From:	European Data Protection Supervisor
To:	[redacted]
CC:	[redacted]
Sent at:	28/03/18 17:20:39
Subject:	our ref. 2018-0207 D-0714:EDPS informal comments on the draft Proposal for a Directive establishing common minimum standards for the protection of persons reporting on breaches in specific Union policy areas

Dear Madame,

P ease f nd herew th attached a scanned etter and ts annex sent to you by nterna ma .

S ncere y yours

EDPS Secretariat
Te . +32 2 283 19 00 | ax +32 2 283 19 50
edps@edps.europa.eu
European Data Protection Supervisor
Posta address: Rue W ertz 60, B 1047 Brusse s
Off ce address: Rue Montoyer 30, B 1040 Brusse s
@EU_EDPS www.edps.europa.eu

Informal comments of the EDPS on the draft proposal for a Directive establishing common minimum standards for the protection of persons reporting on breaches in specific Union policy areas

1. Introduction

The present informal comments concern the draft Proposal for a Directive of the European Parliament and of the Council establishing common minimum standards for the protection of persons reporting on breaches in specific Union policy areas ("the draft Proposal").

The overall objective of the draft Proposal is to enhance the detection of breaches in specific policy areas of Union law which can cause serious harm to the public interest by ensuring effective protection of whistleblowers and by introducing effective reporting channels.

We welcome that we have been given the opportunity to provide informal comments to the Commission before the adoption of the draft Proposal.

2. Comments

- We welcome that the draft Proposal refers in several recitals and Articles to the protection of personal data. Foremost, Article 16 of the draft Proposal explicitly states that any processing of personal data carried out pursuant to this Directive, including the exchange or transmission of personal data by the competent authorities, falls under Regulation (EU) 2016/679 ("GDPR") and at Union level under Regulation (EC) No 45/2001.

- Recitals 12, 31 and 58 of the draft Proposal seem to implicitly refer to the data breach notification as laid down in Article 33 of the GDPR as an example for already existing internal and external reporting channels. We recall that Article 33 of the GDPR does not contain any reference to internal or external reporting channels, it merely obliges controllers to inform the supervisory authority of a personal data breach. We therefore recommend to reconsider these references.

- In recital 54 of the draft Proposal the protection of personal data of the reporting person and the concerned person are explicitly stated. We want to point out that a report sent to the competent authority will most likely contain references to third persons, like witnesses, colleagues or other employees. For the sake of clarity and in order to raise awareness, we recommend to include in recital 54 also a reference to the protection of the data of such third persons.

- We recall that personal data must be collected for specified, explicit and legitimate purposes and must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.[1] Hence, the personal data collected and processed for the purpose of the draft Proposal, i.e. the detection of unlawful activities in specific policy areas of Union law, should be limited to such data which are relevant

[1] Article 5(1)(b) and (c) of the GDPR; see also Article 6(1)(b) and (c) of Directive 95/46.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

for the specific case.[2] Consequently, the draft Proposal should set out explicitly which personal data or which categories of personal data may (or shall) be processed. It should also explicitly stipulate that the processing of personal data should be limited to such data which are strictly and objectively necessary to verify the allegations made. The level of detail of the draft Proposal with respect to the possibility (or obligation) to process specific (categories of) personal data will have implication for the legal basis for the processing (e.g. processing necessary for compliance with a legal obligation to which the controller is subject (Article 6(1)(c) of the GDPR); or necessary for the performance of a task carried out in the public interest (Article 6(1)(e) of the GDPR). This, in turn, may have an impact on the rights data subjects will have (e.g. in accordance with Article 21 of the GDPR, a right to object when the processing of personal data is based on Article 6(1)(e) of the GDPR).

- Furthermore, the draft Proposal should stipulate that personal data which are not relevant for a specific case should immediately be deleted by the competent authorities, as this will help to avoid the collection of excessive personal data. Moreover it should be made clear, that personal data should not be further processed in a manner that is incompatible with the envisaged purpose.[3]

- We would also like to recall that personal data should not be kept in a form which permits identification of the individual concerned for longer than necessary for the purpose(s) of the processing.[4] Against this background, we observe that the draft Proposal does not lay down a fixed - and proportionate - retention period, following the expiry of which the personal data should be deleted. We recommend to introduce a relevant provision to this effect.

- We note that Articles 4 and 5 of the draft Proposal obliges the Member States to establish internal and external reporting channels in order to receive and handle information by whistleblowers, whereas these channels should be secure and ensure confidentiality. Even though we welcome that recital 54 foresees that in addition to Regulation (EU) 2016/679 the competent authorities should establish adequate data protection procedures, we recommend to introduce - for the sake of clarity - a reference to Article 25 and Article 35 of the GDPR in this context.

- We welcome the fact that in Articles 4 and 7 of the draft Proposal a need to know principle is established, as this will contribute to an enhanced protection of the reporting person and the concerned person.

- In accordance with Article 9 of the draft Proposal, Member States shall ensure that the competent authorities publish on their websites in a separate, easily identifiable and accessible section certain information about the communication channel, the applicable procedures, etc. We recommend to include in this Article also information pursuant to Article 13 of the GDPR, since the information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection.

- Moreover, we recommend that all individuals affected by a report - i.e. the reporting person, the concerned person and third persons - should be provided with a specific

[2] http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf.
[3] Article 5(1)(b) of the GDPR; see also Article 6(1)(b) of Directive 95/46.
[4] Article 5(1)(c) of the GDPR; see also Article 6(1)(e) of Directive 95/46.

data protection statement as soon as practicably possible. Such a statement should include information on the identity and contact details of the controller, possible recipients or categories of recipients of the personal data and the data subjects' rights, in particular the right of access, the right to rectification and erasure and the right to restriction of processing. With regard to the reporting person such a data protection statement could be communicated in the course of the follow-up (Article 4(d) and 5(2) (b) of the draft Proposal), whereas for third persons, in particular witnesses, before they are being interviewed. In cases where the information of the concerned person would impede the investigation, the communication of the data protection statement could be deferred as long as such a deferral is considered necessary.

Brussels, 28 March 2018

GIOVANNI BUTTARELLI
SUPERVISOR

[redacted]
Director-General
DG Justice and Consumers
European Commission
B-1049 Brussels

Brussels, 28 MAR 2018
[redacted]D(2018)0714 **C2018-0207**
Please use edps@edps.europa.eu for all correspondence

Subject: EDPS informal comments on the draft Proposal for a Directive establishing common minimum standards for the protection of persons reporting on breaches in specific Union policy areas

Dear [redacted],

I am writing in reply to a consultation of the EDPS on 16 March 2018, in connection with the inter-service consultation concerning a draft proposal for a Directive establishing common minimum standards for the protection of persons reporting on breaches in specific Union policy areas.

We welcome the informal consultation of the EDPS at this stage of the procedure. You will find attached a note containing our preliminary comments.

These comments are without prejudice to a formal Opinion that may follow under Article 28(2) of Regulation 45/2001. In that Opinion, also other relevant elements may be discussed.

Our services are at your disposal, should you need any clarification in relation with this letter.

Yours [redacted]

Giovan[redacted]

Cc: [redacted]

Contact person: [redacted]