European Asylum Support Office

SUPPORT IS OUR MISSION

Data Protection Impact Assesment (DPIA) Methodology

General Guidelines: you will complete this impac assessment (DPIA) in 4 steps

- 1st step: fill in the **Knowledge Base** with information about your processing operation
- 2nd step: based on the information of the Knowledge Base, answer the questions of the **DPIA Template (Part I)**, which will ask you to assess and rate various Data Protection risks
- 3rd step: based on the answers you provided in the DPIA Template (Part I), you will describe the measures you envisage to **address/mitigate risks (Part II)**
- 4th step: you will then give a **general conclusion** about the Data Protection Impact of your operation **(Part III)**

Knowledge Base

Description of the envisaged processing operation

This part is meant to provide a general overview of the envisaged processing operation.
The different steps you will identify within the processing operation will serve as a base to fill in the risk assessment and the necessity and proportionality assessment.

Flowchart
What personal data do we collect?
Identification data (name or pseudo/alleged name, username, user identification and geographical area) (Occasionally) Certain personal characteristics (age, gender, nationality) Views and/or comments on migration routes, smuggling of human beings/human trafficking and asylum processes Images and videos / any other information published on a website or social media page.
From where / whom do we get that information?
Posts made by users in social media (Facebook, Instagram, YouTube, Twitter) which are relevant to EU asylum and migration issues, within Arabic, Pashto, Dari, Urdu, Turkish, Russian, Tigrinya, Kurmanji Kurdish, Pidgin English, Hausa, Edo, as well as French communities.
What we do with this information?

1

The information consulted by SMM reaserchers is translated directly and mentally into English and transcribed without the use of any IT tools. They are simultaneously transcribed into the draft report. The social media posts are not collected, recorded, stored, retrieved, transmitted, disseminated or shared with third parties. The same applies to the original text of any posts in the source language, which are not copy-pasted or transferred. The reports are shared with stakeholders.
Where do we keep it?
No personal data is either stored or transmitted. The processing of personal data is limited to the consultation of social media posts by SMM researchers on their web browsers. On-screen visual texts are directly translated into English (not copy-pasted, saved, stored or transmitted) without IT tools, while any images which contain personal data are directly redacted to be unrecognizable before being saved, thus making the process non-reversible. The cached memory of the web browsers (internet history of pages which have been visited) is deleted at the end of every week in order to ensure that no links to the visited social media pages are stored. No links / hyperlinks are included in the SMM Reports.
Who do we give it to? / Do we share this with other stakholders?
No personal data is either stored or transmitted.

Detailed description of the purpose(s) and supporting assets			
Your process may include the following steps. Please fill in the blanks for the steps that are included in your process.	Description of the process	Description of the purpose. Please distinguish between purposes when necessary.	Supporting assets Please refer to the typology of supporting assets provided below and indicate for each step you identified which are the supporting assets.
Collection of the personal data			
Merging datasets			
Organising/structuring the data			
Retrieving/consulting/using the data	Relevant social media posts are viewed by SMM reasearchers and are translated directly and mentally into English and transcribed without the use of any IT tools. They are simultaneously transcribed into the draft report. The	The purpose of the SMM is to provide EASO management and relevant stakeholders (Member States, European Institutions and EU Agencies, UNHCR, IGC, Interpol and IOM) with reports on the latest shifts in asylum and migration	Social media posts are viewed by SMM reaserchers via the web browser on their computers. The information is then translated into the text of the draft SMM report using Word documents. The final version of the SMM Report is issued as a

	social media posts are not collected, recorded, stored, retrieved, transmitted, disseminated or shared with third parties. The same applies to the original text of any posts in the source language, which are not copy-pasted or transferred.	routes, smuggling offers and the discourse among social media community users on key issues – flight, human trafficking and EU+ asylum systems/processes.	PDF document.
Editing/altering the data	Any screenshots used to illustrate the final version of the SMM Reports are created by the SMM reaserchers using a snipping tool, which enables for the blacking out/redacting of images and the blurring of any personal data such as names and phone numbers that may have been included in the original post. The process is irreversible.	No personal data is included in the SMM reports.	Windows snipping tool.
Discolsing/ransferring the data			
Restricting the access to the data			
Storing of the data			
Erasing/destroying the data	No personal data is included in the SMM reports. The information viewed in social media posts is translated mentally by SMM researchers into the draft text of the SMM reports. The cached memory of the web browsers (internet history of pages which have been visited) is deleted at the end of every week in order to ensure that no links to the visited social media	After the SMM researchers consult the social media posts, no further processing operation is deemed necessary (purpose of the SMM Reports). All possible measures are taken to keep any personal data out of the SMM Reports.	Web browser. Cache memory deleted every week.

3

	pages are stored.		
Other			

Interaction with other processes	
Does this process rely on personal data being fed in from other systems? (Y/N)	No
Are the data from this process re-used in other processes? (Y/N)	No

Knowledge base for the description of supporting assets Typology of supporting assets		
Information systems	Hardware and electronic data media	Example: Computers, communication relays, USB drives, hard drives
	Software	Example: Operating systems, messaging, databases, business application
	Computer channels	Example: Computer channels: Cables, WiFi, fiber optic
Organisations	People	Example: Users, IT administrators, policymakers
	Paper documents	Example: Print, photocopies, handwritten documents
	Paper transmission channels	Example: Mail, workflow

Knowledge base to fill in the DPIA Template (see Part I below)

Rating likelihood			
1. Negligible	2. Limited	3. Significant	4. Maximum
It does not seem possible that the data protection principle (fairness, transparency, etc.) could be affected.	It seems difficult that the data protection principle (fairness, transparency, etc.) could be affected.	It seems possible for the data protection principle (fairness, transparency, etc.) to be affected.	It seems extremely likely that the data protection principle (fairness, transparency, etc.) would be affected.

Rating impact			
1. Negligible	2. Limited	3. Significant	4. Maximum
Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem.	Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties.	Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties.	Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome.
Examples	Examples	Examples	Examples
Physical : classical negligible physical impacts include lack of adequate care for a dependent person (minor, person under guardianships), transient headaches.	**Physical** impacts : minor illness, lack of care leading to a Minor but real harm, Defamation resulting in physical or psychological retaliation.	**Physical** impacts : Serious physical ailments causing long-term harm, Alteration of physical integrity (following an assault, an accident at home, work, etc.)	**Physical** impacts:Long-term or permanent physical ailments (e.g. due to disregard of contraindications), Death , Permanent impairment of physical integrity.
Material impacts : - Loss of time in repeating formalities or waiting for them to be fulfilled- Receipt of unsolicited mail (e.g. spams)- Reuse of data published on websites for the purpose of targeted advertising (information to social networks, reuse for paper mailing)- Targeted advertising for common consumer products	**Material** impacts : - Unanticipated payments (e.g. fines imposed erroneously), - Denial of access to services, blocked account - Lost opportunities of comfort (i.e. cancellation of leisure, termination of an online account)- Missed career promotion- Receipt of unsolicited targeted mailings likely to damage the reputation of data subjects- Cost rise (e.g. increased insurance prices)- Non-updated data (e.g. position held previously)- Processing of incorrect data creating malfunctions - Targeted online advertising on a private aspect that the individual wanted to keep confidential- Inaccurate or inappropriate profiling	**Material** impacts: - Non-temporary financial difficulties (e.g. obligation to take a loan)- Targeted, unique and non-recurring, lost opportunities (e.g. home loan, refusal of studies, internships or employment, examination ban)- Prohibition on the holding of bank accounts- Damage to property- Loss of housing, Loss of employment- Separation or divorce- Financial loss as a result of a fraud (e.g. after an attempted phishing), Misappropriation of money not compensated- Blocked abroad	**Material** impacts:- Financial risk- Substantial debts- Inability to work- Inability to relocate- Loss of evidence in the context of litigation- Loss of access to vital infrastructure (water, electricity)
Moral impacts:- annoyance caused by information received/requested- Fear	**Moral** impacts : - Refusal to continue using information systems - Minor but	**Moral** impacts:- Serious psychological ailments (depression, phobia)- Feeling	**Moral** impacts :- Long-term or permanent psychological ailments-

5

of losing control over one's data- Feeling of invasion of privacy without real or objective harm (e.g. commercial intrusion)- Lack of respect for the freedom of online movement due to the denial of access to a commercial site	objective psychological ailments (defamation, reputation)- Relationship problems with personal or professional acquaintances (e.g. image, tarnished reputation)- Feeling of invasion of privacy without irreversible damage- Intimidation on social networks	of invasion of privacy with irreversible damage- Feeling of vulnerability after a summons to court- Feeling of violation of fundamental rights- Victim of blackmailing- Cyberbullying	Criminal penalty- Abduction- Loss of family ties- Inability to sue- Change of administrative status and/or loss of legal autonomy (guardianship)

DPIA Template - Part I

Impact Assesment

Part I. A. – Necessity and Proportionality Assessment

Necessity Need for the processing in order to achieve aims assigned to the organisation		**Proportionality** Ensure that advantages resulting from processing are not outwieghted by the disadvantages that processing causes			
How and why are the proposed processing operations an effective means for your organisation to fulfil the mandate assigned to it?	Have you considered alternatives for fulfilling this task? Why is the chosen approach the least intrusive one?	Benefits of the processing	Risks to the fundamental rights arising from the processing		
			Risk	Likelyhood (rate from 1 to 4, see knowledge base)	Impact (rate from 1 to 4, see knowledge base)
EASO's SMM activities aim to support the implementation of the Common European Asylum System (CEAS) by alerting Stakeholders, notably migration and asylum authorities of EU+ Member States, as well as relevant EU Institutions / EU Agencies, and relevant International Organisations (UNHCR, IOM, IGC and Interpol) of developments which are relevant to such implementation. It does this by:	N The information included in the SMM reports can only be retrieved from social media platfroms. No personal data is included in the SMM Reports.	See explanation provided under "Necessity" (of the processing)	Data subjects are not immediately aware of the processing operation	3	2

6

• Supporting management and the different sectors/units within EASO with research on and information from social media in the languages that the project covers. Examples of such sectors/units include within the Department of Operations, Country of Origin Information (COI), Information and Analysis Unit (IAU), and the Department of Asylum Support (DAS); • Supporting the different EU Institutions/Agencies with tailor-made reports and ad hoc research on social media regarding specific asylum related incidents/trends; • Providing national authorities of the EU+ Member States with the latest relevant findings related to the situation and concerns of asylum seekers/refugees en route to as well as in the EU and raising awareness of new trends, gaps or misinformation; • Gaining an in-depth knowledge about the mixed migration dynamics and the perception of national and EU asylum-related rules, laws and practices by members of the communities of concern; • Identifying fake news and/or disinformation regarding the different aspects of the Common European Asylum System (CEAS) and bringing them to the attention of the migration and asylum authorities of the Member States.					

7

Please rate the overall necessity of the process from 1 (low) to 4 (imperative)	Please rate the overall proportionality of the process from 1 (low) to 4 (imperative)
3	3

PART I. B. - Risk Assessment: Assessing likelihood & impact
For each step of the processing operation (collection of data, merging data sets, etc.), answer Yes/No to the questions about the principles of data potection that they may affect. Your processing operation may not involve all the steps that are linked to a question, or may include additionnal steps, which you can indicate in "other" : please refer to the information you provided in Part I of the Knowledge Base to see which are the steps of your specific processing operation. To rate the possible impact of the process on each of the 7 data protection principles, please refer to Part II of the Knowledge base.

1 Fairness

Questions	Step of the operation Only answer (Yes/No) to the steps included in your processing operation					
	Collection	Merging datasets	Retrieval/consultation/use	Disclosure/Transfer	Storage	Other
1. Is the processing of this data something that people can expect, even whithout reading the information that you give them ?			Y In light of high level EU political statements and the EU's narrative on cmbatting abuses to the CEAS, it can reasonably be exoected by the data subjects that such public information and posts are used by EASO and other EU institutions.			
2. Consent						

a. If you rely on consent, is it really freely given?						
b. If you rely on consent, can people revoke it?						
Please indicate how.						
c. If your processing operation relies on consent, please indicate how you document that people gave it. If it relies on a legal obligation, internal rules or other, please indicate which.						
3. Could this operation decrease the likelihood that people exercise their fundamental rights (e.g. freedom of expression, belief...) ?E. g. When investigating e-mails, if one checked the content instead of only checking the traffic data, this would decrease the likelihood that people exercise their freedom of expression.			N			
4. Could this processing operation lead to discrimination ?			N			
5. Is it easy for people to exercise their rights to access, rectification, erasure, etc. ?			Y Privacy statement is made available on EASO's web site.			

Based on your answers, assess the likelihood that a Data Subject would be affected by an unfair processing of his/her data (rate from 1 to 4)	Based on your answers, assess the impact if a Data Subject were affected (rate from 1 to 4)
2	2

2 Transparency

Questions	Step of the operation Only answer (Yes/No) to the steps included in your processing operation

9

	Collection	Merging datasets	Retrieval/consultation/use	Editing/Alteration	Disclosure/Transfer	Storage	Other
1. Is the information you provide complete and easy to understand?			Y	Y			
2. Do you make sure the information you provide actually reaches the individuals concerned? Answer Y/N and indicate how.			Y Since the information needed for SMM Reports is gathered from publicly available sources (social media posts) the most effective way of informing data subjects is by publishing the privacy notice for the SMM project on EASO's website.	Y (see explanation in column to the left)			
3. Is it targeted to the audience? E.g. job applicants may require tailored information. Answer Y/N and indicate how.			Y Efforts were made to keep the language used in the privacy notice as easily understandable by data subjects (social media users).	Y			
4. In case you defer informing people, please indicate how you justify this.							

Based on your answers, assess the likelihood that a Data Subject would be affected by an untransparent processing of his/her data (rate from 1 to 4)	Based on your answers, assess the impact if a Data Subject were affected (rate from 1 to 4)

10

3	2

3 Purpose limitation

Questions	Step of the operation Only answer (Yes/No) to the steps included in your processing operation							
	Collection	Merging datasets	Organisation/ Structuring	Retrieval/ consultation/ use	Editing/Alteration	Disclosure/Transfer	Storage	Other
1. Have you identified all purposes of your process?				Y	Y			
2. Are all purposes compatible with the initial purpose?				Y	Y			
3. Is there a risk that the data could be reused for other purposes?				N	N			
Please indicate how you ensure that data are only used for their defined purposes.				No original data (social media posts) as viewed by the SMM team is saved, stored or transmitted.	The draft version of the SMM Reports is also checked by the DPO (before approval is given for the final version) in order to ensure that no screenshots included in the reports contain any personal data.			
4. In case you want to re-use data for scientific research, statistical or								

11

historical purposes, do you apply appropriate safeguards?								
Please indicate which safeguards you apply.								

Based on your answers, assess the likelihood that a Data Subject would be affected by a default of purpose limitation (rate from 1 to 4)	Based on your answers, assess the impact if a Data Subject were affected (rate from 1 to 4)
2	2

4 Data minimisation

Questions	Step of the operation Only answer (Yes/No) to the steps included in your processing operation							
	Collection	Merging datasets	Organisation/ Structuring	Retrieval/ consultation/ use	Editing/Alteration	Disclosure/Transfer	Storage	Other
1. Do data you collect measure exactly what you need to achieve your goal?				Y	Y			
2. Are there data items you could remove/mask without compromising the purpose of the process?				N All possible data which can be removed/masked is alrady removed from the Reports.	N			
3. When you collect data, for instance								

12

in forms, do you clearly distinguish between mandatory and optional information?								
4. If you want to keep information for statistical purposes, do you appropriately manage the risk of re-identification? Answer Y/N and indicate how.								

Based on your answers, assess the likelihood that a Data Subject would be affected by a default of data minimisation (rate from 1 to 4)	Based on your answers, assess the impact if a Data Subject were affected (rate from 1 to 4)
2	2

5 Accuracy

Questions	Step of the operation Only answer (Yes/No) to the steps included in your processing operation							
	Collection	Merging datasets	Organisation/ Structuring	Retrieval/ consultation/ use	Editing/Alteration	Disclosure/Transfer	Storage	Other
1. Are the data of sufficient quality for the purpose?				Y	Y			
2. Do your tools allow upgrading/correcting data where necessary?								
3. Do your tools allow consistency checks? E. g. automatically checking if								

birth dates entered are in the right format.								
4. Do you take sufficient mesures to ensure the accuracy of data you collect yourself, and review it? Answer Y/N and indicate how.								
5. Do you take sufficient mesures to ensure that the data that you obtain from third parties is accurate, and do you review it? Answer Y/N and indicate how.								

Based on your answers, assess the likelihood that a Data Subject would be affected by the processing of inaccurate data (rate from 1 to 4)	Based on your answers, assess the impact if a Data Subject were affected (rate from 1 to 4)
2	2

6 Storage limitation

Questions	Step of the operation Only answer (Yes/No) to the steps included in your processing operation				
	Retrieval/ consultation/use	Restriction	Storage	Erasure/ Destruction	Other
1. Is the retention period defined by EU legislation ?	N			N	
2. Can you distinguish retention periods for different parts of the data ?	N			N	

Please indicate the retention period.	No personal data is included in the SMM reports.				
3. Is it really necessary to keep data for this period with regard to the purpose ? Please indicate the purpose for retaining the data for this period.					
4. If you cannot delete the data immediately after the retention period, can you restrict or block access to it ?					
5. Will your tools allow automated erasure at the end of the storage period ?					

Based on your answers, assess the likelihood that a Data Subject would be affected by a default of storage limitation (rate from 1 to 4)	Based on your answers, assess the impact if a Data Subject were affected (rate from 1 to 4)
2	2

7 Security

Questions	Step of the operation Only answer (Yes/No) to the steps included in your processing operation								
	Collection	Merging datasets	Retrieval/ consultation/	Editing/ Alteration	Disclosure/ Transfer	Restriction	Storage	Erasure/ Destruction	Other

15

			use						
1. Do you have a procedure to perform an identification, analysis and evaluation of the information security risks that could affect personal data and the IT systems supporting their processing?			Y Not formalised. Following EDPS's recommendations this process can be formalised.	Y Not formalised. Following EDPS's recommendations this process can be formalised.	Y Not formalised. Following EDPS's recommendations this process can be formalised.				
2. Do you target the impact on people's fundamental rights, freedoms and interests, and not only the risks to the organisation?			Y	Y	Y				
3. Do you take into account the nature, scope, context and purpose of processing when assessing the risks?			Y	Y	Y				
4. Do you manage your system vulnerabilities and threats for your data and systems?									
5. Do you have resources and staff with assigned roles to perform the risk assessment?			Y	Y	Y				
6. Do you systematically review and update the security measures in relation to the									

16

context of the processing and the risks?									

Based on your answers, assess the likelihood that a Data Subject would be affected by a breach of security in the processing of his/her data (rate from 1 to 4)	Based on your answers, assess the impact if a Data Subject were affected (rate from 1 to 4)
2	2

Risk treatment (Part II)

Measures envisaged to address the risks (likelihood and impact)

Generic controls							
Preventive: Do you prevent risks from materialising?	Y/N	Detective: Do you monitor your processing operations in order to ensure that you quickly notice breaches?	Y/N	Repressive: Do you ensure that you have means in place to quickly end detected breaches?	Y/N	Corrective: Do you ensure that you have the means to undo or limit damage after the fact?	Y/N
Do you sufficiently raise awareness among staff to prevent unauthorised data sharing ?	Y	Do you use logging operations and self-monitoring to detect data breaches or illicit use ?		Do you have procedures to correct inaccurate data ?		Do you keep backups, so you can revert to the status quo ante after systems have been compromised?	
Do you keep conservation periods and the amount of data collected to the minimum ?	Y						
Do you have a user management that allows you to quickly deactivate access rights of persons who no longer have a need to know (e.g. because they changed jobs) ?	Y	Do you keep track of when and how you informed people about the processing ?		Do you certificate revocation mechanisms to stop the use of compromised credentials ?		Do you inform your recipients after an unauthorised transfer and instructing them to delete the data?	

17

Do you segregate personal data so that breaches of confidentiality in one repository do not affect others ?								
Do you encrypt storage devices ?								

Controls by Data Protection Principle														
	Fairness		Transparency		Purpose limitation		Data minimisation		Accuracy		Storage limitation (retention period)		Security	
Impact and Likelihood rates found in Part I	Impact	Likelihood	Impact	Likelihood	Impact	Likelihood	Impact	Likelihood	Impact	Likelihood	Impact	Likelihood	Impact	Likelihood
	2/4	2/4	3/4	2/4	2/4	2/4	2/4	2/4	2/4	2/4	2/4	2/4	2/4	2/4
Exemples of generic controls to mitigate these weaknesses. Please cross out if not applicable	Check allowed/expected use when re-using data-sets		Automatically notifying data subjects		Limiting export functionalities Avoiding generic identifiers		Collecting age ranges instead of birth dates		Consistency checks Data quality reviews		Distinguishing between conservation period for different parts of data, restricting access to relevant profile		Ex: Information Security Risk Management framework.	
Other controls you propose to apply														

PART III – CONCLUSION

Based on the knowledge base, on the results of the necessity and proportionality assessment (Part I. A.), on the impact and likelyhood assessment (Part I. B.) and on the risk treatement (Part II), please conclude about the overall impact of the process regarding personnal data.

18

EASO's SMM activities aim to support the implementation of the Common European Asylum System (CEAS) by alerting stakeholders of developments which are relevant to such implementation.

All measures are taken in order to ensure that the data processing is kept to what is strictly required for achieveing this prupose. In this context, the processing operations are limited to the visual consultation of social media posts and (occasionally) editing snapshots taken from social media in order to ensure that no personal data is transmitted in the SMM Reports. This latter process is irreversible and no personal data of any sort is stored by EASO.

No personal data is included in the SMM Reports, so no personal data is shared/disclosed to the recipients of the SMM reports.

Measures were taken to ensure transparency about this processing of personal data by posting the privacy notice on EASO's website.

19