on the transferred personal data and to specify how compliance with these restrictions will be enforced in practice (directive 3(c) of the Annex)[18]; or clarifying the legal possibilities to continue the processing of the already transferred data in case of suspension or termination of the Agreement (directive 6 of the Annex)[19].

14. In this context, the recommendations in this Opinion are aimed at clarifying and, where necessary, further developing the safeguards and controls in the future Agreement with respect to the protection of personal data. They are without prejudice to any additional recommendations that the EDPS could make on the basis of further available information and the provisions of the draft agreements during the negotiations.

15. In addition, the EDPS believes that there will be added value in developing international cooperation for the protection of personal data between the respective supervisory authorities of the EU and New Zealand, in line with Article 51 of Regulation (EU) 2018/1725 and Article 40 of Directive (EU) 2016/680. Moreover, such cooperation may help avoiding possible misinterpretations and conflicts in the course of the application of the Agreement and, if necessary, facilitate the functioning of the dispute settlement mechanism envisaged in directive 4 of the Annex.

3. RECOMMENDATIONS

3.1. Substantive legal basis of the Council Decision

16. The explanatory memorandum of the Recommendation states that it is based on Article 218 TFEU. The preamble to the draft Council Decision refers more specifically to Article 218 (3) and (4) TFEU. However, the preamble does not refer to any substantive legal basis for the envisaged Agreement.

17. In accordance with Article 296 (2) TFEU and the settled case law of the CJEU[20], the EDPS questions the fact that the citations in the preamble to the Council Decision only refer to the appropriate procedural legal basis and do not equally refer to the relevant substantive legal basis. The EDPS recalls that, in a similar law enforcement context, the CJEU found that *"the Council Decision on the conclusion of the envisaged Agreement [between Canada and the European Union on the transfer and processing of Passenger Name Record] data must be based jointly on Article 16(2) and Article 87(2)(a) TFEU"*[21].

18. According to the negotiating directives, the Commission should simultaneously pursue several objectives during the negotiations of the envisaged Agreement, among which allowing the transfer of personal data and ensure respect for the fundamental rights enshrined in the Charter, including the rights to privacy and the protection of personal data. The envisaged Agreement would thus relate directly to the objective pursued by Article 16 TFEU. **Therefore, the EDPS recommends adding in the preamble of the Council Decision a reference to the appropriate substantive legal bases for the future Agreement, which should include Article 16 TFEU.**

3.2. Purpose limitation

19. Purpose limitation is among the key principles of the EU data protection framework. Purpose limitation requires, on the one hand, that personal data are collected for specified, explicit and legitimate purposes and, on the other hand, that personal data are not further processed in a manner that is incompatible with those purposes. The Europol Regulation states in this respect that "*it contributes to transparency, legal certainty and predictability and is particularly of high importance in the area of law enforcement cooperation, where data subjects are usually unaware when their personal data are being collected and processed and where the use of personal data may have a very significant impact on the lives and freedoms of individuals*"[22]. More specifically, Article 18 of the Europol Regulation lays down an exhaustive list of purposes for data processing activities by Europol that are considered legitimate.

20. The EDPS welcomes that directive 2 of the Annex limits the exchange of data under the future Agreement only to crimes and related criminal offences falling within Europol's competence in accordance with Article 3 of Europol Regulation, in particular, preventing and combating terrorism, disrupting organised crime and fighting cybercrime, and also envisages that the Agreement should specify its scope and the purposes for which Europol may transfer personal data to the competent authorities of New Zealand. Furthermore, directive 3(b) of the Annex underlines the principle of specificity, according to which the data should not be processed for other purposes than for the purposes of the transfer.

21. Given the strong emphasis placed on purpose limitation in the Europol Regulation and for additional legal certainty, **the EDPS recommends that the future Agreement explicitly lays down the list of the criminal offences regarding which personal data could be exchanged. Moreover, the transferred personal data should be related to individual cases.**

3.3. Storage limitation

22. Directive 3(c) of the Annex provides that personal data *"shall not be retained for longer than is necessary for the purposes for which they have been transferred"*. Directive 3(f) further requires that the agreements should lay down rules on storage, review, correction and deletion of personal data. In that regard, the EDPS would like to point out that the Europol Regulation contains an elaborate regime for data storage with technical and procedural safeguards, which ensure that storage and erasure obligations are complied with in practice. Article 31 requires Europol to conduct reviews of the necessity and proportionality of storing the data every three years. This is without prejudice to different retention periods communicated by data providers when sending the data to Europol, which are binding for Europol. Any decision to store the data after the first three years must be duly justified and the motivation must be recorded. Europol is also bound to erase the data that have been erased in the systems of the data provider as soon as it is informed thereof.

23. **The EDPS recommends that the future Agreement provides for a periodic review of the need for storage of the transferred personal data as well as other appropriate measures ensuring that the time limits are observed, e.g. a requirement for Europol to inform New Zealand authorities, to whom data have been communicated or transferred, about the moment when the data will be erased from its systems**.

3.4. Right to information

24. The EDPS welcomes the fact that directive 3(e) of the Annex requires that the future international agreement ensures *"enforceable rights of individuals whose personal data are processed by laying down rules on the right of access, rectification and erasure, including the specific grounds which may allow any necessary and proportionate restrictions"*. Furthermore, directive 3(f) provides for that the Agreement should lay down rules, inter alia, "*on information to be made available to individuals*".

25. The right to information is of utmost importance as it allows the exercise of the other data protection rights, including the right to remedies, and ensures fair processing of the data[23]. Data subjects usually have no knowledge of the fact that their data are processed and transferred for law enforcement purposes. In the case of Europol, the Europol Regulation does not include any obligation for Europol to proactively inform data subjects of the fact that the agency is processing personal information regarding them. Data subjects have to exercise their right of access to find out if Europol is processing data about them. Nonetheless, in its Opinion 1/15, the CJEU found that *"air passengers must be notified of the transfer of their PNR data to Canada and of its use as soon as that information is no longer liable to jeopardise the investigations being carried out by the government authorities"* considering that *"[t]hat information is, in fact, necessary to enable the air passengers to exercise their rights to request access to PNR data concerning them and, if appropriate, rectification of that data, and, in accordance with the first paragraph of Article 47 of the Charter, to an effective remedy before a tribunal"*[24].

26. **The EDPS recommends that the future international agreement lays down clear and detailed rules regarding the information that should be provided to the data subjects, which should include information about the applicable regime for EU data subjects to exercise their rights of access, rectification and erasure in New Zealand.**

4. CONCLUSIONS

27. Transfers of personal data gathered in the context of criminal investigations and further processed by Europol to produce criminal intelligence are liable to have a significant impact on the lives of the individuals concerned, as they will potentially be used in prosecution cases in the receiving country under its national law. Therefore, the international agreement must ensure that the limitations to the rights to privacy and data protection in relation to the fight against serious crime and terrorism apply only in so far as is strictly necessary.

28. The EDPS welcomes the objective of the negotiation mandate to ensure respect for the fundamental rights and observe the principles recognised by the Charter, in particular the right to private and family life, recognised in Article 7 of the Charter, the right to the protection of personal data in Article 8 of the Charter and the right to effective remedy and fair trial in Article 47 of the Charter. Moreover, the EDPS appreciates the fact that Commission has incorporated into the proposed negotiating mandate with New Zealand a number of the specific recommendations already expressed by the EDPS in his Opinion 2/2018 on eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries.

29. The EDPS recommendations in this Opinion are aimed at clarifying and, where necessary, further developing the safeguards and controls in the future Agreement with respect to the protection of personal data in the specific context of New Zealand. They are without prejudice to any additional recommendations that the EDPS could make on the basis of further available information during the negotiations.

30. To this end, the EDPS repeats its position from his previous opinions[25] that the Council Decision authorising opening of negotiations pursuant to Article 218 TFEU should contain a reference not only to the procedural legal basis but also to the relevant substantive legal basis, which should include Article 16 TFEU. Next, in line with the principle of purpose limitation, the future Agreement should explicitly lay down the list of the criminal offences regarding which personal data could be exchanged. Furthermore, to ensure the practical implementation of the principle of storage limitation, the future Agreement should specifically provide for periodic review of the need for further storage of the transferred personal data. Finally, given the special importance of the right to information for the exercise of the other data protection rights, the EDPS underlines the need for clear and detailed rules regarding the information that should be provided to the data subjects.

31. The EDPS remains at the disposal of the Commission, the Council and the European Parliament to provide advice at further stages of this process. The comments in this Opinion are without prejudice to any additional comments that the EDPS could make as further issues may arise and would then be addressed once further information is available. To this end, the EDPS expects to be consulted later on the provisions of the draft Agreement before its finalisation.

Brussels, 31 January 2020

Wojciech Rafał WIEWIÓROWSKI

Notes

[1] OJ L 119, 4.5.2016, p. 1.
[2] OJ L 295, 21.11.2018, p. 39.
[3] OJ L 119, 4.5.2016, p. 89.
[4] OJ L 135, 24.5.2016, p. 53.
[5] COM(2015) 185 final.
[6] Council Document 10384/17, 19 June 2017.
[7] Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy http://europa.eu/globalstrategy/en
[8] COM(2019) 551 final.
[9] See directive 1 of the Annex.
[10] For further details see the EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines_en.pdf
[11] See Judgments in Joined Cases C-293/12 and C-594/12 DRI, paragraph 52; Case C-73/07 Satakunnan Markkinapörssi and Satamedia, paragraph 56; Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert, paragraphs 77 and 86.
[12] https://www.privacy.org.nz/
[13] Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand, OJ L 28/12, 30.1.2013
[14] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108.
[15] See EDPS Opinion 2/2018 on eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries, adopted on 14 March 2018, https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_international_agreements_europol_en.pdf
[16] See Point 4.1. of the EDPS Opinion 2/2018.
[17] See Point 4.2. of the EDPS Opinion 2/2018.
[18] See Point 4.3. of the EDPS Opinion 2/2018.
[19] See Point 4.8. of the EDPS Opinion 2/2018.
[20] CJEU judgments in Case C-43/12 Commission v Parliament and Council, para. 29 and Case C-263/14 Parliament v Council, para. 43.
[21] CJEU, Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, para. 232.
[22] Recital 26 of the Europol Regulation.
[23] Case C-201/14, Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenţia Naţională de Administrare Fiscală, ECLI:EU:C:2015:638, in particular para. 32 and 33 where the Court found that *"the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed, and their right to object to the processing of those data" and that "That information concerns the identity of the data controller, the purposes of the processing and any further information necessary to guarantee fair processing of the data"*.
[24] CJEU, Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, para. 220.
[25] See EDPS Opinion 6/2019 on the negotiating mandate of an Agreement between the EU and Japan for the transfer and use of Passenger Name Record data, EDPS Opinion 2/2019 on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence and EDPS Opinion 3/2019 regarding the participation in the negotiations in view of a Second Additional Protocol to the Budapest Cybercrime Convention, available at https://edps.europa.eu/data-protection/our-work/our-work-by-type/opinions_en