I. RECORD OF PERSONAL DATA PROCESSING OPERATION (Art. 31)

1.	Name of the processing operation	**360° feedback exercise**
2.	Reference number/Issue	ETF-DPR-42/Issue 1
3.	Date	11/10/2019
4.	Business owner	Nadège Perrine Head of HR Unit Nadège.Perrine@etf.europa.eu
5.	Controller	Cesare Onestini Director of the ETF Cesare.Onestini@etf.europa.eu
6.	Joint controller(s)	Not applicable
7.	Processor(s)	Not applicable
8.	Data protection officer	Tiziana Ciccarone / Laurens Rijken DataProtectionOfficer@etf.europa.eu

9.	Purpose of the processing	• The purpose of the processing is to provide feedback to all managers and team leaders on their managerial performance and behaviour. Further processing: The resulting individual reports will be considered in the current performance management exercise
10.	Legal basis for the processing	• ETF Governing Board Decision ref. GB/18/DEC/014 – implementing rules on middle management staff • Staff Regulations, Condition of Employment of Other Servants of the European Union (CEOS) articles 43, 44 • ETF Governing Board Decision ref. GB/15/DEC/008 Implementing articles 43 and 44 of the SR for temporary staff; • Minutes of the Management Team meeting of 28 January 2019 adopting the follow up to the staff engagement survey, presented to all staff on 1 February 2019
11.	Categories of data subjects	Receiving 360° feedback: ETF Director, managers and team leader Providing 360° feedback: All ETF Temporary, Contract, Local Agents and SNEs
12.	Categories of personal data	For the managers / team leaders who receive feedback: Name, e-mail and the feedback they receive on their performance and behaviour For the staff members giving feedback: Name, email and feedback given
13.	Time limits for keeping of data	• The individual feedbacks are destroyed by the contractor once the reports are produced. • The reports are destroyed by the contractor once they are given to the relevant managers / HR Unit at the ETF. • The individual reports are retained for a period of two calendar years following the year in which they are distributed.by the respective manager and Director after which they are destroyed by them. • The overall reports are retained for a period of four calendar years following the year in which they are distributed, for comparison purposes in case the exercise is repeated.
14.	Categories of ETF recipients of data	• Managers / team leaders receiving feedback -> individual reports • Their manager -> individual reports of the managers / team leaders under their responsibility and, if applicable, overall report for their

		department
		• The Director -> individual reports of all managers / team leaders and overall report for all managers / team leaders
15.	Categories of external recipients of data	• The contractor entrusted with the organisation and performance of the exercise
16.	Transfers of data to third country or international organisation	Not applicable

17.	Technical and organisational security measures	• The contractor's on-line tool uses an anonymity mechanism – which means that the feedback and replies given cannot be linked to the name of the respondent. Access is on need to know basis by contractor staff with user authentication. • Paper reports are directly handed to the recipients • No electronic copies
18.	Information to the data subject	Provided in privacy statement

II.   COMPLIANCE CHECK AND RISK SCREENING OF PERSONAL DATA PROCESSING OPERATION (Art. 26 and 39)

Name of the processing operation	**360° feedback exercise**
Reference number	ETF-DPR-42/Issue 1
Date	11/10/2019

A.   Compliance check

19.	**Lawfulness** (Legal basis and necessity for processing, point 10) ☐ Necessary for performance of tasks in the public interest attributed by EU or MS legislation ☒ Necessary for the management and functioning of the organisation ☐ Necessary for compliance with legal obligation incumbent on controller ☐ Necessary for performance of a contract to which the data subject is party ☐ The data subject has given consent ☐ Necessary in order to protect the vital interests of the data subject or of another natural person	Details (if needed):
20.	**Purpose definition** (Point 9) • Do you list all purposes? • Are the purposes specified, explicit, legitimate? • Where information is also processed for other purposes, are you sure that these are not incompatible with the initial purpose(s)?	• Yes • Yes • Yes
21.	**Data minimisation** (Point 12) • Do you really need all data items you plan to collect? • Are there any you could do without?	• Yes • No
22.	**Accuracy** (Point 12) • How do you ensure that the information you process about people is accurate? • How do you rectify inaccurate information?	• Information processed automatically in on-line tool. • Rectification takes place upon request of data subject by outsourced contractor
23.	**Storage limitation** (Point 13) • Explain why you chose the storage period(s) mentioned • Are they limited according to the maximum or minimum "as long as necessary, as short as possible"? • In case you only need some information for longer, can you split storage periods?	• The period of two calendar years for individual reports, following the year in which they are distributed, is to allow for appeal and audit trail The period of four calendar years for aggregate reports, following the year in which they are distributed, is to allow for comparison purposes in case the exercise is repeated • As short as possible • See first bullet
24.	**Transparency** (Point 18) • How do you tell people about your processing? • If you do not want to inform people (or only	• Privacy statement is attached in invitation to exercise. • Not applicable

	inform them after the fact), consult your DPO	
25.	**Data subjects rights** (Point 18) • Can people contact you if they want to know what you have about them, want to correct or delete the data, have it blocked or oppose to the processing? • Could there be situations where you would want to refuse e.g. granting access? In case so please describe them	• Yes • Not applicable

B.   Risk screening

26.	**Does the processing involve any of the following?**		
	• Data relating to health, (suspected) criminal offences or otherwise considered sensitive	☐ Yes	☒ No
	• Evaluation, automated decision- making or profiling	☐ Yes	☒ No
	• Monitoring data subjects	☐ Yes	☒ No
	• New technologies that may be considered intrusive	☐ Yes	☒ No
	• Exclusion databases	☐ Yes	☒ No
	• Large-scale processing of special categories of personal data (disease surveillance, pharmacovigilance, central databases for law-enforcement cooperation)	☐ Yes	☒ No
	• Internet traffic analysis breaking encryption	☐ Yes	☒ No
	• E-recruitment tools automatically pre-selecting/excluding candidates without human intervention	☐ Yes	☒ No
	• Management of personal files	☐ Yes	☒ No
	• Staff evaluation procedures (annual appraisal)	☒ Yes	☐ No
	• 360° evaluations for helping staff members develop training plans	☒ Yes	☐ No
	• Staff selection procedures	☐ Yes	☒ No
	• Establishment of rights upon entry into service	☐ Yes	☒ No
	• Management of leave, flexitime and telework	☐ Yes	☒ No
	• Access control systems (non biometric)	☐ Yes	☒ No
	• Video surveillance (limited scale)	☐ Yes	☒ No

C.   Conclusions

	Actor	Date	Signature
27.	**Business owner** Nadège Perrine Head of HR Unit **Conclusion** Threshold assessment required according to Risk screening		
	Data Protection Officer: Tiziana Ciccarone / Laurens Rijken **Conclusion** I confirm that a threshold assessment is required		

III.   THRESHOLD ASSESSMENT OF PERSONAL DATA PROCESSING OPERATION (Art. 26 and 39)

Name of the processing operation	**360° feedback exercise**
Reference number	ETF-DPR-42/Issue 1
Date	11/10/2019

A.   Criteria for high risks identification

28.	Systematic and extensive **evaluation** of personal aspects or scoring, including profiling and predicting	☐ Yes	☒ No
	Examples: a bank screening transactions in accordance with applicable law to detect possibly fraudulent transactions; profiling staff based on their transactions in a case management system with automatic reassignment of tasks. *Counterexamples: standard appraisal interviews, voluntary 360° evaluations for helping staff to develop training plans.*		
	….		
29.	Automated-**decision making** with legal or similar significant effect: processing that aims at taking decisions on data subjects	☐ Yes	☒ No
	Example: automated staff appraisal ('if you're in the lowest 10% of the team for the number of cases dealt with, you'll receive a "unsatisfactory" in your appraisal, no discussion'). *Counterexample: a news site showing articles in an order based on past visits of the user.*		
	….		
30.	Systematic **monitoring**: processing used to observe, monitor or control data subjects, especially in publicly accessible spaces. This may cover video-surveillance but also other monitoring, e.g. of staff internet use.	☐ Yes	☒ No
	Examples: covert CCTV, smart CCTV in publicly accessible spaces, data loss prevention tools breaking SSL encryption, tracking movements via location data. *Counterexample: open CCTV of garage entry not covering public space.*		
	….		
31.	**Sensitive data**: data revealing ethnic or racial origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for identification purposes, data concerning health or sex life or sexual orientation, criminal convictions or offences and related security measures or otherwise considered sensitive.	☐ Yes	☒ No
	Examples: pre-recruitment medical exams and criminal records checks, administrative investigations & disciplinary proceedings, any use of 1:n biometric identification. *Counterexample: photos are not sensitive as such (only when coupled with facial recognition / biometrics or used to infer other sensitive data).*		
	….		
32.	Data processed on a **large scale**, whether based on number of people concerned and/or amount of data processed about each of them and/or permanence and/or geographical coverage	☐ Yes	☒ No
	Example: European databases on disease surveillance. *Counterexample: invalidity procedures under Article 78 of the Staff Regulations in a medium-sized EUI.*		
	….		
33.	Datasets **matched or combined** from different data processing operations performed for different purposes and/or by different data controllers in a way	☐ Yes	☒ No

	that would exceed the reasonable expectations of the data subject.		
	Examples: cross-checking access control data and self-declared working hours following a suspicion of fraudulent declarations in an administrative inquiry (following the applicable rules). *Counterexample: further use of data processed for a grant application when auditing the grant process.*		
	….		
34.	Data concerning **vulnerable data subjects**: situations where an imbalance in the relationship between the position of the data subject and the controller can be identified.	☐ Yes	☒ No
	Examples: children, asylum seekers. *Counterexamples: delegates in a Council Working Party (for attendance lists), members of expert groups (for travel cost).*		
	….		
35.	**Innovative** use or applying technological or organisational solutions that can involve novel forms of data collection and usage. Indeed, the personal and social consequences of the deployment of a new technology may be unknown	☐ Yes	☒ No
	Examples: machine learning, connected cars, social media screening of job applicants. *Counterexample: 1:1 biometric access control using fingerprints.*		
	….		
36.	**Preventing** data subjects from **exercising a right** or using a service or a contract.	☐ Yes	☒ No
	Examples: exclusion databases, credit screening. *Counterexample: determination of rights upon entry into service (e.g. expatriation or dependent child allowances).*		
	….		

B.   Conclusion

	Actor	Date	Signature
37.	**Business owner** Nadège Perrine Head of HR Unit **Conclusion** No further action required		
	Data Protection Officer: Tiziana Ciccarone / Laurens Rijken **Conclusion** I confirm that no further action is required		
	Data Controller Cesare Onestini, Director of the ETF		