

**From:**

**To:**

**CC:**

**Sent at:**

**Subject:**

[REDACTED]  
EDPS-Europol <EDPS-Europol@edps.europa.eu>:  
SUPERVISION <supervision@edps.europa.eu>: [REDACTED]

[REDACTED]  
DPF Data Protection Function  
<DPF@europol.europa.eu>

03/05/22 14:34:28

Case 2022-0454 Consultation on Europol's MB Decisions  
- meeting of 29 April

Dear [REDACTED]

Let me first thank you and all Europol colleagues for the openness that led to the very fruitful meeting we held on Friday.

As already discussed during the meeting, please find attached in bullet points some kind of minutes including our main takeaways of the meeting. Please indicate whether you agree on how the different points are reflected and do not hesitate to share with us your comments, if any.

As to the steps forward: we are available to have a second meeting on the 16 May. Until that date (it may as well be the day of the meeting itself) you will have received a first input on our side.

Best regards,  
[REDACTED]



[REDACTED]  
[REDACTED]  
[REDACTED]  
**European Data Protection Supervisor**  
Postal address: Rue Wiertz 60, B-1047 Brussels  
Office address: Rue Montoyer 30, B-1000 Brussels  
[@EU EDPS](#) [www.edps.europa.eu](http://www.edps.europa.eu)

This email (and any attachment) may contain information that is internal or confidential. Unauthorised access, use or other processing is not permitted. If you are not the intended recipient please inform the sender by reply and then delete all copies. Emails are not secure as they can be intercepted, amended, and infected with viruses. The EDPS therefore cannot guarantee the security of correspondence by email.

**ZIP Archive with 1 entry**

Meeting on Europol MB Decisions\_03\_05\_2022.docx

## Meeting on Europol MB Decisions (29/04/2022)

- Tight time-frame:  
Publication 27 June / Entry into force/application: 28 June
- 4 MB Decisions are identified as priority for the Management Board - if not in place: then a legal vacuum would exist. Considering this legal vacuum risk, Europol seeks EDPS feedback as soon as possible
- The MB Decisions all provide for an 'one entry system'. This means that:
  - Data not having being categorised according to Annex II of the Europol Regulation, i.e. 'non-DSC data' are only 'assigned' to an Analysis Project ('AP'). They will not be accepted into the AP until the extraction is performed, i.e. the data cannot be used in intelligence reports;
  - For the functional separation of data, there will be different containers with dedicated access rights; only senior analysts will get access to non-DSC data (Europol has a matrix for access rights).
  - Currently non-DSC data is stored in the Computer Forensic Network
  - the data review reminders will be pushed automatically (in DAP - Data Analysis Portal)
- Which data can be searched against which data?
  - Non-DSC cannot be searched against non-DSC data;
  - Currently DSC data are checked against non-DSC ( [REDACTED] ); and they will continue to be;
  - Non-DSC data would be searched against DSC data: according to Europol this is the purpose of the legislator for Articles 18(6a) and 18a, i.e. to proceed to the Data Subject Categorisation
- Unified Search Engine will be configured accordingly - different users would have different possibilities depending on the labelling of the data (DSC/non-DSC).  
If data is processed in the context of Article 18a only, USE will perform searches only within this investigation file
- Article 18a (1)(a)(ii): provides for the cross checking of data pursuant to Article 18(2) (a) in exceptional and duly justified cases
  - Article 18(2)(a) is applied for processing in the context of the Europol Information System. This possibility under Art. 18a would mean that non-DSC data would be exposed to certain MSs for cross-checking purposes. At this point in time, Europol does however not have a specific business case to further explain to the EDPS in which cases this provision will be used;
  - Europol reads this provision also in relation to Article 20(2a) - joint operation analysis - which applies only to DSC data;
  - Europol did not proceed to provide criteria regarding the cases that this new provision of Article 18a could be used both because they are working under very strict time limits and because the provision of such criteria requires more experience.

- Intelligence stemming from other APs will not be shared and used in 18a APs. Operational analysis will be conducted in the context of each 18a AP (example of ATM attacks in different countries leading to the identification of suspects).
- Data quality coordinator: The inclusion in the implementing rules was not considered necessary (legal provision should remain generic enough) - his role and task is a function internal to Europol and is described in other internal Europol documents.
- New purpose of scientific research:
  - Article 33a is very comprehensive and did not need to be further complemented
  - Europol will adopt a relevant processes (there they will differentiate between research and innovation and innovative tools in operational analysis);
  - However a strong indicator could be cases where academia or other third parties participate (e.g. Horizon 2020)
- Article 33a: what is meant by 'binding general scope' that the MB shall establish for the research and innovation projects of Europol?  
According to Europol this is the way suggested for the MB to keep control of the types of projects that Europol will participate to.
- Europol has not yet considered how to apply the provisions about data subject rights and sensitive data to non-DSC data. This is excluded from the scope of the implementing rules discussed today. However, there will be:
  - No exclusion of non-DSC data from access rights
  - Processes will be adjusted
- Conscious decision not to provide further criteria for the 'assessments' in the implementing rules (e.g. there will be no further details as to when the extension of period of processing under 18(6a) will be considered 'justified', or when it should be deemed relevant that the DPO informs the EDPS where a third country provides investigative data to Europol). Each assessment will be substantiated and documented.