The Hague,	17 March 2021		
EDOC#	1156601	v	13A

Europol Action Plan addressing the risks raised in the European Data Protection Supervisor (EDPS) Decision on 'Europol's Big Data challenge'

Progress Report March 2021

Contents

1. Introduction

In September 2020, Europol received from the European Data Protection Supervisor (EDPS) a decision regarding the processing of large datasets (referred to as 'Europol's Big Data Challenge').

The EDPS decision arrived at the conclusion that the handling of large datasets for analysis work (and beyond that for all operational processing purposes based on Article 18(5) in connection with Article 18(2) of the Europol Regulation) has to commence on the basis of information with a Data Subject Categorisation (DSC)[1], already when contributed from Member States and operational cooperation partners, or as soon as it is processed by Europol.

The EDPS decision highlighted that it is not possible for Europol from the outset, upon the receipt of large datasets, to ascertain that all underlying information complies with the DSC laid down in Annex II of the Europol Regulation (ER), thus implying compliance risks with respect to the ER.

The EDPS requested Europol to come up with an Action Plan to address the compliance risks identified by the EDPS.

Europol produced an Action Plan which was provided to the EDPS on 17 November 2020. It focuses on two aspects relating to fundamental information security principles, as well as to data protection controls, which Europol is currently implementing, namely to:

- Reduce the risks for data subjects by ensuring an enhanced data review;
- Continue Europol's efforts for building a dedicated New Forensic Environment (NFE), which provides additional features and improvements to Europol's operational environment for handling large and complex datasets on a new technical platform.

In December, the EDPS replied to the Action Plan presented, expressing "… appreciation for the work provided by Europol in elaborating the Action Plan …", while at the same time requesting further information.

This document represents a progress report on the implementation of the Action Plan, detailing the measures taken within six months since the date of the EDPS Decision, as requested in the Decision. It also includes answers to the questions put forward in December 2020 by the EDPS. The Data Protection Impact Assessment (DPIA) is part of this progress report. The DPIA summarises the overall assessment of the risks and corresponding mitigating measures. This DPIA includes an overall assessment of the risks of non–compliance with the list of DSC, as set out in Annex II of the ER, as well as an assessment of the residual risk level which is based on the risk assessment of the Action Plan itself. This addresses the EDPS request regarding information concerning the risk assessment in relation to the data protection aspects concerned.

This report covers each action, with the following structure:

- Description of the action;
- Main stakeholder(s);
- Status of the action;
- Progress of the implementation of the action;

[1] As set out in Annex II of the Europol Regulation (i.e. suspects, potential future criminals, contacts, associates, victims, witnesses and informants of criminal activities)

- Risk(s) identified in relation to the implementation of the action;
- Answers to the questions put forward by the EDPS in December 2020.

Finally, the report ends with an update on other activities.

2. Data Protection Impact Assessment (DPIA)

Serious and organised crime and terrorism remain a key threat to the internal security of the EU. All criminal and terrorist activities have a serious impact on our EU societies. Serious and organised crime deeply affects all layers of society; in addition to the direct impact on the daily lives of EU citizens, it also undermines the economy, state institutions and the rule of law. It is Europol's role in fighting crime and terrorism to target criminal and terrorist networks and to provide an answer to victims and societies targeted by crime and terrorism. To do this, Europol is processing operational and strategic information, including personal data, in support of Member States' investigations.

Europol is determined to make Europe a safer place. Compliance with fundamental rights in Europol's activities is an integral part of a safer Europe. Efficient and effective data protection represents the foundation for the successful delivery of Europol's Mission. The trust that Europol has built up for over 20 years is inextricably linked to its strong, transparent and robust data protection as well as security regime.

Europol considers data protection as an opportunity, especially in light of Europol's Strategy 2020+, highlighting that Europol aspires to be the model EU law enforcement organisation with robust performance, good governance and accountability.

Europol has a strong data protection regime in order to safeguard personal data thus protecting the rights of citizens. More specifically, the DSC under the provisions of the ER is aimed at limiting processing operations by Europol to data subjects which have a verified connection with a criminal activity. This protects the fundamental rights and freedom of citizens.

It must be noted that the EDPS Decision on 'Europol's Big Data Challenge', although pertaining to the digital world, does not represent, in essence, new risk types to data subjects. Law enforcement and judicial authorities have invariably dealt with information and data that may not be linked to criminal activity, for instance when seizing documents in a house search or by conducting lawful telephone interception. What has changed is the volume of data processed, now requiring innovative tools to support a swift handling of the data, in particular with a view to minimising any remaining risk profile for data subjects.

The details of the risk assessment, conducted by Europol in order to identify the potential risks of non–compliance with the DSC referred to in Annex II of the ER, is presented in this progress report.

2.1. Methodology and definitions

The risk assessment is based on Europol's corporate risk management process, assessing probability and impact (*see Annex 4 for terminology*).

The corporate risk management terminology allows for a more granular assessment of impact and probability (on a 4-by-4 scale), further to the Europol Data Protection Function (DPF) guidelines for assessing risks under Article 39 of the ER (4-by-3 scale in terms of impact and probability).

The risk assessment covers:

- An assessment of the risks related to DSC compliance (Chapter 2.2 below);
- The mitigating measures addressed with the Actions 1-5 of the Action Plan, including the related risks of non-implementation (detailed in Chapter 3 below);
- An assessment of the residual risk level after mitigation.

The results of the assessment are compiled in a table with the following columns:

- Column 1: Risk ID
- Column 2: Description of risk of the DSC non-compliance
- Column 3: Impact
- Column 4: Probability
- Column 5: Risk of DSC non-compliance
- Column 6: Recommended controls/mitigating actions
- Column 7: Risk of non–implementation of the mitigating actions
- Column 8: Risk treatment options
- Column 9: Residual risk level after mitigation

2.2. Overview of the risks identified in relation to DSC compliance

Europol identified risks in relation to the DSC compliance and the impact such risks could have on data subjects, in order to protect the fundamental rights and freedom of citizens via mitigating actions. The following risks were identified:

1) Lack of awareness by Europol of contributions that may include personal data lacking DSC in accordance with Annex II of the ER.
2) Data lacking DSC is initially flagged but not further acted upon throughout the data lifecycle.
3) Exposure of personal data lacking DSC in accordance with Annex II of the ER.
4) Processing of personal data lacking DSC in accordance with Annex II of the ER longer than it is strictly necessary and proportionate.
5) Sensitive data categories (Article 30 of the ER) are pending assignment.
6) Data review related to DSC compliance not performed systematically.

Risk 1: Lack of awareness by Europol of contributions that may include personal data lacking DSC in accordance with Annex II of the ER.

Impact: The potential lack of awareness by Europol of contributions that may include personal data lacking DSC could result in the involuntary processing of personal data of individuals who are unrelated to criminal activity.

As acknowledged by the EDPS, it is not possible for Europol from the outset, upon the receipt of large datasets, to ascertain that all underlying information complies with the list of DSC, as set out in Annex II of the ER (i.e. suspects, potential future criminals, contacts, associates, victims, witnesses and informants of criminal activities). As outlined in the update for Action 1, the probability is assessed as low, in particular given the results of monitoring Secure Information Exchange Network Application (SIENA) with respect to contributions without a DSC.

Impact	**SERIOUS**
Probability	**LOW**
Risk	**MEDIUM**

The proposed flagging, as per Action 1, mitigates this risk by ensuring that Europol has immediate visibility on data that may lack the DSC and is able to prioritise the processing of such contributions with the aim to ensure full compliance at the earliest possible stage.

Risk 2: Data lacking DSC is initially flagged but not further acted upon throughout the data lifecycle.

Impact: A lack of DSC initially flagged but not further acted upon throughout the data lifecycle could result in the involuntary processing of personal data of individuals who are unrelated to criminal activity.

Impact	**SERIOUS**
Probability	**LOW**
Risk	**MEDIUM**

The proposed labelling throughout Europol's processing environments, as per Action 2, mitigates this risk by ensuring that Europol has continued visibility on data that may lack the DSC and is enabled to prioritise the processing of such contributions with the aim to ensure full compliance at the earliest possible stage, in particular through Actions 4 and 5 of the Action Plan. This reduces the probability of the risk to a low level.

Risk 3: Exposure of personal data lacking DSC in accordance with Annex II of the ER.

Impact: The exposure of personal data still lacking DSC in accordance with Annex II within Europol's Analysis System (EAS) could lead to a situation in which such information is included into an analysis report, even though the link to criminal activity has not yet been verified.

Impact	**SERIOUS**
Probability	**LOW**
Risk	**MEDIUM**

The proposed additional measures limiting access rights to data files where the DSC is pending and enhancing data minimisation, as per Action 3, mitigate this risk by reducing the number of Europol staff who could be exposed to information without a DSC. These staff members are specifically trained and are thus aware of the risk of processing personal data without a DSC. Against this background, the probability of the risk is considered as low.

Risk 4: Processing of personal data lacking DSC in accordance with Annex II of the ER for longer than it is strictly necessary and proportionate.

Impact: The processing of personal data lacking DSC entails the risk that also personal data beyond the scope of Annex II of the ER may be included. Processing of personal data must be limited to what is strictly necessary and proportionate, aiming at the determination of the DSC as soon as it is possible. If data is not reviewed, this could result in continuous non-compliant processing operations.

Impact	**SERIOUS**
Probability	**LOW**
Risk	**MEDIUM**

The increase of the regular reviews of large datasets to check alignment with Annex II of the ER and the relevant data categories (as defined in the corresponding Opening Decision of all Analysis Projects - APs), as per Actions 4 and 5 of the Action Plan, mitigates this risk. The probability of the risk is therefore assessed as low.

Risk 5: Sensitive data categories (Article 30 of the ER) are pending assignment.

Complementing in particular Risk 4, there is also the specific risk that sensitive categories of data (without a DSC) are processed further.

Impact: The processing of personal data lacking DSC entails the risk that also sensitive data categories could be affected. Such processing must be limited to what is strictly necessary and proportionate, to allow for the determination of the DSC as soon as it is possible. If data is not reviewed, this could result in continuous non-compliant processing operations. Given that the legislator intended to protect sensitive data categories as per the provisions set out in Article 30 of the ER, the impact of the risk for data subjects would be severe (as the highest impact category according to Europol's corporate risk management methodology).

Impact	**SEVERE**
Probability	**LOW**
Risk	**HIGH**

The proposed measure to increase the regular reviews of large datasets to check alignment with Annex II of the ER and the relevant data categories (as defined in the corresponding Opening Decision of all Analysis Projects - APs), in particular as per Actions 4 and 5 of the Action Plan, mitigates this risk. The probability of the risk is assessed as low.

Risk 6: Data review related to DSC compliance not performed systematically.

Impact: The processing of personal data without a DSC entails the risk of impairing overall data compliance. In particular against the background of the description of Risk 2 above, it is evident that the impact of the identified Risk 6 would be serious, if the corresponding mitigation actions are not consistently followed through in a systematic manner.

Impact	**SERIOUS**
Probability	**LOW**
Risk	**MEDIUM**

The appointment a Data Quality Control Coordinator mitigates this risk. The task of the Data Quality Control Coordinator is to monitor that personal data is collected and processed for a specific purpose and is processed compliantly by Europol, in a manner that ensures the appropriate security of data processing and the overall protection of the rights and freedoms of data subjects. The Data Quality Control Coordinator oversees the operational data management for the purposes of data quality control and assurance, with a view to ensuring that the data protection safeguards, as stipulated in the ER, are upheld. This includes the continuous implementation of the data review arrangements, thus contributing to persistent data quality improvement and compliance with Annex II of the ER. Accordingly, the probability for the risk is assessed as low.

2.3. Conclusion

Combining the assessment of the DSC non-compliance risks, in addition to the risk profile regarding the implementation of the mitigation actions (i.e. the Actions 1 to 5 of the Action Plan (detailed in Chapter 3), Europol currently assesses the **residual risk profile** for the identified risks as **low**.

2.4. Data Protection Impact Assessment (DPIA) - Summary table

1	2	3	4	5	6	7	8	9
Risk ID	Description of risk of the DSC non-compliance	Impact	Probability	Risk of DSC non-compliance	Recommended controls/ mitigating actions	Risk of non-implementation of mitigating actions	Risk treatment options	Residual risk level after mitigation
R1	Lack of awareness by Europol of contributions that may include personal data lacking DSC in accordance with Annex II of the Europol Regulation (ER).	SERIOUS	LOW	MEDIUM	Member States and operational cooperation partners will flag those contributions sent to Europol concerning which the DSC is pending. During the extraction, data minimisation takes place based on the restrictions in the respective Analysis Project (AP) Opening Decision (categories of data subjects, crime area, relevance and in agreement with the data provider (on what is expected/needed)).	LOW	☒ Mitigate Risk by implementing recommended controls ☐ Accept Risk	LOW
R2	Data lacking DSC is initially flagged but not further acted upon throughout the data lifecycle.	SERIOUS	LOW	MEDIUM	After accepting a request for support by MS or operational cooperation partners, Europol will label all data files in its data environment for which the DSC assessment or determination is pending.	LOW	☒ Mitigate Risk by implementing recommended controls ☐ Accept Risk	LOW
R3	Exposure of personal data lacking DSC in accordance with Annex II of the ER.	SERIOUS	LOW	MEDIUM	Implement additional security measures by limiting access rights for these data files where DSC is pending and enhancing data minimisation.	LOW	☒ Mitigate Risk by implementing recommended controls ☐ Accept Risk	LOW
R4	Processing of personal data lacking DSC in accordance with Annex II of the ER for longer than it is strictly necessary and proportionate.	SERIOUS	LOW	MEDIUM	Every Analysis Project (AP) will be asked to increase the regular reviews of large datasets to check the alignment data with Annex II of the ER and the relevant data categories (defined in the AP Opening Decision). This also includes the processing of data in the current [redacted]	LOW	☒ Mitigate Risk by implementing recommended controls ☐ Accept Risk	LOW
R5	Sensitive data categories (Article 30 of the ER) are pending assignment.	SEVERE	LOW	HIGH	The dedicated review activities dedicated focus on identifying sensitive data categories.[2]	LOW	☒ Mitigate Risk by implementing recommended controls ☐ Accept Risk	LOW

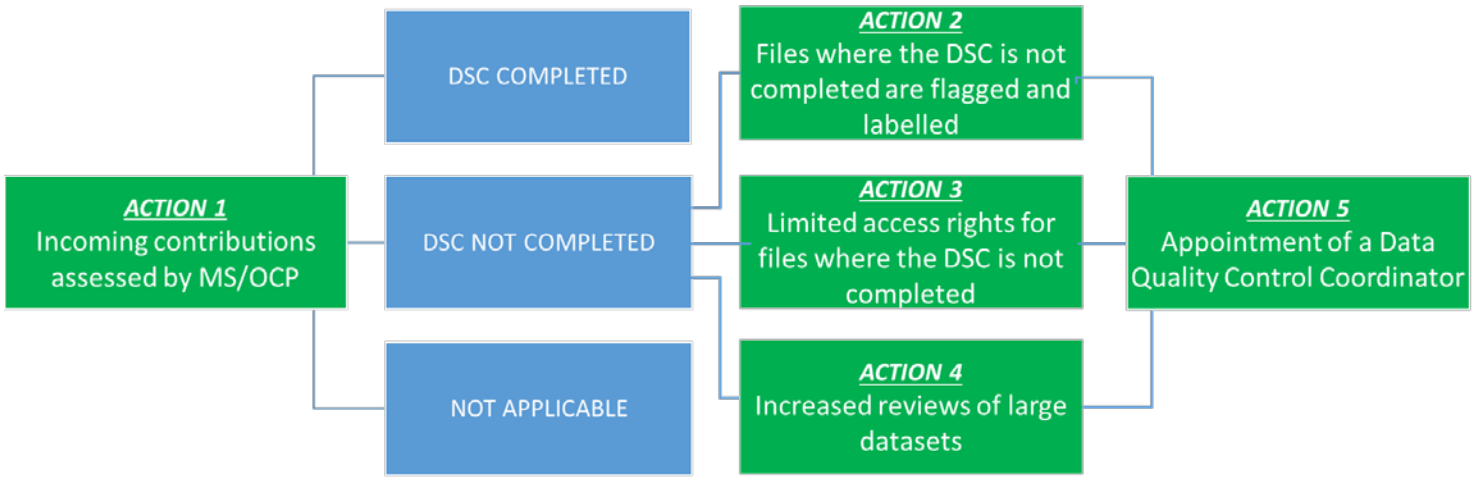
[2] Risk 5 recognises the particular rights of data subjects concerning sensitive data

1	2	3	4	5	6	7	8	9
Risk ID	Description of risk of the DSC non-compliance	Impact	Probability	Risk of DSC non-compliance	Recommended controls / mitigating actions	Risk of non-implementation of mitigating actions	Risk treatment options	Residual risk level after mitigation
R6	Data review related to DSC compliance not performed systematically.	SERIOUS	LOW	MEDIUM	Appointment of and subsequent action plan of a full-time senior operational analyst as Data Quality Control Coordinator for the data review.	LOW	☒ Mitigate Risk by implementing recommended controls ☐ Accept Risk	LOW

3. The Action Plan

The Action Plan contains five (5) mitigation actions which are summarised below:

- Action 1: In the information exchange between Member States (MS), operational cooperation partners and Europol, those contributions concerning which the data is pending assessment or determination of the DSC shall be flagged by the contributor. Europol's Secure Information Exchange Network Application (SIENA) is being updated in order to realise this technical change, which is included as a priority in the ICT work planning for 2021.
- Action 2: After accepting a request for support by MS or operational cooperation partners, Europol labels all data files in its data environment for which the DSC assessment or determination is pending.
- Action 3: Implement additional security measures by limiting access rights for these data files where the DSC is pending and enhancing data minimisation.
- Action 4: Every Analysis Project (AP) is asked to increase the regular reviews of large datasets to check the alignment data with Annex II of the ER and the relevant data categories (defined in the AP Opening Decision).
- Action 5: Europol appoints a full-time senior operational analyst as Data Quality Control Coordinator for the data review. A Data Quality Control Action Plan is developed and implemented.



(See Annex 3 for a visualisation of the actions in the data landscape)

3.1. Action 1: Flagging of contributions sent to Europol where the DSC is pending.

DESCRIPTION OF THE ACTION

In the information exchange between Member States (MS), operational cooperation partners and Europol, those contributions concerning which the data is pending assessment or determination of the DSC shall be flagged by the contributor. Europol's Secure Information Exchange Network Application (SIENA) is being updated in order to realise this technical change, which is included as a priority in the ICT work planning for 2021.

At the end of 2020, Europol monitored SIENA for two full weeks in order to ascertain the number of SIENA contributions without a DSC. During the first week, out of 2,500 contributions received, only 65 contributions had no DSC (2.6%) and during the second week, out of 2,320 contributions received, only 18 contributions had no DSC (0.8%). Therefore, it appears that the compliance risk with regard to information (which is not related to a DSC) affects a very small proportion of the contributions Europol receives.

Action 1 is of vital importance because if MS do not have the possibility to clearly flag contributions where the DSC is pending, it is challenging for Europol to identify those contributions individually.

STAKEHOLDERS

External Stakeholders:	ALL Member States (MS) and operational cooperation partners
Internal Stakeholders:	Capabilities Directorate Business Project Management (CDBPM) and Operations Directorate

STATUS

PROGRESS

For this activity, the main internal stakeholders are Europol's Capabilities Directorate Business Product Management (CDBPM) and the Operations Directorate. In-depth discussions have been held between the Analysis and Operational Centre (Analysis and Strategic Coordination Unit), CDBPM, ICT and DPF. Feedback from the Heads of Europol National Units (HENUs), the Information Management Working Group and the Corporate Matters Working Group of the Europol Management Board (MB), to keep the impact to MS and operational cooperation partners at a minimum, was taken into consideration.

Following the discussions and a detailed assessment by CDBPM, a proposal has been made for the adding of radio buttons to SIENA *(see Annex 1)*.

The following steps will need to be taken by the users when sending a SIENA message to Europol:

- The field will be activated by default and will only appear when a Europol recipient is selected.
- The user will need to select either *Completed* if the DSC assessment has been carried out, *Not Completed* if the assessment has not been carried out, or *Not Applicable* when the DSC assessment is not applicable.

Timeline for implementation: The implementation is planned for the SIENA release 4.10 in **May 2021.**

In order to verify that the flagging is performed and monitored properly an extra measure is taken. In addition to the field where the Member States and Operational Cooperation Partners will flag contributions for which the DSC assessment has not been completed, during the acceptance phase, Europol will also have a new additional field in SIENA where Europol upon acceptance of the contributions will perform a **second assessment** (additional action added after the EDPS reply in December 2020). This is in order to further reduce the risk that data without a DSC is processed or integrated into the analysis work.

Timeline for implementation: This change is planned for a SIENA release in the **second half of 2021**.

In conclusion, data sent to Europol will be assessed at national level and upon arrival at Europol (acceptance phase).

Risks identified in relation to the implementation of the action:

The following risks have been identified:

- Non-agreement by MS
  - The Member States have agreed to the flagging of the DSC assessment in SIENA.
- Implementation of the action
  - The SIENA update has been integrated into the ICT Work Plan and is linked to "SIENA – Compliance requirements for data intake and processing in the Operations Directorate"[3].

Impact	**SERIOUS**
Probability	**VERY LOW**
Risk of non-implementation	**LOW**

Additional questions from EDPS[4]:

Europol is committed to performing the SIENA update and Europol's ICT Department is currently working on this.

On the question regarding the measures that will be put in place to verify that the flagging is performed and done properly, this has been addressed in the implementation approach, detailed above regarding the additional field in SIENA for Europol's second assessment.

On the question regarding the monitoring and the verification that the labelling is done correctly, contributions with no DSC will be automatically labelled ([redacted]) in the data environment, in case that the data is not forensic data. In case of forensic data, the data is manually stored in a specific folder which is labelled as DSC not completed as per Action 3. This manual activity is reviewed under the data review mechanism (Action 4).

These measures have been integrated into the ICT Work Plan 2021 and are part of the description 'SIENA – Compliance requirements for data intake and processing in OD (*see Annex 5*).

[3] Europol ICT Work Plan 2021, Appendix page 10: "SIENA – Compliance requirements for data intake and processing in Operations Department".
[4] EDPS Decision on the own initiative inquiry on Europol's big data challenge, Europol Action Plan, WRW/FC/vm/ D(2020) 2821 C 2019-0370 (same reference for all Actions 1 to 5 of the Action Plan)
[5] [redacted]

3.2. Action 2: Labelling of data files where the DSC is pending.

DESCRIPTION OF THE ACTION

After accepting a request for support by MS or operational cooperation partners, Europol labels all data files in its data environment for which the DSC assessment or determination is pending.

By labelling the data to show whether the DSC assessment has been completed or not (Action 1), the risk of data without a DSC being further processed or integrated into the analysis work and analytical reporting is low.

STAKEHOLDERS

Internal Stakeholders:	Information and Communication Technology (ICT)
	Operations Directorate

STATUS

PROGRESS

With the full implementation of the new analysis environment (the replacement of [redacted]), Europol will ensure that data where the DSC is not completed will be automatically labelled after being forwarded via Siena into the analysis environment.

Timeline for implementation:

- **Q3 2021** for CT data – linked to the replacement of [redacted]
- The replacement of [redacted] will take place in **2022**.

Risks identified in relation to the implementation of the action:

The following risks have been identified:

- Implementation of the action
  - The labelling of data files where the DSC is pending is being integrated into the ICT Work Plan.

Impact	**SERIOUS**
Probability	**VERY LOW**
Risk of non-implementation	**LOW**

Additional questions from EDPS:

Regarding the question whether Europol will define a maximum retention period for datasets which are waiting to be flagged in the Europol data environment, Europol will keep the datasets for as long as is necessary and proportionate for the support to the investigation concerned. Europol will do its utmost and take all necessary measures to ensure that this is done in the shortest time possible and in line with the rules of data retention as defined by the ER. Furthermore, Europol will keep a record of the data without a DSC in the Data Quality Logbook and assess it on a quarterly basis to ensure that the necessity and proportionality still exists.

On the question regarding the exact nature of the risk, reference is made to Chapter 2.2 above.

Regarding additional measures to be put in place to enhance the confidentiality of raw data, under Action 3, the data will be stored in an area with limited access rights.

3.3. Action 3: Limiting access rights for data files where the DSC is pending.

DESCRIPTION OF THE ACTION

Implement additional security measures by limiting access rights for these data files where the DSC is pending and enhancing data minimisation.

In addition to labelling the data, access rights to data with no DSC will be limited.

STAKEHOLDERS

Internal Stakeholders:	Information and Communication Technology (ICT)
	Operations Directorate

STATUS

PROGRESS

Forensic Environment

Access rights are already limited in the [redacted] and will be more limited in the [redacted] upon deployment. Specific folders have been created in the [redacted] where data with no DSC will be stored.

Timeline for implementation:

- All APs were asked to create the specific designated folder within their AP folders on the CFN by **3 March 2021**. This was completed on time.
- The same folder structure as for the CFN will be used for the NFE, which is due to go live in **Q2 2021**.

Future Data Environment

In the future data environment (the replacement of [redacted]), contributions for which the DSC is still pending (labelled under action 2) will have limited access rights.

Timeline for implementation:

- [redacted] should be replaced in **Q3 2021** and [redacted] in **2022**.

Risks identified in relation to the implementation of the action:

The following risks have been identified:

- Implementation of the action
  - The limiting of access rights for data files where the DSC is pending is being integrated into the ICT Work Plan.

Impact	**SERIOUS**
Probability	**VERY LOW**
Risk of non-implementation	**LOW**

Additional questions from EDPS:

In relation to the criteria used to define who are given access to the raw (forensic) data and tasked with the extraction process, a limited, designated number of Europol staff with a dedicated forensic training will be given access to the NFE. It will be their responsibility to liaise with the relevant AP in order to identify the DSC and extract the data where the DSC has been identified. Europol has a list of Europol staff with access to all folders on the current [redacted]. These access rights are given on need-to-know basis, only to those assigned to the specific AP.

In relation to the time limit put on the fulfilment of the extraction task, the extraction task can be a lengthy process depending on the data. As per our previous answer under Action 2, during the regular data review process (which is done quarterly), the raw data are assessed and a decision is made whether to keep it or delete it in line with the data review process.

For the content of the review at the level of extraction, the designated Europol staff will assess the DSC provided and its relevance according to the Opening Decision of the respective AP. If the DSC is not provided, the designated Europol staff will work to identify the DSC, or delete the data unless these are needed to maintain the chain of evidence.

With regards to the concerns over assessing a dataset without knowing its content, Europol ensures that the necessity and proportionality is met based on the context in which it was sent to Europol.

In terms of deletion, again, the raw data will be reviewed following the data review process mentioned under Action 2 and a justification will be recorded if it needs to be kept. Until its deletion, it will remain in the location it was placed.

A guideline document has been produced for all Europol staff who process personal data.[6]

3.4. Action 4: Increased reviews of large datasets.

DESCRIPTION OF THE ACTION

Every Analysis Project (AP) is asked to increase the regular reviews of large datasets to check the alignment data with Annex II of the ER and the relevant data categories (defined in the AP Opening Decision).

The change in order to mitigate the risk of non-compliance is the fact that data where the DSC is missing is more visible (due to the flagging in Action 1 and the labelling in Action 2) and therefore we have a means to prioritise this data for review.

Once contributions without a DSC have been identified, as well as being labelled, these are also recorded in a logbook and are regularly reviewed[7] to ensure that the necessity and proportionality of the data processing. Therefore, the extra measure that Europol is taking is that the data that is flagged (Action 2) and in separate folders (Action 3) is increasingly reviewed. Every 3 months, the Analytical Projects have to review these contributions under action 2 and 3. The review is recorded in the Data Quality Logbook (see Action 5).

[6] Data Review for data where the DSC is pending - Guidelines
[7] Data Quality Logbook

STAKEHOLDERS

Internal Stakeholders:	Analysis Projects (APs) within the Operations Directorate

STATUS

PROGRESS

Europol has created a Data Quality Logbook in which data without a DSC is also recorded *(see Figure 1 for a mock-up of the logbook)*.

AP	RECEIVED DATE	SIENA NUMBER	ASSESSMENT DUE BY	CONTRIBUTOR	DATE OF ASSESSMENT	DONE BY	DECISION
SMOKE	15/12/2020	123456-1-1	15/03/2021	Spain			
TERMINAL	20/01/2021	121212-1-1	20/04/2021	France			
CANNABIS	24/02/2021	132323-4-2	24/05/2021	Germany			
FURTUM	25/02/2021	1454545-1-7	25/05/2021	Netherlands			

Figure 1: Mock-up of the Data Quality Logbook

Risks identified in relation to the implementation of the action:

The following risks have been identified:

- Implementation of the action
  - The increased reviews of large datasets has been incorporated into the data review mechanism and is overseen by the newly appointed Data Quality Control Coordinator.

Impact	**SERIOUS**
Probability	**VERY LOW**
Risk of non-implementation	**LOW**

The data review process is done on a quarterly basis. The Data Quality Control Coordinator provides all Analysis Projects a list of SIENA messages to be reviewed every quarter, in line with the data protection safeguards of the ER. Europol has updated the data review guideline for the analysts. Furthermore, Europol has designated points of contact for every AP to ensure that the data review is done timely and accurately.

Once the DSC has been assessed, the data is reviewed as part of the data review process described above. If the data is not deemed relevant then is deleted following the normal process. In relation to data being kept in order to preserve the chain of evidence, more information will be provided in the upcoming progress reports.

3.5. Action 5: Appointment of a Data Quality Control Coordinator.

DESCRIPTION OF THE ACTION

Europol appoints a full-time senior operational analyst as Data Quality Control Coordinator for the data review.

STAKEHOLDERS

Internal Stakeholders:	Operations Directorate, Analysis and Strategic Coordination Unit

STATUS

PROGRESS

Action 5 has been completed following the appointment of a Senior Analyst as the Data Quality Control Coordinator. Furthermore, a profile for the role has been prepared and is shared for information with the EDPS (*see Annex 2*).

The work of the Data Quality Control Coordinator is to ensure the implementation of the data review mechanism and that data processing is performed in line with the Europol Regulation, in particular with Annex II.

In the meantime, the Data Quality Control Coordinator is working on identifying data stored within [redacted] where there is potentially no DSC.

Starting with the 'oldest' data (prior to 2015), work has been done to identify those contributions which are in [redacted] but which have no entities linked to them. These are then being scrutinised to see if any of the data contained within does not have a DSC. Focus is being made on certain file types (e.g. Excel, mdb and PDF) which are likely to contain lists of data, as this is where there is a higher risk of data not having a DSC assigned.

Where large data sets are found and the DSC is not immediately seen, the relevant APs are being consulted so that they can ascertain if there is in fact data with no DSC.

In addition to the appointment of a Senior Analyst as the Data Quality Control Coordinator, another senior analyst has been temporarily assigned to follow up on the full implementation of the overall EDPS Action Plan.

Within the operational units in the Operations Directorate, Single Points of Contact (SPOCs) have been appointed for all APs in relation to data quality. These SPOCs are the represent the nexus between the Data Quality Control Coordinator and their respective APs for all data quality work aspects. They are also responsible for ensuring that all data reviews are completed and on time for their respective APs and for updating the logbook with all contributions received by their APs where the DSC is pending.

Moreover, the SPOCs also participate in bi-weekly meetings on the implementation of the Action Plan and the related quality control measures. In the planning of the Data Analysis Development Team in the Analysis and Strategic Coordination Unit, it is planned to have two additional data quality controllers.

Risks identified in relation to the implementation of the action:

The following risks have been identified:

- The risk that the activities in relation to data review are not monitored.

Impact	**SERIOUS**
Probability	**VERY LOW**
Risk of non-implementation	**LOW**

Additional questions from EDPS:

A profile for the role of Data Quality Control Coordinator is attached in *Annex 2* and the Data Quality Control Action Plan can be found in *Annex 6*.

4. Other activities

Process descriptions

Europol will review the internal data processes [formal process descriptions which are already existing] and will align them with the process landscape. Consequently, the processes will be adapted to the implementation of the Action Plan.

Training and manuals

Europol is updating the training manuals for analysts and specialists. A dedicated training will be given to those concerned.

Evaluation of the Action Plan

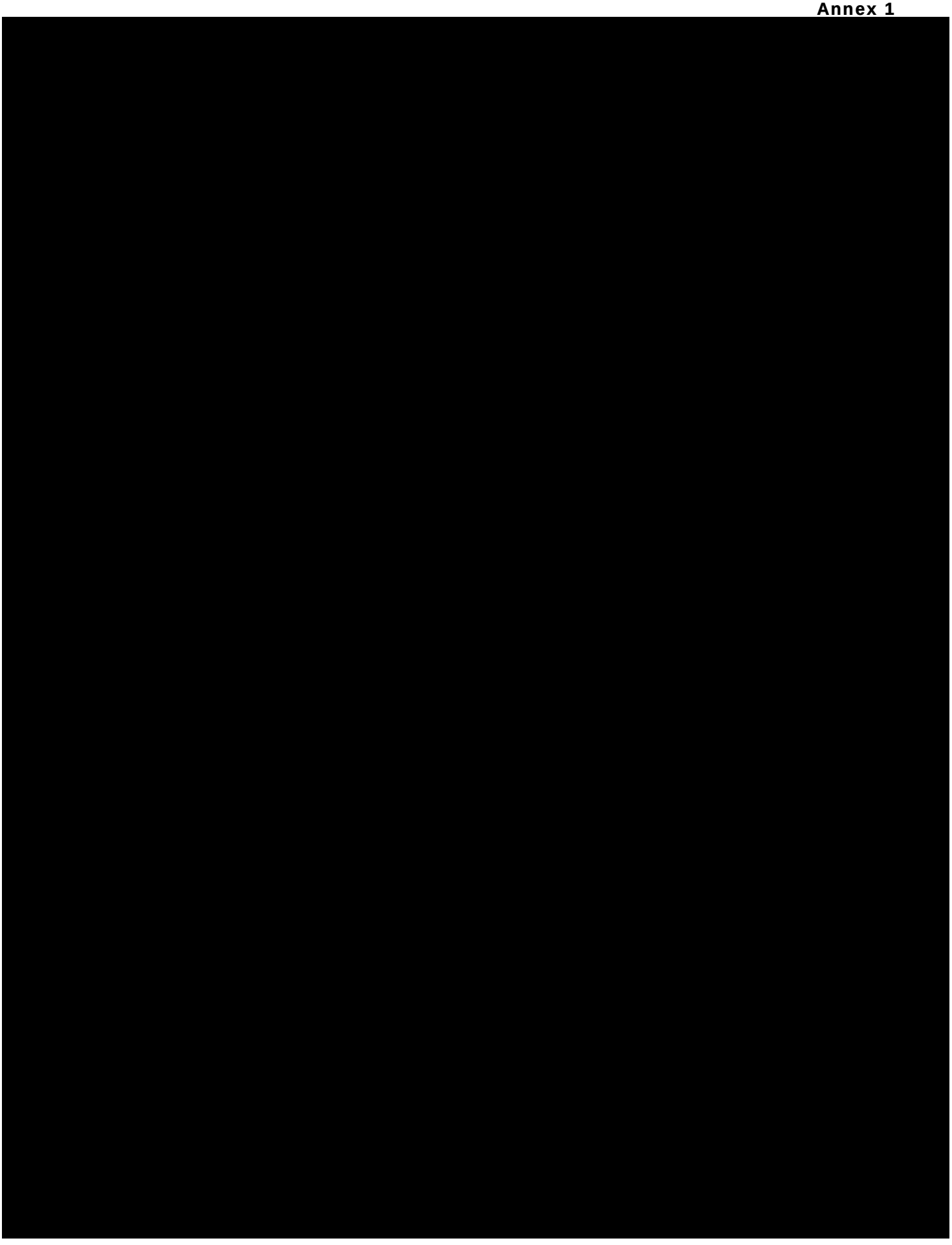
Europol will prepare an evaluation of the Action Plan in **Q3 2021**.

5. Reference documentation[8]

DOCUMENT TITLE
EDPS Decision on the own initiative inquiry on Europol's big data challenge
Europol Action Plan addressing the risks raised in the European Data Protection Supervisor (EDPS) Decision on 'Europol's Big Data challenge'
EDPS Decision on the own initiative inquiry on Europol's big data challenge - Europol Action Plan
Proposed folder architecture of the CFN
Data Quality Logbook
Role profile of the Data Quality Control Coordinator
List of Single Points of Contact (SPOCs)
Action Plan Data Quality Control Coordinator

[8] The documents are available at Europol.

Annex 1



Annex 2

Operational Data Quality Control Coordinator

Description of main tasks and responsibilities

Purpose of the function:

The purpose of the post is to monitor that personal data are collected and processed for a specific purpose and is processed fairly and lawfully by Europol, in a manner that ensures the appropriate security of data processing and the overall protection of the rights and freedoms of data subjects.

The successful candidate oversees the operational data management for purposes of data quality control and assurance, ensuring the quality of information processed by Europol in the Operations Directorate, ultimately guaranteeing that data protection principles and safeguards as stipulated in the Europol Regulation (2016/794) are upheld. S/he is responsible for the continuous implementation of the data review mechanism, data quality improvement and that data processing is performed adequately and in line with the Europol Regulation (2016/794). The person shall review and adjust data when needed. The person will be a senior analyst in Operations Department with an extensive experience in Operational Analysis and data review. The post is a restricted post.

Reporting lines:

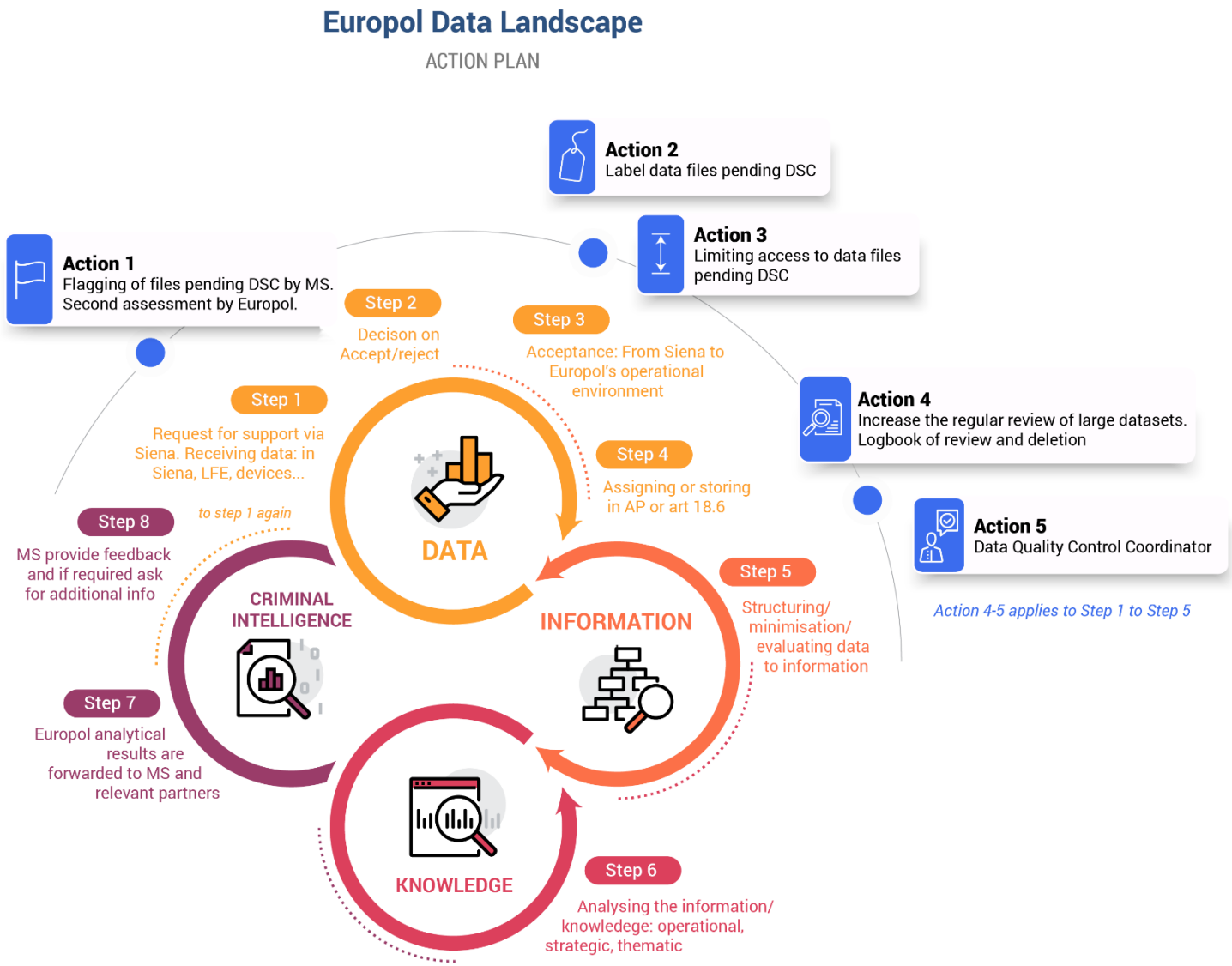
The Data Quality Control Coordinator is embedded in the Data Analysis Development and Support Team falling under remit of the Operational and Analysis Centre, working in close cooperation with the Data Protection Function but moreover in close cooperation with the operational analysts and specialist in the Operational Centres. The incumbent reports to the Head of Team Data Analysis Development and Support Team and the Head of Unit of the Analysis and Strategic Coordination Unit.

The post holder carries out the following main duties:

- Conduct continuous data review in order to ensure that only data whose categories of personal data and categories of data subjects as specified in the Europol Regulation (ER) and its Annex II are collected and processed;
- Analyse, review and adjust data for quality improvement purposes, identify trends and suggest areas of impact;
- Identify and review, adjust data entries non-compliant with established legal obligations, business rules and processes;
- Monitor and ensure that applicable principles of data retention and deletion are safeguarded as laid out in the ER;
- Monitor and ensure that the labelling of specific files, including complex datasets, and compliance with adequate access rights are safeguarded in line with the outlined provisions as specified in the ER and the requirements set out by the European Data Protection Supervisor (EDPS);
- Ensure that personal data that is inaccurate, with regard to the purpose of processing and data subject categorisation, are erased or rectified without delay by the responsible Analytical Projects or units;
- Identify, present and inform management and the Data Protection Function (DPF) on information related to data issues via a Quarterly Data Quality Monitoring Report;
- Assist in the development of operational procedures and methods for data quality control and assurance;
- Identify operational improvement opportunities in Data Quality Monitoring and Assurance;
- Serve as the main point of contact and provide cross-departmental support and advice in managing the Operations Directorate's quality monitoring exercises;
- Prepare periodical data quality reports for internal and external reporting purposes;

- Ensure timely follow-up on corrective and preventive actions;
- Oversee and coordinate continuous quality improvement with specific quality indicators following these key components: identification, investigation, implementation, improvement, and monitoring;
- Continuously monitor the operational data quality across the Operations Directorate, by following data quality checks/ controls;
- Be a contact point for DPF and Capabilities Directorate.

Annex 3[9]

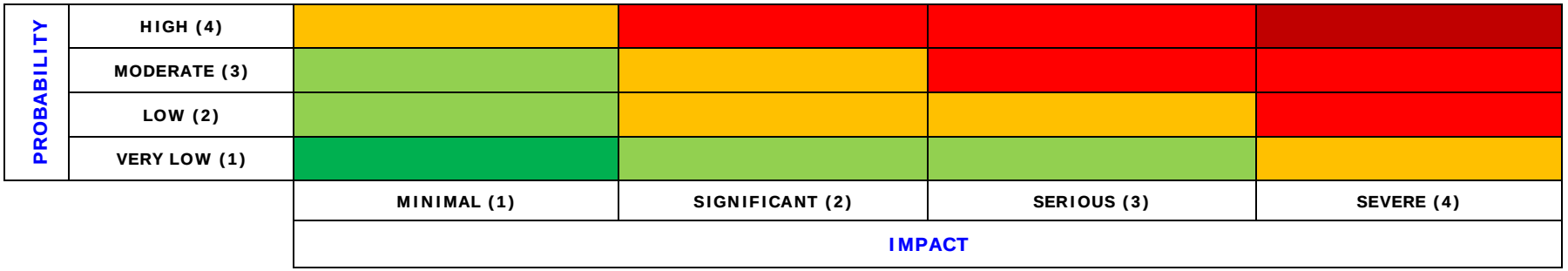


[9] The graph has been updated to reflect the developments in this progress report

Annex 4

Risk Management Terminology

Impact	Influence the uncertain event (or set of events), should it (they) materialise, would have on the business objective, categorised as: (1) Minimal (time–scale, cost–benefit and/or quality implications are negligible) (2) Significant (time–scale, cost–benefit and/or quality implications are within the agreed tolerance level), (3) Serious (time–scale, cost–benefit and/or quality implications are outside the agreed tolerance level) or (4) Severe (time–scale, cost–benefit and/or quality implications affect the viability of the entire business objective).
Probability	Likelihood the uncertain event (or set of events), should it (they) materialise, would have on the business objective, categorised as either: (1) Very low: uncertain event (or set of events) is (are) extremely unlikely to occur; (2) Low: uncertain event (or set of events) is (are) unlikely to occur, (3) Moderate: uncertain event (or set of events) is (are) may occur or (4) High: uncertain event (or set of events) is (are) likely to occur.
Risk	A risk is an uncertain event or set of events that, should it occur, would have an effect on the achievement of objectives related to the business planning (i.e. the Europol Strategy or the annual work programme). This means that risks can be understood in two dimensions: Threats (expected negative effect on a business objective) or opportunities (expected positive effect on a business objective).
Risk description	Statement setting out the cause, the uncertain event or set of events (depicting the area of variable future developments, in terms of threats or opportunities) and the impact (describing the impact the risk would have on the achievement of the concerned objectives).



Annex 5

Extract of ICT Work Plan 2021

5. Appendices

To improve readability of the main sections of this document, the tables there show an abridged version of scope. In the following pages, a more detailed description of the resource allocation and corresponding scope items are listed for the Portfolio Streams in the ICT Work Plan 2021 that have the highest priority and greatest need to communicate expectations outside of Europol.

5.1.1. MS Facing Systems

In Scope for 2021

Description	*Budget*	*Man-Days*
SIENA – Compliance requirements for data intake and processing in OD		
SIENA – improve performance		
SIENA – Notifications via email/SMS – implementation		
SIENA – UI Improvements – high priority		
SIENA – SIENA 3 Training EOL	-	970
SIENA – Alignment of environments		
SIENA – BPL Web Application		
SIENA – Brexit		

Annex 6

Action Plan of the Data Quality Control Coordinator

EDOC# 1159740 v2

Data Quality Control

Action Plan

Table of Contents

1. Purpose of this document

The purpose of this document is to define the action plan of the Data Quality Control Coordinator. This document provides the overview of the actions to be implemented in relation to data quality control. The implementation of the actions are detailed separately in specific guideline documents.

2. Background

In June 2020, a Data Quality Control Coordinator for Europol's Operations Directorate was appointed. The Data Quality Control Coordinator's work is to ensure the implementation of Europol's review mechanism and that data processing is performed in line with the Europol Regulation.

In September 2020, Europol received from the European Data Protection Supervisor (EDPS) a decision regarding the processing of large datasets (referred to as 'Europol's Big Data Challenge').

The EDPS decision arrived at the conclusion that the handling of large datasets for analysis work (and beyond that for all operational processing purposes based on Article 18(5) in connection with Article 18(2) of the Europol Regulation) has to commence on the basis of information with a Data Subject Categorisation (DSC)[10], already when contributed from Member States and operational cooperation partners or as soon as it is processed by Europol.

The EDPS decision highlighted that it is not possible for Europol from the outset, upon the receipt of large datasets, to ascertain that all underlying information complies with the list of the DSC, thus implying compliance risks with respect to the Europol Regulation.

The EDPS requested Europol to come up with an Action Plan to address the compliance risks identified by the EDPS.

Europol subsequently produced an Action Plan which focused on fundamental information security principles and data protection controls.

The last control, Action 5, focuses on the appointment of the Data Quality Control Coordinator as a way of mitigating the overall risk of processing of personal data where the DSC is not known, by ensuring that data processing is performed in line with the Europol Regulation, in particular with Annex II.

The Data Quality Control Coordinator will work in close cooperation with the Data Protection Function and produce a monthly progress reporting on the enhanced data review activities.

The monthly progress reporting will pay particular attention to the labelling of specific files, the compliance with access rights, and the deletion of data. A summary of the progress reporting will also be made available to the European Data Protection Supervisor (EDPS) on a quarterly basis.

[10] As set out in Annex II of the Europol Regulation (i.e. suspects, potential future criminals, contacts, associates, victims, witnesses and informants of criminal activities).

3. Four Layers of Data Protection in Europol

The process of data review at Europol rests on the principle of four layers of data protection.

1. Operations Directorate (OD) staff members processing operational data in an operational analysis project (AP) or in the Central Information Hub (O11) who:
   - assess the contributions due for reviewing;
   - decide on deletion or continued retention;
   - justify continued retention.

2. Data Quality Control Coordinator who:
   - monitors the implementation and quality of the data review process and advises staff members responsible for APs and other staff members as appropriate;
   - coordinates the review process where necessary (e.g. for SOC data – identify cases that need to be reviewed, send the list to the AP responsible, delete the contributions that are not being kept, etc.).

3. Data Protection Function (DPF) who:
   - ensure the internal application of data protection provisions on the processing of personal data;
   - monitor compliance and advise Europol staff.

4. European Data Protection Supervisor (EDPS)

4. Definition

4.1. Objectives

The primary objective is to ensure that data processing is performed in line with the Europol Regulation.

4.2. Scope

The scope of this action plan is to establish a data quality control monitoring system for Europol that will cover sufficiently the operational and governance needs of the organisation. The end purpose is to have a structured system in place, which will facilitate control of daily operations, ensure business continuity and foster data protection enhancement.

5. Actions

5.1. Defining Internal and External Stakeholders

The following internal stakeholders have been identified:

- Data Quality Control Coordinator
  The Data Quality Control Coordinator is a Senior Operational Analyst within the Operational and Analysis Centre.
- EDPS Action Plan Implementation Team
  In addition to the Data Quality Control Coordinator, Europol has established a dedicated task force in the Operations Directorate to ensure the implementation of the action plan addressing the risks raised in the EDPS Decision on 'Europol's Big Data challenge'.
- Operations Directorate – SPOC data quality
  All analysts and the appointed single points of contact for data quality issues from the Analysis Projects and Operational Centre.
- Europol's Data Protection Function.
- Europol Management.

The following external stakeholders have been identified:

- EU MS and operational partners
- Heads of Europol National Units
- Europol Management Board
- European Data Protection Supervisor

5.2. Defining Roles and Responsibilities

Data Quality Control Coordinator

The Data Quality Control Coordinator will help ensure the consistent implementation of the enhanced data review activities.

The task of the Data Quality Control Coordinator is to monitor that personal data is collected and processed for a specific purpose and is processed fairly and lawfully by Europol, in a manner that ensures the appropriate security of data processing and the overall protection of the rights and freedoms of data subjects.

The Data Quality Control Coordinator oversees the operational data management for purposes of data quality control and assurance, ensuring the quality of information processed by Europol in the Operations Directorate, ultimately guaranteeing that data protection principles and safeguards as stipulated in the Europol Regulation are upheld. This includes the continuous implementation of the data review mechanism, data quality and data compliance improvement.

The Data Quality Control Coordinator will:

- Run daily queries in order to identify data wrongly inserted;
- Check that everyone involved in the data review process is aware of their role and responsibilities and ensure that adequate training is provided where necessary;
- Check that data reviews are being properly carried out and documented;
- Check that all follow-up actions are being properly discharged;
- Ensuring that the data quality logbook is kept up to date.

Single Points of Contact (SPOCs)

Within the operational units in the Operations Directorate, Single Points of Contact (SPOCs) have been appointed for all APs in relation to data quality. These SPOCs are the represent the nexus between the Data Quality Control Coordinator and their respective APs for all data quality work aspects. They are also responsible for ensuring that all data reviews are completed and on time for their respective APs and for updating the logbook with all contributions received by their APs where the DSC is pending.

Moreover, the SPOCs also participate in bi-weekly meetings on the implementation of the EDPS Action Plan and the related quality control measures.

5.3. Preparing the Quarterly Data Review Process

The data review process is done on a quarterly basis. The Data Quality Control Coordinator provides all Analysis Projects a list of Siena messages to be reviewed every quarter, in line with the data protection safeguards of the Europol Regulation.

Developing the DSC Review Process

Once contributions without a DSC have been identified, they are recorded in a logbook and are reviewed every 3 months to ensure that the necessity and proportionality of the data processing is there.

Perform the Sensitive Data Categories Review

On a monthly basis, the Data Quality Control Coordinator will conducted searches to identify any sensitive data categories processed without justification.

Update and Maintain the Data Quality Logbook

All data quality issues are recorded in a logbook which is monitored by the Data Quality Control Coordinator.

Perform Progress Reporting

The Data Quality Control Coordinator will produce a monthly progress reporting on the enhanced data review activities. The monthly progress reporting will pay particular attention to the labelling of specific files, the compliance with access rights, and the deletion of data. A summary of the progress reporting will also be made available to the European Data Protection Supervisor (EDPS) on a quarterly basis.

Regularly Updated Guidelines

All in-house guidelines relating to data quality and data reviews are to be updated.

Training

Plan and execute training to be given to all analysts in relation to data quality, including the data review processes and DSC compliance.

Planning and Executing Regular Evaluations of the Data Review

Regular evaluations of the data review processes will be conducted. A dedicated evaluation on the DSC review is planned for end 2021.

6. Reference documentation

DOCUMENT TITLE
Role profile of DQCC
Data Review Manual
Guidelines for the Data Review for Data where the DSC is pending
Data Quality Logbook
List of Single Points of Contact
EDPS Decision on the own initiative inquiry on Europol's big data challenge
Europol Action Plan addressing the risks raised in the EDPS Decision on 'Europol's Big Data challenge'
EDPS Decision on the own initiative inquiry on Europol's big data challenge - Europol Action Plan
Europol Action Plan addressing the risks raised in the EDPS Decision on 'Europol's Big Data Challenge' – Progress Report March 2021