Prior Checking Opinion regarding Restrictive Measures (Sanctions) of the European External Action Service (EEAS)

Brussels, 18 December 2015 (2014-0926)

1. Proceedings

On 3 October 2014, the Data Protection Officer (DPO) of the EEAS submitted a notification under Article 27 of Regulation (EC) 45/2001[1] ("the Regulation") concerning "Restrictive Measures (Sanctions) procedures of the EEAS in pursuit of specific foreign and security policy of the EU - Preparation and follow-up" to the EDPS for prior checking.

The notified processing operations were already in place at the time of notification; the deadline under Article 27(4) of the Regulation therefore does not apply.[2]

2. The facts

The EEAS is involved in the preparation and follow-up[3] of sanctions adopted at the EU level against specific natural and legal persons.

In this context, the EEAS (more precisely unit SecPol4) carries out the following tasks:

- To prepare Decisions by the Council of the European Union (Council) and, where applicable, Council Implementing Regulations for all EU sanctions regimes, including autonomous regimes[4], "mixed" EU/UN regimes[5] and regimes implementing UN sanctions[6], where natural persons, legal persons, entities, bodies or groups are designated in relation to imposing a travel ban and/or an asset freeze on them for specific reasons in relation to the natural or legal persons concerned as set out in the statement of reasons in the legal act[7]. The Council has not delegated its implementing powers to the EEAS. The High Representative proposes the legal acts including implementing acts, but the Council retains the decision making function.

[1] OJ L 8/1, 12/01/2001

[2] On 15 October 2014, the EDPS asked several questions for clarification; the EEAS provided answers on 23 February 2015. On 2 October 2015, the draft opinion was sent to the EEAS DPO for comments, which were received on 17 December 2015

[3] On the activities of other EU institutions in this context, see EDPS cases 2010-0426 (European Commission / Foreign Policy Instruments Service, notably for publication of the consolidated list on the internet) and cases 2012-0724 to -0726 (Council, notably for review process and decisions on delisting).

[4] Regimes in which the EU imposes restrictive measures without a UN Security Council resolution.

[5] Regimes in which sanctions imposed by the UN Security Council are implemented in EU law, but additional persons/entities are added.

[6] Sanctions regimes imposed by the UN Security Council and implemented one-to-one in EU law.

[7] Except for sanctions regimes where the Council has delegated the implementing power to the Commission. In these regimes the Implementing Regulation is prepared by the Commission.

- To reply to letters to the EEAS by listed persons or entities, or by their lawyers. In those cases where lawyers have written to the EEAS in representation of their clients, the data processing may include data concerning the lawyers or the law firm representing a listed person or entity. Data concerning the persons or entities listed may also include information on Court cases before an EU Court in relation to such persons and entities.
- In cases where a person or entity writes to the EEAS claiming that a confusion of identity has occurred in relation to a listed person or entity or to point out that due to a similarity in identifying data such confusion may occur, the data of that person or entity may also be retained and processed in order to clarify the situation.
- In the context of a review of the sanctions regimes, in particular where an update of such data would be required in order to ensure the data contained in the Council Decision reflect the current data available. In this case too, the data may be processed in order to prepare an amendment to a Council Decisions and, where applicable, to a Regulation.

Unit SecPol4 coordinates and manages, inter alia, the EU's restrictive measures (sanctions) policy in pursuit of specific foreign and security policy objectives of the EU, including implementation – in cooperation with relevant Commission services – of relevant UN Security Council resolutions, to promote peace and security.

The EU's sanctions policies are a part of the EU's Common Foreign and Security Policy, as laid down in Chapter 2 of the Treaty on European Union. Sanctions Decisions are taken on the basis of Article 29 of the Treaty. The data processing referred to here takes place in this context.

The categories of data subjects are the following:

- Natural or legal[8] persons included or considered for inclusion in travel ban and/or asset freezing lists in sanctions legal instruments, as decided upon in the framework of the EU's Common Foreign and Security Policy
- Lawyers representing listed persons
- Persons who have written to the EEAS in relation to a possible confusion of identity in otherwise in relation to a listed person

The categories of data that may be processed are the following:

- Name (first name/s, last name)
- Gender
- Address
- Date and place of birth
- Nationality, passport and ID card numbers
- Fiscal and social security numbers
- Address or other information on whereabouts
- Function or profession
- Names of the father and of the mother
- Telephone and fax numbers, email address
- Information on the grounds for listing (statement of reasons), possibly including criminal records or proceedings.

The sources of data may be the following:

[8] Insofar as their name allows identifying a natural person.

- for the purposes of preparation:
  - the United Nations (in particular Security Council Resolutions as publicized on the UN website or notified by means of *note verbale* from the UN);
  - EU Member States;
  - EU institutions, in particular the Council or the European Commission (Commission), or EU delegations;
  - The External Action Service;
  - authorities of third states or other international stakeholders[9];
  - public sources;
- as well as, for the purposes of follow-up:
  - all sources listed above for the purposes of preparation;
  - the listed legal or natural person/data subject, or those representing such person;
  - natural persons claiming that a confusion of identity has occurred in relation to a listed person or entity or to point out that due to a similarity in identifying data such confusion may occur.

The EEAS notes that the Council is the legislative authority for the legal instruments concerning restrictive measures (Council Decisions and Council Regulations) and that Council Regulations are prepared by the Commission while the EEAS prepares most Council implementing Regulations. The EEAS also notes that the publication of data in legal acts is ultimately a matter entirely within the discretion of the Council.

Recipients of personal data are the relevant staff in the EEAS, in the EU Delegation(s) dealing with a particular sanctions case, the Council in the context of preparing EU sanctions decisions; in the review process, the EEAS may contact third countries in order to check the veracity of supporting documents.

A privacy statement is publicly available on the EEAS website, but is not proactively communicated to data subjects. In reply to access/rectification requests, restrictions based on Article 20 of the Regulation may be used. The EEAs states that requests deemed legitimate will be answered within 15 working days.

Personal data processed in the notified processing operations will be stored for a period of 5 years following delisting, or 5 years following a Court judgment on the listing (whichever period is longer).

3. Legal analysis

3.1. General remarks

The processing notified forms part of a larger complex of processing operations: regulations establishing restrictive measures under Article 215 TFEU are adopted by the Council, as are Decisions under Article 29 TEU. The Council is the entity that data subjects may take to Court to challenge their listing. It also decides on requests for review and delisting.[10] The Commission is involved in some specific sanctions regimes and provides a constantly updated consolidated public list of persons and entities subject to restrictive measures.[11]

The processing operations notified by the EEAS are very similar to those notified by the Council.[12] For this reason, the recommendations in this opinion are based on the ones issued to the Council. It could be worthwhile for the EEAS to coordinate its activities regarding data

[9] Other than the United Nations.
[10] See joint Opinion in EDPS cases 2012-0724 to -0726.
[11] See Opinion in EDPS case 2010-0426.
[12] See footnote 10.

protection in this area with those of the Council, for example as concerns informing data subjects.

As the processing operations for the preparation and review of sanctions involve different EU institutions, it **should be clearly documented who is responsible for which aspects**, in order to avoid any gaps of accountability. While it is clear that listing decisions are in the end Council decisions, the responsibility for the ancillary processing operations is not always completely clear. This should be remedied. The outcome of this documentation of responsibilities could even be that there is joint controllership for certain parts of the processing.

This Opinion, as well as the recommendations, applies to the general procedures in place at the EEAS for processing personal data in the context of restrictive measures. It is not limited to the sanctions regimes currently in place, but is an "umbrella opinion" applying also to future sanctions regimes imposing restrictive measures insofar as the processing operations foreseen are substantially identical to those analysed in this prior check.

3.2. Prior checking

Article 27(1) of the Regulation subjects to prior checking by the EDPS all "*processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*". Article 27(2) of the Regulation contains a list of processing operations that are likely to present such risks.

Point (a) of this list includes the processing of personal data related to "*suspected offences, offences, criminal convictions or security measures*" as one such risky processing operation. Such data may be processed in the context of the notified processing operations on restrictive asset freezing measures as the reasons for listing often refer to criminal offences and convictions.

In addition, the processing operations also falls under Article 27(2)(d) of the Regulation as it concerns the processing of personal data with the "*purpose of excluding individuals from a right, benefit or contract*". The purpose of the notified processing operations is to exclude listed individuals from certain rights, notably the full enjoyment of their property rights and access to their funds and economic resources.

Both of these points have been mentioned in the notification form. The notified processing operations are therefore subject to prior checking.

Since prior checking is designed to address situations that are likely to present certain risks, the Opinion of the EDPS should be given prior to the start of the processing operation. In this case, however, the processing operations have already been established. Accordingly, the time limits of Article 27(4) of the Regulation do not apply. This case has been dealt with on a best-effort basis.

In particular given the significant risks for data subjects, the EDPS regrets the long delay between the start of the processing operations and the notification. The recommendations made by the EDPS should be implemented without undue delay.

3.3. Lawfulness of the processing

Article 5 of the Regulation contains the conditions for lawfulness of processing. Article 5(a) declares lawful processing that is "*necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in a Community institution or body*".

According to Article 29 of the TEU, the High Representative for Foreign and Security Policy may submit proposals relating to common foreign and security policy to the Council. This includes the submission of proposals for targeted sanctions against specific persons. This provision covers the processing of personal data in the preparation of sanctions

Similarly, replying to enquiries from listed persons or persons claiming confusion with a listed person can be covered under this legal basis, as well as under the specific decisions and regulations for each specific regime, provided that they provide for a relevant role for the EEAS.

For the review process, the specific sanctions regimes contain provisions on the review process. The EEAS should follow its role as defined there.

3.4. Processing of special categories of data

The notified processing operations may involve the processing of special categories of data under Article 10 of the Regulation, notably of data relating to (suspected) "*offences, criminal convictions or security measures*". Such data can notably be processed as part of the statements of reasons.

According to Article 10(5) of the Regulation, such data may only be processed if "authorised by the Treaties […] or other legal instruments adopted on the basis thereof".

The EDPS would like to highlight that the very fact of appearing on the list of persons whose assets are to be frozen can render the published personal data as such "sensitive", in that listings related to terrorism or human rights infringements imply the suspicion of being related to criminal activity. This is not necessarily the case for all listings. In the context of this prior check, sensitive data are in general the grounds for listing which can include convictions, arrests and imprisonments.

Whereas the processing of special categories of data for the preparation of listing decisions in general could be based directly on Article 29 TEU, the publication of special categories of data should be directly provided by the specific legal basis for each restrictive measure.

3.5. Data Quality

According to Article 4(1)(c), data must be adequate, relevant and non-excessive in relation to the purposes for which collected and/or further processed. Additionally, data must be accurate and where necessary kept up to date pursuant to Article 4(1)(d).

With regard to the criteria of data processed being "*adequate, relevant and non-excessive*", the EDPS would like to emphasise that personal data published should be strictly limited to what is necessary to identify the person concerned. In this respect, data on family members (e.g. parents) should only be included in the published lists when necessary in order to identify the listed person.

As regards the requirement that data must be accurate and kept up to date, this relates to the rights of access and to rectify data (see point 3.10 below). This ensures that data processed are accurate, complete and up to date in the meaning of Article 4(1)(d) of the Regulation.

Given the serious consequences that restrictive measures have on affected persons, utmost attention must be given to the accuracy of the personal data. While the review procedure for listed persons can serve to rectify mistakes resulting in wrong listings, **the EEAS should**

make the utmost efforts to ensure the quality of the data already at the stage of establishing the lists. [13]

3.6. Conservation of data/ Data retention

Article 4(1)(e) of the Regulation states that data should be kept in a form which permits identification of data subjects for no longer than is necessary for which the data are collected and/or further processed.

Personal data will be stored for a period of 5 years following delisting, or 5 years following a Court judgment on the listing (whichever period is longer).

This period appears non-excessive.[14]

3.7. Transfer of data

Depending on the recipient, specific rules for transfers of personal data apply under Article 7 to 9 of the Regulation.

For all transfers within the EEAS or to other EU institutions and bodies Article 7 of the Regulation applies. This Article states that data may only be transferred if "*necessary for the legitimate performance of tasks covered by the competence of the recipient*". **In addition recipients should be reminded in case of such transfer that they should process data only for the purposes for which they were transmitted.**

The EEAS indicated that there were no Article 8 transfers.

The EEAS also mentioned possible transfers to third countries in order to check the veracity of supporting documents provided by listed persons during the review process.

Transfers to recipients other than EU institutions and bodies and which are not subject national legislation implementing Directive 95/46/EC are regulated in Article 9 of the Regulation. In the case at hand, such transfers would appear to fall under the derogations foreseen in Article 9(6).[15] The **EEAS should ensure that such transfers only take place when the criteria of Article 9 are fulfilled**.

3.8. Processing of personal number or unique identifier

Article 10(6) of the Regulation provides that "*the European Data Protection Supervisor shall determine the conditions under which a personal number or other identifier of general application may be processed by a Community institution or body*".

Sometimes, national identification card or passport numbers can also be included in the publicly accessible lists. The publication of such special categories of data can be necessary in order to allow economic operators to implement the freeze and to identify the correct person, avoiding risks of coincidence of names and in relation to persons who have different aliases.

While the EDPS understands that the need to process unique identifiers of individuals in order to correctly identify the persons concerned by the asset freezing measures, he would like to encourage an **evaluation, in general and on a case by case basis, of the need to process**

[13] See also EDPS Opinion of 07/05/2014 in cases 2012-0724 to -0726, pages 14-16 and EDPS Opinion of 22/02/2012 in case 2010-0426, pages 23-25 (published versions).
[14] It is identical to the periods found to be non-excessive in cases 2012-0724 to -0726.
[15] For further information see point 6 of the EDPS position paper on the transfer of personal data to third countries and international organisations by EU institutions and bodies, available here: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf. See also section 3.7 in EDPS opinion in cases 2012-0724 to -0726.

such data in case persons concerned can be easily identified without recourse to these data. As identification card or passport numbers can act as identifiers across different contexts, their processing should be limited to what is necessary; if persons can be readily identified without recourse to this information, then it should not be processed.

3.9. Information to the data subject

The processing operations concern personal data which have not been obtained by the data subject. Article 12 of the Regulation lists the information the data controller must provide to the data subject in relation to the processing activities. This information must include *–inter alia–* the identity of the controller, the purposes of the processing, the legal basis, the recipients of the data, the existence of the rights of access to and the right to rectify the data.

In principle, according to Article 12(1), data subjects must be informed of the processing of personal data about them which has not been obtained directly from them "*at the time of undertaking the recording of personal data or, if a disclosure to a third party is envisaged, no later than the time when data are first disclosed*".

Article 12(2) states that the information obligation shall not apply if providing it would involve a "disproportionate effort".

Exemptions from the right to information are foreseen in Article 20(1)(a) and (d) of the Regulation, allowing restrictions if they are necessary for "*the prevention, investigation, detection and prosecution of criminal offences*" or "*the national security, public security or defence of the Member States*", respectively. In these cases, data subjects have to be informed of the principal reasons for the restriction and their right to recourse to the EDPS (Article 20(3)); even the provision of this information may be deferred for as long as it would deprive the restriction of its effect (Article 20(5)).

Currently, there is no proactive provision of information to the data subject.

The exemption of Article 12(2) can be used if providing the information would indeed require a disproportionate effort, which cannot be claimed if the address or other contact information for the listed person is known.

A deferral until publication of the listing decision may be justified under Article 20 for the initial listing decision, as otherwise there would be no 'surprise effect' and to-be-listed persons could move their assets elsewhere. However, the deferral of the information to be provided pursuant to Article 12 of the Regulation can only be relied on for the first listing decision, but not for subsequent listing decisions in the case that new grounds for listing become available.[16]

Therefore, the EEAS **should proactively provide information to data subjects where the criteria of Article 12(2) and Article 20 of the Regulation are not fulfilled.**

3.10. Right of access and rectification

Article 13 of the Regulation grants data subjects a right of access to data stored about them. Article 14 grants the right to have inaccurate or incomplete data rectified "without delay". According to Article 20 of the Regulation, certain restrictions may be imposed on these rights if they are necessary for a number of reasons enumerated in that Article.

[16] See T 228/02 paras. 128-130. This line was confirmed in the subsequent cases T 284/08, paras. 36, 37, 44 and in the appeals case C 27/09, paras. 61, 62, 65-67.

The EEAS stated that it may impose such restrictions in response to such requests. The EDPS would like to point out that **it is a good practice to document internally any assessment with regard to Article 20 of the Regulation made by the EEAS**.

The justification should provide concrete reasons, linked to the specific case, as to why the application of a restriction is necessary. General considerations, such as simply quoting (parts of) Article 20 of the Regulation, are not enough.

It may also be necessary to have two parts to the justification. The reason is that under Article 20(3) of the Regulation, the data subject has to be informed of the "principal reasons" for the restriction. This should go beyond merely citing the relevant provisions of Article 20(1), but need not contain the full justification.

The full reasoning should be documented internally at the time of applying the restriction, for example in a note to the file. This documentation should show why the restriction constitutes a necessary measure to safeguard one (or more) of the interests to be protected under Article 20(1) points (a) to (d) of the Regulation. Restrictions should be limited in time and should be reviewed.

3.11. Right to object

Article 18(a) of the Regulation grants data subjects a right "*to object at any time, on compelling legitimate grounds relating to his or her particular situation, to the processing of data relating to him or her, except in the cases covered by Article 5(b), (c) and (d)*".

The EDPS is aware of the fact that the activities of establishing and amending the lists and the processing connected to the publication and information exchange, which all involve processing of personal data, are at the core of the purpose of the asset freezing measures. Indeed the whole process is set up in order for economic operators to be able to quickly and clearly identify the names and personal details of persons whose assets have to be frozen on the basis of UN or EU autonomous listings.

However, Article 18(a) requires that the objection has to be based on "*compelling legitimate grounds*" and that the objection has to be "*justified*". A listed person would have to meet this standard in order to be able to object successfully.

3.12. Security measures

[…]

4. Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the considerations above are fully taken into account. Specifically, the EEAS should implement the following recommendations:

- clearly document which entity is responsible for which aspects of the processing;
- make the utmost efforts to ensure the quality of the data already at the stage of establishing the lists;
- remind Article 7 recipients that they should process data only for the purposes for which they were transmitted;
- ensure that transfers to Article 9 recipients only take place when the criteria of that Article are fulfilled

- evaluate, in general and on a case by case basis, the need to process unique identifiers in case persons concerned can be easily identified without recourse to them;
- proactively provide information to data subjects where the criteria of Article 12(2) and Article 20 of the Regulation are not fulfilled;
- when using Article 20 to restrict data subjects' rights, document the full reasoning internally at the time of applying the restriction, for example in a note to the file.

Done at Brussels, 18 December 2015

(**signed**)

Wojciech Rafał WIEWIÓROWSKI