EUROPEAN COMMISSION
DIRECTORATES-GENERAL
EMPLOYMENT, SOCIAL AFFAIRS AND INCLUSION
REGIONAL AND URBAN POLICY
Joint Audit Directorate for Cohesion - DAC.1 - Audit I

ARACHNE

FAQ on data protection and related issues

Status as of 10th July 2024

1. *Could you elaborate when the DPIA was last updated? Was the data processing in the context of RRF taken account in this last update and, if so, what were the results? Would it be possible to share the observations by the DPO?*

   In accordance with Art. 39 and 40 of the Regulation (EU) 2018/1725, the Commission services have performed a Data Protection Impact Assessment (DPIA) to analyze, identify, and minimize the data protection risks of the processing operation by ARACHNE. The outcome of the assessment showed that considering the safeguards, security measures, and mechanisms to mitigate the risk, the processing of personal data does not represent a high risk to the rights and freedoms of natural persons, as validated by the Commission Data Protection Officer (DPO) on 22/07/2022.

   The tool ARACHNE was updated on 14/02/2022 to enable Member States to upload Recovery and Resilience Facility (RRF) data. The modification made in terms of data processing was the inclusion of Ultimate Beneficial Owners (UBO) information as well. Since ARACHNE was validated only after this update, UBO data was already considered in the DPIA. It is important to note that UBO data is not specific to RRF; it can be uploaded for companies and organizations involved in projects for all types of European funds.

   Regarding the observations by the DPO, the DPIA is a comprehensive document that includes an analysis of the risks associated with the processing of personal data and the measures in place to mitigate those risks. The DPO's validation indicates that the measures and safeguards implemented are sufficient to protect the rights and freedoms of natural persons. The DPIA considers the scale of personal data collection, the use of algorithms, and other relevant factors to ensure compliance with data protection regulations.

2. *Since Arachne has been specifically updated to accommodate RRP before the validation by the DPO, could the Commission elaborate how the current security measures and safeguards in place are to be considered sufficient?*

   The Commission acknowledges the significant expansion of personal data collection associated with the RRF and the incorporation of algorithms within the ARACHNE system. Following these updates, a thorough DPIA was conducted, considering the enhanced scope and complexity of data processing. The DPO has reviewed the updated DPIA along with the implemented security measures and safeguards and has found them to be adequate. These measures encompass strict access controls, adherence to the principle of data minimization, and ongoing assessments of processing activities, ensuring rigorous protection of personal data.

   It is imperative to note that a DPIA is not mandatorily required to undergo updates with every minor modification to the system. The operative processing within ARACHNE is fundamentally grounded on Article 5(1)(a) and (b) of Regulation (EU) 2018/1725. Consequently, under Article 39(10) of the same regulation, unless specified otherwise, the requirement to update the DPIA is not applicable if the processing has a legal basis in a legal act adopted based on the Treaties, which governs the specific processing operation or set of operations, and a data protection impact assessment has been conducted as part of a broader impact assessment preceding the enactment of that legal act.

   Furthermore, it is important to clarify that DPIAs do not necessarily require approval from the DPO by default. The primary responsibility for the DPIA rests with the data controller. The Commission remains committed to data protection, ensuring that any significant alterations to ARACHNE or changes in processing operations will undergo an appropriate review of the DPIA, as mandated by the applicable legal framework, to maintain ongoing compliance with data protection regulations.

3. *Could you elaborate more about the scope of the DPIA? For example, does the DPIA include all the different purposes for processing personal data? If yes, could all these different purposes be shared with us?*

   Following the new Regulation (EU) 2018/1725 of 23 October 2018 (EUDPR) and the Implementing Rules (Commission Decision (EU) 2020/969) a new Data Protection Record and a Data Protection Impact Assessment for ARACHNE have been prepared by the Commission services and validated on 22/07/2022 by the Commission DPO and published on 27/11/2023 in the Register of the Data Protection Officer (see link: https://ec.europa.eu/dpo-register/detail/DPR-EC-00598.4.)

   The Data Protection Impact Assessment (DPIA) for ARACHNE encompasses the creation of an adequate and accurate fraud prevention and detection tool (Arachne), whose purpose is to generate risk indicators across various categories to assess project and entity riskiness. In particular, the purpose of the processing of the personal data is to produce a series of pre-defined risk indicators divided in several risk categories to provide an objective view on the riskiness of projects and the related entities (i.e. beneficiaries, (sub)contracts, contractors/suppliers): procurement process, contract management, funding eligibility, project performance, funded projects concentration, basic logicality/reasonability of project data, reputational and fraud alerts, including final beneficial owner as of Q4 2022.

4. *Which risks have you identified in the DPIA?*

   Security measures and risks identified in the DPIA include, amongst others, access permissions, physical security measures, ensuring the security of IT channels, encryption of personal data,

review of security measures, data breach handling mechanisms and maintenance of software.

5. *What risks have been identified with regard to the purpose of processing personal data to produce a series of pre-defined risk indicators (i.e., risks connected to the use of this algorithm) and what are the mitigating measures in place?*

   The Commission acknowledges the importance of a thorough risk analysis in the context of processing personal data to produce pre-defined risk indicators through ARACHNE. The purpose of this processing is to provide an objective assessment of the riskiness associated with various projects and related entities, such as beneficiaries, (sub)contracts, contractors, and suppliers. This is achieved by analyzing data to identify potential risks in areas like procurement processes, contract management, funding eligibility, project performance, and others.

   In terms of risks connected to the use of the algorithm for generating these risk indicators, the Commission has identified several potential risks, including the accuracy of the risk indicators, the potential for bias in the algorithm, and the misuse of personal data in any funds managed by Arachne, including among others ESIF funds and RRF. To mitigate these risks, the Commission has implemented a range of measures. These include:

   1. Regular validation and testing of the algorithm to ensure its accuracy and to minimize any potential biases. This includes the use of updated and verified data from Member States authorities and agencies, as well as cross-verifications before uploading data into ARACHNE.

   2. Access permissions and physical security measures to prevent unauthorized access to personal data. This includes the use of EU-Login and two-factor authentication, as well as a zone-based network architecture with multiple firewalls.

   3. Ensuring the security of IT channels and the encryption of personal data during transmission and storage. The communication between ARACHNE front-end and back-end is fully encrypted.

   4. Regular review of security measures and data breach handling mechanisms to respond promptly to any security incidents. This includes the implementation of security measures in line with the Commission Decision (EU, Euratom) 2017/46 and its subsequent versions.

   5. Maintenance of software and systems to prevent vulnerabilities and ensure the ongoing integrity and confidentiality of the data processing. The Commission has a dedicated IT team that regularly updates and patches the ARACHNE system to address any potential security vulnerabilities.

   6. Data minimization and retention policies to ensure that only necessary data (in detail, personal data ex art. 4 of the GDPR) is collected and stored for no longer than required. The Commission adheres to the principles of data minimization and storage limitation, ensuring that personal data is not kept longer than necessary for the purposes for which it was collected.

   7. Transparency and communication with data subjects regarding the processing of their data and their rights. The Commission provides a privacy statement on the ARACHNE website and ensures that data subjects are informed about their rights and how to exercise them.

   8. Data Protection Impact Assessment (DPIA) to analyze, identify, and minimize data protection risks of the processing operation by ARACHNE. The outcome of the assessment showed that taking into account the safeguards, security measures, and mechanisms to mitigate the risk,

the processing of personal data does not represent a high risk to the rights and freedoms of natural persons, as validated by the Commission DPO on 22/07/2022.

9. Consultation with the European Data Protection Supervisor (EDPS) when necessary, to ensure compliance with data protection regulations and to address any concerns raised by Member States regarding data protection.

These measures are designed to ensure that the processing of personal data within ARACHNE is carried out in a secure, lawful, and fair manner, in full compliance with EU data protection law.

6. *Which risks have you identified in the DPIA?*

Security measures and risks identified in the DPIA include access permissions, physical security measures, ensuring the security of IT channels, encryption of personal data, review of security measures, data breach handling mechanisms and maintenance of software.

7. *Does the DPIA include a separate section about data processing and privacy risk mitigation specifically with regard to the RRF? If yes, could you share this information with us? If not, I would like to request if the DPIA includes information about similar data processing purposes such as the RRF?*

The DPIA on Arachne does not contain a specific section dedicated exclusively to the RRF. However, it's vital to understand that the DPIA has been crafted to ensure full compliance with the GDPR, and the data processing and risk mitigation strategies are applied across the board to all funding instruments that we manage. This approach guarantees that the principles safeguarding data privacy and protection are uniformly applied, which includes the activities associated with the RRF. While the DPIA may not explicitly mention the RRF, the processes and safeguards it describes are certainly applicable to it as part of our overarching commitment to data protection. The purpose of processing does not change with the extension by RRF. No new steps within DPIA is necessary linked thereto.

8. *What measures are (currently) taken to mitigate privacy risks specifically with regard to RRF and the responsibilities of member states uploading data into ARACHNE?*

In addressing privacy risks associated with the RRF, it's important to emphasize that our risk mitigation measures are not tied to specific categories of data but to the processing activities themselves. The extension of data categories under the RRF does not necessitate a separate risk assessment as such. Our comprehensive privacy risk mitigation framework applies to all data processing under the RRF, ensuring adherence to the GDPR and the specific requirements of the Common Provision Regulation (CPR).

The data that Managing Authorities are required to make publicly available under Article 49.3 of the CPR, although similar to the data used in ARACHNE, serves a different purpose—ensuring public transparency as opposed to ARACHNE's role in performing verifications and controls pursuant to Article 69 of the CPR. The ARACHNE privacy statement, available on its homepage, specifies the details of data processing activities and outlines the protective measures for data subjects.

Data processing within ARACHNE is informed by the information that program authorities are mandated to collect under Article 69 of the CPR. This processing adheres to Regulation (EU) 2018/1725, specifically Article 5(1)(a) and 5(1)(b), which provide the legal basis for tasks carried out in the public interest or official authority and for processing necessary to fulfill a legal

obligation, respectively.

We maintain a strong commitment to managing all privacy risks effectively. The safeguards we have implemented are designed to ensure the protection of data across all operations within ARACHNE, regardless of whether the data is for RRF or other purposes. This holistic approach to risk management ensures that the integrity and security of all personal data are consistently upheld within our data processing practices.
The ARACHNE data processing specifics are clearly detailed in its privacy statement, which can be accessed on the ARACHNE homepage. The privacy statement delineates the protections in place for data subjects, while Article 49.3 pertains to the obligations of Managing Authorities. Data collection for ARACHNE is derived from mandatory information that the program authorities are required to collect under Article 69 of the CPR. Moreover, this processing is conducted in accordance with Regulation (EU) 2018/1725, particularly under Article 5(1)(a), which pertains to tasks performed in the public interest or by official authority of the Union institution, and Article 5(1)(b), which relates to processing necessary for compliance with a legal obligation of the data controller. We are committed to ensuring that all privacy risks are managed effectively, with appropriate measures in place to protect the data processed within the framework of the RRF and ARACHNE.

9. *What are the safeguards in place to ensure that the data submitted in the context of the RRF is not processed for other goals?*

While there isn't a dedicated section within the DPIA specifically for RRF-related data, it is important to clarify that projects associated with the RRF are uploaded into dedicated RRF modules within Arachne. This modular approach ensures data segregation, effectively creating a separate environment for the RRF, which in turn helps prevent the processing of this data for unrelated purposes. Furthermore, it's important to emphasize that the safeguards we have in place for the protection of data within the RRF are technically equivalent to those applied to the Common Provision Regulation (CPR) data. This consistent application of safeguards across different funding streams helps to streamline protection measures and minimize the risk of any unintended data processing activities.

For all data uploaded into Arachne, a comprehensive set of organizational and technical measures safeguard personal data. These measures are extensively documented in the Data Protection Record, which is publicly accessible on the Register of the Commission's Data Protection Officer (DPO) at the following link: https://ec.europa.eu/dpo-register/detail/DPR-EC-00598. The documentation includes key information, such as:

The identity and contact details of the controller, the DPO, and, where applicable, the processor and joint controller.
The specific purposes for which data is processed.
Descriptions of the data subject categories and the types of personal data processed.
Recipient categories to whom data may be disclosed, including those in third countries or international organizations.
Where applicable, details of data transfers to third countries or international organizations, including safeguards.
Envisaged retention periods for different data categories.
A general description of the technical and organizational security measures, as prescribed by Article 33 of Regulation 2018/1725.
The DPIA, validated by the DPO on 22 July 2022, thoroughly assessed the principles of proportionality, necessity, and integrity. Data subjects are informed of their rights through a privacy statement available on the ARACHNE website and, depending on the Member State's decision, through data protection clauses in grant/contract application documents.

To ensure data accuracy, verification is conducted at the time of collection and periodically thereafter. The principles of data minimization, storage limitation, and additional technical safeguards such as encryption and secure storage protocols are rigorously applied to uphold personal data protection by design.

The DPIA clearly outlines the purposes for data processing, which are regularly reviewed to maintain accuracy and relevance. Should there be an intention to use personal data for a new purpose, compatibility with the original purpose is verified, or specific consent is obtained for the new purpose, thereby ensuring continued adherence to data protection principles, and mitigating any privacy risks.

This cohesive approach to data protection is designed to address concerns from Member States and provide assurance that all data, irrespective of the funding source, is treated with the same high level of security and privacy.

10. *Could you please share (a summary of) the DPIA analysis on proportionality and subsidiarity?*

The DPIA analysis on proportionality aligns with Article 125(4)(c) of Regulation (EU) No 1303/2013 and Article 74 of Regulation (EU) 2021/1060, focusing on effective and proportionate anti-fraud measures. Data collection is limited to operational information of projects and contracts sourced from programme authorities, and data from public databases, minimizing intrusion into personal privacy. The processing aims to identify potential fraud risks while respecting individual rights to privacy and data protection, ensuring proportionality between intrusion and aim.

Consideration has been given to competing interests, balancing the necessity of anti-fraud measures with privacy rights, and data protection regulations. Risk scoring indicators are used as aids in internal anti-fraud strategies and control procedures, subject to human review and judgment, rather than automated decision-making.

With reference to subsidiarity, the collection of data for ARACHNE is based on information that programme authorities need to collect under Article 69 of the CPR and is processed under Regulation (EU) 2018/1725, notably Art. 5(1)(a) (Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body) and Art. 5(1)(b) (Processing is necessary for compliance with a legal obligation to which the controller is subject).

11. *What is necessity (what does knowledge about 1 individual (chairpersons of school boards, foundations, etc) contribute to the assessment of whether funds are well spent by the organization?), proportionality (does the goal outweigh the infringement on the rights and freedoms of those involved: how have those interests been weighed?) & subsidiarity (e.g., can the goal not be achieved in a less privacy invasive way through monitoring by a ministry itself?)*

The necessity of processing personal data within the ARACHNE system, including data about individuals such as chairpersons of school boards and foundations, is to assess ex-ante risks linked to an applicant when applying for funding. This contributes to the assessment of whether funds are well spent by the organization by identifying criticalities and risk management, promoting the use of a risk-based approach to the planning of verifications of projects, and complementing the risk assessments with regards to fraud and irregularities.

The proportionality of the processing is addressed by ensuring that only a limited amount of personal data is collected for specific purposes. The data comprises operational information of projects and contracts uploaded by the programme authorities or sourced from public databases.

The derived risk scoring indicators identifying possible risk of fraud and/or irregularities will be checked by the programme authorities according to their internal anti-fraud strategy and control procedures before drawing any conclusions and will not be used to take automatic decisions.

Subsidiarity is considered in the sense that the ARACHNE tool is designed to be an integrated IT tool for data mining and data enrichment aimed at supporting Member States Authorities, Agencies, and Intermediate Bodies in their administrative controls and management checks on EU (co)funded projects. ARACHNE provides a harmonized and standardized tool that can be utilized across EU Member States to increase the efficiency and effectiveness of controls and audits, thereby offering a centralized solution that may not be as effectively achieved through individual monitoring by separate ministries and/or authorities at national level.

12. *What risks have been identified (such as the sticking of a negative label on a person ("higher risk of misuse of funds"), on the basis of which further research is done, without the knowledge of the person concerned and without our being able to objectively establish that this label was rightly stuck on someone) and what are the mitigating measures taken by the EC?*

The identified risks associated with the ARACHNE system include the potential for data exposure due to administrator error, software vulnerabilities, abuse of access privileges, and unauthorized access, among others. These risks could lead to confidentiality breaches, integrity breaches, and availability breaches, which might result in consequences such as identity theft, fraud, damage to reputation, or dissemination of sensitive personal data.
The European Commission has taken several mitigating measures to address these risks:

Access Control: Access to ARACHNE is restricted and controlled. Users are identified and granted access based on their role within the management and control system for specific operational programs. Periodic reviews of user accounts are conducted to ensure that access rights are terminated when no longer needed or justified.

Physical Security: Technical and organizational security measures are implemented to protect personal data against accidental or intentional destruction, loss, or unauthorized access. This includes managed firewalls, port and application filtering, and network address translation via firewalls and load balancers [1].

Encryption: Communication between the ARACHNE front-end and backend is encrypted to ensure the confidentiality of data during transmission.

Data Breach Handling: Procedures are in place for handling personal data breaches, including notification to the European Data Protection Supervisor (EDPS) in case of a breach of the rights and freedoms of natural persons.

Regular Review: The security plan and implemented security measures are reviewed and updated on a yearly basis or sooner if there is a change in the system's environment.

Transparency: The Commission ensures transparency by providing a privacy statement that informs data subjects about their rights and how to exercise them. This includes information on how to request changes to their data and the "Feedback loop" procedure for correcting wrong data mapping.

These measures are designed to prevent the undue negative labeling of individuals and to ensure that any risk indicators produced by ARACHNE are used appropriately and in accordance with data protection regulations.

13. *What independent audits (/certification) have been done/are being done on privacy & information security of both processes and systems?*

    To date, no external independent audits or certifications have been specifically conducted concerning the privacy and information security of the processes and systems for ARACHNE. It's crucial to distinguish between the Data Protection Impact Assessment (DPIA) and independent audits. The DPIA, which focuses on assessing and mitigating data protection risks, is an internal process conducted by the data controllers within the European Commission and it has been completed in line with Regulation (EU) 2018/1725. The DPIA was thoroughly documented and has received validation from the Commission's Data Protection Officer (DPO).
    In contrast, audits are typically performed by external parties, and in the context of the European Commission, such audits regarding data protection and security can be conducted by the DPO and the European Data Protection Supervisor (EDPS). These audits are separate from the DPIA process and are intended to independently evaluate the effectiveness of privacy and security measures.
    Furthermore, ARACHNE is governed by an IT Security Plan that incorporates a detailed risk assessment. This plan has been approved by the ARACHNE Steering Committee and adheres to the Commission Decision C(2006) 3602. The plan is in alignment with the security standards established within the European Commission and ensures that robust technical and organizational measures are continuously upheld to safeguard personal data.

    The European Commission remains committed to the highest standards of data protection and security. Regular reviews and updates to our security measures are part of our ongoing efforts to ensure that personal data is protected against any potential risks. Should the need for an independent audit arise, it will be conducted in accordance with the relevant procedures and the oversight of the DPO and EDPS.

14. *What information should we provide to data subjects about the EC's processing operations and their rights (and where they can exercise them) and is there a difference in rights and obligations for a measure that has already been implemented (and accounted for) before the measure was included in the RRP (ex post) and a measure that has yet to be implemented (ex ante)?*

    Data subjects should be informed about their rights regarding the EC's processing operations as outlined in the privacy statement attached to the data processing records. This information should include the rights of data subjects as per Articles 17 to 24 of the Regulation (EU) 2018/1725, which cover the right of access, right to rectification, right to erasure (right to be forgotten), right to restriction of processing, notification obligation regarding rectification or erasure of personal data or restriction of processing, right to data portability, right to object, and rights related to automated individual decision making, including profiling. The privacy statement should be published on a website, with the EC's example being available at http://ec.europa.eu/esf/home.jsp. Guidance for data subjects on how and where to consult the privacy statement is provided at the beginning of the processing operation.
    Data protection rights apply to all data subjects regardless of when the measure was implemented. The key factor is that data subjects are informed about their rights and the processing of their personal data in a timely and transparent manner.

15. *While a DPIA is mainly focused on privacy rights, the IAMA looks at a broader range of fundamental rights and specifically assesses the impact of algorithms. Do you know whether an IAMA is conducted for Arachne?*

    The Impact Assessment on Algorithmic Management (IAMA) is not an obligation stated by the EU data protection regulation, specifically Regulation (EU) 2018/1725. This regulation mandates a

Data Protection Impact Assessment (DPIA) for processing operations likely to pose a high risk to the rights and freedoms of natural persons, particularly when using new technologies.

The DPIA conducted for ARACHNE has considered the necessary safeguards, security measures, and mechanisms to mitigate the risk, and the processing of personal data by ARACHNE does not represent a high risk to the rights and freedoms of natural persons. This assessment was validated by the Commission Data Protection Officer on 22 July 2022.

Since the IAMA is not a requirement under the current data protection regulation and considering that the DPIA did not identify high risks associated with the use of ARACHNE, we can conclude that an IAMA is not needed for ARACHNE based on the information available and the risk assessment conducted. However, it is important to note that while the DPIA is focused on data protection and privacy rights, an IAMA could potentially cover a broader range of fundamental rights impacts. The decision to conduct an IAMA would be at the discretion of the Commission services, based on their assessment of the necessity to address broader impacts of algorithmic processing beyond privacy and data protection.

16. *Will the European Commission be qualified as a controller of Arachne since they determine the purpose and means of the Recovery and Resilience Facility (RRF)?*

Under direct management, the European Commission is the sole controller of the data related to the RRF. This means the Commission determines the purposes and means of the processing of personal data within the ARACHNE framework. As the sole controller, the Commission is responsible for ensuring that all data processing complies with EU data protection laws, specifically Regulation (EU) 2018/1725. This responsibility includes overseeing processing activities, safeguarding personal data, and upholding the rights of data subjects.

In contrast, under shared management, both the Commission and Member States might act as controllers, sharing responsibility for determining the purposes and means of data processing. However, this is not the case with the RRF.

Conditions on Storage of data

1. *Is the data storage in ARACHNE subject to a data storage protocol and deletion deadlines?*

The Commission IT department (DIGIT), responsible to store data for Arachne, implements all technical and organizational security measures to protect the personal data against accidental or intended destruction or loss of data, or non-authorized access. The Data Centre policy ensures that state of the art physical security is applied.

The European Commission implements security measures to protect server hardware, software, and the network from accidental or malicious manipulations and loss of data. All data is stored on European Commission servers, in line with the technical security provisions laid down in the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission, its subsequent versions, its implementing rules and the corresponding security standards and guidelines, as well as the Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on the security in the Commission, and the Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information, its implementing rules and the corresponding security notices.

Personal data held is regularly reviewed and is not kept any longer than it is needed (for the purpose it was collected). Personal data is not kept for longer than for the intended purpose, except for archiving purposes in the public interest, scientific or historical research purposes or

statistical purposes. In such cases, these personal data are clearly identified.
Please find below a table summarizing the retention period per data category:

Data category	Retention period
All projects, contracts and expenses data, which are uploaded by the Member States in the ARACHNE database	10-year period from the last payment claim for the period by the programme authorities to the Commission
External database containing data on companies and legal representatives, Enforcements and Sanctions lists, PEP (Politically Exposed Persons) list and Adverse Media	Data will be updated regularly, i.e. on a monthly to quarterly basis.
All risks computed for each Member States projects	10-year period from the last payment claim for the period by the programme authorities to the Commission.

2. *The data will remain on the servers for 10 years. Could the Commission share the (legal) grounds/provisions to motivate the necessity to store information for a period of 10 years?*

The necessity to store information for a period of 10 years on the servers is motivated by the retention period policy, which states that all projects, contracts, and expenses data uploaded by the Member States in the Arachne database, as well as all risks computed for each Member State's projects, are to be retained for a 10-year period from the last payment claim for the period by the programme authority to the Commission in accordance with the Common Retention List. This retention period is aligned with the legal and financial management requirements for EU funds to ensure proper auditing, accountability, and potential investigations into fraud or irregularities.

Opinion of European Data Protection Supervisor of 17 February 2014

3. *The EDPS presumes the compatibility with Regulation EC No. 45/2001 subject to certain conditions (p.15). The EDPS had doubts in view of the legal basis according to Regulation EC No. 45/2001. How has the Commission dealt with those reservations?*

ARACHNE was put in production in 2013. The European Data Protection Supervisor (EDPS) refers, in his opinion of 24 April 20141, to Regulation EC No. 45/2001 of the European Parliament and of the Council of 18 December 2000 (on the protection of individuals regarding the processing of personal data by the Community institutions and bodies and on the free movement of such data). The EDPS stated in this opinion that there was a sufficient legal basis for the processing performed by ARACHNE, notably:

"(…) that the combination of Article 34 and Section 7 of Regulation 1828/2006 as well as Chapter 2.2.3 of the COM's Communication on the Anti-Fraud Strategy constitute a sufficient legal basis for the purposes of Article 5(a) of the Regulation."

Further on, Regulation EC No. 45/2001 has been superseded by Regulation (EU) 2018/1725 of 23 October 2018 (EUDPR) and the corresponding Implementing Rules (Commission Decision (EU)

[1] *Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Commission regarding the "Risk analysis for fraud prevention and detection in the management of ESF and ERDF" - ARACHNE Brussels, 17 February 2014 (2013-0340)"*

2020/969). Consequently, a new Data Protection Record and Data Protection Impact Assessment for ARACHNE were prepared by the EC services and validated on 22/07/2022 by the Commission Data Protection Officer (hereafter also the Commission DPO). The Commission DPO, on the merit of the analysis carried out, did not consider it necessary to submit the DPIA to the EDPS.

4. *Has ARACHNE been reviewed in view of the requirements of the Regulation (EU) 2018/1725, especially Art. 5?*

   Following the new Regulation (EU) 2018/1725 of 23 October 2018 (EUDPR) and the Implementing Rules (Commission Decision (EU) 2020/969) the Commission services consider that Article 5(a) and 5(b) is applicable for the processing performed by ARACHNE:

   "(…)

   5(a) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body.

   5(b) Processing is necessary for compliance with a legal obligation to which the entity of the operational controller is subject (…)"

5. *Has the European Data Protection Supervisor been involved on the basis of the Regulation (EU) 2018/1725?*

   Following Regulation (EU) 2018/1725 of 23 October 2018 (EUDPR) and the Implementing Rules (Commission Decision (EU) 2020/969), a new Data Protection Record has been validated by the Commission DPO on 22/07/2022 (ref. https://ec.europa.eu/dpo-register/detail/DPR-EC-00598.3). Prior consultation of the EDPS has not been deemed necessary by the Commission DPO.

6. *Has the COM carried out an assessment of the impact of the envisaged processing operations on the protection of personal data accordingly Art. 39, 40 of the Regulation (EU) 2018/1725?*

   Following an initial evaluation, the EC services considered the possibility that the processing operations on the protection of personal data by ARACHNE might potentially result in a risk to the rights and freedoms of natural persons.

   In accordance with Art. 39, 40 of the Regulation (EU) 2018/1725 the Commission services have performed a Data Protection Impact Assessment to analyze, identify and minimize the data protection risks of the processing operation by ARACHNE. The outcome of the assessment showed that taking into account the safeguards, security measures and mechanisms to mitigate the risk, the processing of personal data does not represent a high risk to the rights and freedoms of natural persons, as validated by the Commission DPO on 22/07/2022.

7. *Has the COM examined that the different steps of data processing in the context of ARACHNE is compatible with the Regulation (EU) 2018/1725? Is there a written opinion of the Legal Service?*

   Following the new Regulation (EU) 2018/1725 of 23 October 2018 (EUDPR) and the Implementing Rules (Commission Decision (EU) 2020/969) a new Data Protection Record and a Data Protection Impact Assessment for ARACHNE have been prepared by the Commission services and validated on 22/07/2022 by the Commission DPO.

The Commission DPO is the responsible and competent service at the European Commission. The validation procedure does not require a written opinion of the Commission Legal Service.

Sufficiently suspicion of fraud/ conflict of interest/ irregularity

1. *In view of the data mining, the German Data Protection Supervisor has required a sufficiently specified suspicion of fraud/irregularity in his opinion of 2014. In the jurisprudence of the German Constitutional Court, interventions in the data protection rights of the data subjects must be assessed by their intensity. Intensive interventions – such as extended data analysis – require a sufficiently clear and proportionate legal basis. The legal basis must provide clear intervention thresholds for the acting authorities. For which specified situations is datamining by ARACHNE authorised?*

   Article 125(4)(c) of Regulation (EU) No 1303/2013 and Article 74 of Regulation (EU) 2021/1060, state that Managing Authorities have to 'put in place effective and proportionate anti-fraud measures taking into account the risks identified'. ARACHNE uses only a limited amount of personal data collected for specific purposes. The data is either operational information of beneficiaries, projects and contracts uploaded by the programme authorities or public source databases.

   The derived risk-scoring indicators identifying possible risk of fraud and/or of irregularities are taken into account by the programme authorities or the Audit Authorities as part of their internal anti-fraud strategy and control procedures, before drawing any conclusions. These risk-scoring indicators generated by ARACHNE are not used to take automatic decisions.

   The Commission services ensure transparency by complying with the conditions pertaining to the information to be provided, and the rights of data subjects mentioned in Articles 15 to 24 of Regulation (EU) 2018/1725.

   The compliance of the data processing performed in ARACHNE with these articles is detailed in the privacy statement published on the ARACHNE homepage: https://ec.europa.eu/social/main.jsp?catId=325&intPageId=3587

   Programme authorities using ARACHNE must comply with national and European data protection regulations. Therefore, they are obligated to inform beneficiaries that their data will be processed for the purpose of the identification of risk indicators, preferably by inserting data protection clauses in the grant/contract application documents.

2. *Regulation (EU) 2018/1725 states further requirements, which must be observed in order to be able to assume that data processing is lawful. What are the necessary technical and organizational measures? How are the rights of the data subjects guaranteed and the necessary obligations to inform the data subjects complied with in view of the datamining by ARACHNE?*

   Both organisational and technical measures are detailed in the Data Protection Record available on the Register of the Commission DPO at the following link: https://ec.europa.eu/dpo-register/detail/DPR-EC-00598.2

   The records kept in the database include:

a. the name and contact details of the controller, the data protection officer and, where applicable, the processor and the joint controller.

b. the purposes of the processing.
c. a description of the categories of data subjects and of the categories of personal data.
d. the categories of recipients to whom the personal data have been or will be disclosed including recipients in Member States, third countries or international organizations.
e. where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and the documentation of suitable safeguards.
f. where possible, the envisaged time limits for erasure of the different categories of data.
g. where possible, a general description of the technical and organizational security measures referred to in Article 33 of the Regulation 1725/2018.

The data subjects are informed about their rights and how to exercise them through a privacy statement published on the ARACHNE website (publicly available), as well as in the publicly available Commission Register of records on processing of personal data. Upon decision of the Member State, data subjects are informed about their rights through data protection clauses included in grant/contract application documents.

Data Transmission, Data verity and Clarity of Data

1. *Is the data transmission sufficiently encrypted and authenticated according to the technical and organizational standard of EU-Law?*

The authentication to the ARACHNE web application, which is required to upload data files in the system and to retrieve the risk scoring results, is guaranteed via EU-Login and 2-factor authentication.

2. *Do these data only involve project data, contract data and expenses/invoices? Or do these data comprise other information deriving from public sources?*

ARACHNE produces a series of pre-defined risk indicators divided in several risk categories to provide an objective view on the riskiness of projects and the related entities (i.e., beneficiaries, (sub)contracts, contractors/suppliers): procurement process, contract management, funding eligibility, project performance, funded projects concentration, basic logicality/reasonability of project data, reputational and fraud alerts, including BO (beneficial owner data) as of Q4 2022.
These risk checks result in risk indicators on projects and contracts. The risk checks are performed processing, among other data categories, the following personal data:

From the Member States authorities and agencies:

- Beneficiaries and partners: name, address, VAT number, role.
- Key staff: name, function, date of birth.
- (Sub-)Contractors: name, address, VAT number.
- Key experts for service contracts: name, date of birth
- Data on final beneficial owner data (BO) of beneficiaries, contractors, and subcontractors: name, date of birth as of Q3 2022.
- Financial data (e.g. invoices and payments), agreed grants and expenditure declared

From the external public data sources:
a) From a commercial provider (Orbis database through VADIS ref. https://www.moodys.com/web/en/us/capabilities/company-reference-data/orbis.html):
Comprehensive information on companies and their financial statements submitted to regulatory bodies and published as per the national applicable rules and
shareholders/management/key staff: name, function.
b) from a commercial provider (Word Compliance database - LexisNexis)

1) Global PEP List: profiles of Politically Exposed Persons from over 230 countries, including family members and close associates. State owned companies and foreign officials are added to this list.
2) Global Enforcement List: Information from regulatory and governmental authorities, including warnings and actions against individuals and companies, narcotic traffickers, money launderers, fraudsters, human traffickers, fugitives and other criminals.
3) Global Sanctions List: Aggregated information from sanction lists around the world and grouped into the Global Sanction Lists
4) Global Adverse Media List: This is an extensive proprietary database, comprised of public domain news, money launderers, fraudsters, arms dealers, narcotic traffickers, and other criminals. 25.000 newspapers and magazines in more than 35 languages are monitored for risk relevant information for protection from risk entities in the public domain.

3. *Are these other data exclusively retrievable from publicly available sources (i.e., public company registers)? Or are these data retrieved from media and internet reporting?*

   External data is collected and provided to ARACHNE via private data providers, based on a commercial relationship. The private data providers collect data on companies from publicly available information such as official annual reports or balance sheets submitted to regulatory bodies. Notably, data on Politically Exposed Persons, Sanction lists and Enforcement lists are retrieved from regulatory and governmental authorities, whereas adverse media data is collected via the websites of a dedicated list of newspaper and magazines.

4. *How can a high quality of the data be ensured for instance in case of the criteria of credibility? What is the « adverse media list »?*

   The data commercial providers ensure the high quality of data. Several quality review and quality assurance procedures are put in place to ensure that the provided data is correct, up to date and reliable.
   Adverse media is a collection by World Compliance of press articles published by newspapers and magazines holding data on companies and persons that have been linked to illicit activities. As specified by World Compliance, adverse media is an extensive proprietary database of profiles that have been linked to illicit activities from over 30,000 feeds worldwide published by credible media sources.

5. *Is the content of data which is to be stored sufficiently specified beforehand? Specified on a legal basis? Data applicants must worry on a substantial negative effect on their economic and personal reputation.*

   EC services are committed to upholding transparency and ensuring that the rights of data subjects are respected in accordance with Articles (15) to (24) of Regulation (EU) 2018/1725. The processing of personal data within ARACHNE is carried out in compliance with these articles, as explicitly indicated in the Privacy Statement.

   In line with the obligations under Regulation (EU) 2018/1725, programme authorities utilizing ARACHNE are required to adhere to both national and European data protection regulations. Part of this adherence involves the obligation to inform beneficiaries about the specific categories of their data that are available in external databases and that will be processed for the purpose of identifying risk indicators. This crucial information is to be provided to beneficiaries in a clear and transparent manner, which can be effectively achieved by incorporating data protection clauses into the grant/contract application documents. These clauses are designed to inform beneficiaries in advance of the types of data being processed, thereby fulfilling the requirement to provide detailed information on data categories to the data subject.

   Beneficiaries, contractors and suppliers can expect the proposed processing and its outcomes,

when they apply for funding and based on the widely publicised Commission approach of zero tolerance for fraud.

The derived risk-scoring indicators identify a risk of irregularity or of undue concentration of funds / conflict of interest, but do not confirm irregularities. These derived risk-scoring indicators do not result in automatic decisions by the programme administration. Instead, the staff of the programme authorities will further assess the identified risks, perform all controls for legality and regularity of the expenditure before drawing any conclusions, and take these into account for their internal anti-fraud strategy and control procedures.

Such conclusions may indicate potential fraud, prompting the responsible official to forward the case to the appropriate authorities specializing in fraud investigation. Alternatively, the findings might suggest an irregularity that necessitates additional verification by the official overseeing the grant. This additional verification could involve a detailed review process with the beneficiary in question to address and resolve the issues highlighted by the risk indicators. The extent and nature of this review process are determined by the severity of the suspected risk and the predefined priorities of ARACHNE users when dealing with identified risks.

6. *Would you please be so kind to explain the notion of ARACHNE in view of datamining and the rights of parties concerned in view of the collecting and processing of their personal data?*

As illustrated during the live presentation to the German authorities on 14/09/2022, ARACHNE produces a series of pre-defined risk indicators divided in several risk categories to provide an objective view on the riskiness of projects and the related entities (i.e. beneficiaries, (sub)contracts, contractors/suppliers): procurement process, contract management, funding eligibility, project performance, funded projects concentration, basic logicality/reasonability of project data, reputational and fraud alerts. These risk checks result in risk indicators on projects and contracts.

The risk checks are generated processing data from the Member States authorities and agencies, data from external public data sources and from commercial providers.

As referred above, the derived risk scoring indicators identifying possible irregularities will be taken into account by the officials in the programme authorities for their internal anti-fraud strategy and will be verified under their control procedures before drawing any conclusions. The derived risk scoring indicators are not automatic decisions and require the professional assessment of the officials in charge. The results of the risk calculation are internal data used for the purpose of management verifications and audits and are therefore subject to data protection conditions: they are not meant to be and should not be published (neither by the Commission services nor by the programme Authorities).

The legal requirement to ensure availability of data on operations supported by Union funds is available in the Regulations for each period, e.g., in Article 69 and annex XVII of Regulation (EU) 2021/1060 for the period 2021-2027. In case the data subject requests a change to his/her data, he/she should in first instance request the Member State's authorities to implement these changes. Subsequently, the information will be processed by the Commission and the changes will be considered in the risk scoring exercise. Anyhow, in case of change of project data, the Member States can themselves resend this data through the specific ARACHNE functionality (neither the Member States nor the Commission can alter the risk score or other imported data directly in ARACHNE).

The data used for enrichment of the programme implementation information received from the Member States is based on the published annual accounts of beneficiaries and (sub-) contractors.

In case of data change requests, the data subject should submit changes to the organisations (national) responsible for the collection of annual accounts and similar. This information is updated in the ARACHNE database by the external contractor on a quarterly basis and the Commission's risk score will take this into account in the next risk -score. Also here, neither the Member State nor the Commission can alter the risk score or other imported data directly in ARACHNE. Data subject could also contact the Member States' programme authorities to have their publicly available data to be rectified.

ARACHNE contains a functionality called "Feedback loop" made available to data users to correct wrong data mapping between the data sourced by the Member States and the external bases. The requestor must provide sufficient supporting documentation to enable the Commission ARACHNE team to review the reported error or inconsistency. After review, and before resolving the incorrect matching, the Commission ARACHNE team transfers the proposed modification to an authorised person at the European Commission for approval. The modifications thus introduced by the "feedback loop" will be considered by the system ARACHNE and will impact the processing of the concerned personal data for subsequent risk scoring and indicators.

During the assignment of data subject rights to the tool by the Commission ARACHNE team or by the dedicated team in the programme authorities, an ID document, additional information, or an address may be requested to precisely identify the requester. The personal information received shall only be used to identify the data subject on the ARACHNE system and to send back the reply, whereas no other use is allowed. Personal data related to a request to have rights granted, will be kept in the Commission Document Management system, and will be deleted at the end of its administrative purpose (no historical archiving). The ID document will be removed before registering the request for compliance with Regulation 2018/1725 in term of retention period minimisation, and it will be kept only for the time necessary to identify the data subject and to send the reply.

Right to compensation and liability

1. *Do national authorities bear the risk in view of the right to compensation and liability in case of material or non-material damage resulting from the use of ARACHNE according to Art. 82 of the Data Protection Regulation (Reg. (EU) 2016/67)?*

The Commission is bound by Article 65 of Regulation 1725/2018, which indicates the liability in case of material or non-material damage resulting from breach of this regulation when processing of personal data.

2. *List of operations/additional consent by beneficiaries: Beneficiaries are already asked to give their consent to the publication of data in accordance with Art. 49(3) CPR) (list of operations). Does the data on operations required in ARACHNE exceed the data listed in Art. 49(3) lit) a to n and, if so, is, in the Commission's view, an additional consent by beneficiaries for processing data in ARACHNE necessary?*

The list of data that the Managing Authorities shall make publicly available on the website in accordance with Article 49.3[2] of the CPR is similar to a large part of data used in ARACHNE but is

[2] *Art. 49.32 of the CPR states that "… The managing authority shall make the list of operations selected for support by the Funds publicly available on the website in at least one of the official languages of the institutions of the Union and shall update that list at least every 4 months. Each operation shall have a unique code.*

not collected for the same purpose (publicity under 49.3, verifications and controls under ARACHNE in line with Article 69 CPR). Data used in ARACHNE is precisely indicated in the ARACHNE privacy statement available in the related homepage. In fact, Article 49.3 of the CPR is applicable to Managing Authorities while the ARACHNE privacy statement and data protection clauses in the grant/contract application documents (upon decision of the Member States) is applicable to data subjects. The collection of data for ARACHNE is based on information that programme authorities need to collect under Article 69 of the CPR and is processed under Regulation (EU) 2018/1725, notably Art. 5(1)(a) (*Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Union institution or body*) and Art. 5(1)(b) (*Processing is necessary for compliance with a legal obligation to which the controller is subject)*.

3. *Risk-based use of ARACHNE: Is it possible to use the tool for a subset of operations which are associated with a certain level of risk assessed on the basis of indicators such as the level of financial support?*

   Different filter possibilities are offered in the dashboards to select a subset of operations or to operations where specific risk indicator(s) are raising some alerts. This means that is it possible to select for instance only the operations for a specific beneficiary where a potential financial risk is identified or where a potential conflict of interest is detected. Filters can be set on different data attributes of the operation (name, beneficiary, amount, status, start and end date, etc ...), on the different risk category scoring and on all individual risk indicators. Users can also set their own criteria to deal with risk indicators only for specific operations, for example based on a criterion of the financial support allocated.

4. *Alternative Options: Which other systems or mechanisms available on the market would have the same added-value as ARACHNE with regard to the provisions in Art. 325 TFEU?*

   As far as the Commission services know, no single Member State has expressed that they have a similar tool in place at national level to allow seeking information on beneficiaries across Europe. The Commission has not looked for other systems or mechanisms that would be available on the market since it has designed and developed a dedicated tool that is designed specifically for the programmes' needs.

5. *Furthermore, we would like to raise the questions how Commission will proceed with the questions and need for action raised by the EDPS in the context of the amendments proposed for the Financial Regulations?*

   In its Opinion 14/2022 dated 7 July 2022, the EDPS provided the European Commission with eight recommendations with regard to the IT data-mining tool mentioned in the text of the Financial Regulation recast. Many elements of the above-mentioned EDPS recommendations had already been addressed in this updated DPIA and are also reflected in the record and/or privacy statement of ARACHNE (DPR-EC-00598.3) within the public Register of the Data protection officer. The rest were addressed and are reflected in the final text of the Financial regulation recast.

6. *The Arachne charter is quite general. Is there any more detailed policy or other document that provides a clearer picture of the requirements the Commission imposes on the authorities' use of the system?*

   The Commission refrains from mandating or imposing specific national-level policies or guidelines on how ESIF programme authorities, RRF coordinating and implementing bodies, and CAP paying agencies (hereon referred to as 'bodies/authorities') should use Arachne. Instead, these

bodies/authorities are granted autonomy to determine their own approach in incorporating the system's findings into their existing procedures.

Essentially, the Commission offers a tool to identify potential issues but does not oversee how bodies/authorities address or resolve these concerns. It is the responsibility of the bodies/authorities to decide how to manage the information provided by Arachne and integrate it into their operational processes.

This approach allows for flexibility and autonomy, recognizing that different authorities may have varying procedures for handling such matters. By refraining from imposing specific methodologies, the Commission acknowledges diversity and permits adaptation of Arachne's results to individual circumstances.

As part of support activities, the Commission aids bodies/authorities upon request, aiding in the adaptation of their existing procedures to maximize the benefits of Arachne and align them with established workflows.

Arachne serves to alert bodies/authorities to high-risk projects, contracts, contractors, and beneficiaries, aiding in the concentration of administrative efforts for verifications. Should bodies/authorities fail to act, the Commission services can only encourage their use of Arachne and verify the implementation of other proportionate and effective anti-fraud measures.

It is pertinent to note that Commission service auditors have access to Arachne's risk calculations and will evaluate, as part of system audits, whether the arrangements proposed by the bodies/authorities are expected to prevent, detect and correct corruption, fraud and conflicts of interests and to ensure an effective monitoring, in accordance with Article 19(3) of Regulation (EU) 2021/241.

7. *What legal status does the Arachne charter have, and what requirement does it impose regarding not disclosing data from Arachne?*

By using Arachne, bodies/authorities implicitly commit to adhering to the principles outlined in the charter. Either party retains the right to unilaterally terminate this charter. Furthermore, under specific circumstances, the Commission services reserve the authority to withdraw access to Arachne. Consequently, bodies/authorities using Arachne implicitly consent to the terms of the charter.

The charter delineates precise requirements concerning the confidentiality and non-disclosure of data sourced from Arachne, explicitly prohibiting bodies/authorities from disseminating or disclosing such data without appropriate authorization. Failure to uphold these obligations may lead to the revocation of access to the platform.

8. Is there a prohibition on disseminating information originating from Arachne? If affirmative, what are the specifics of such prohibition, delineating the circumstances and nature of the data subject to this restriction? If so, how is it formally regulated, articulated, and what is the Commission's perspective on its implications?

The results of the risk calculation constitute internal data used for the purpose of the protection of the financial interests of the EU and for management verifications. Therefore, they are subject to stringent data protection conditions and should not be published, either by the Commission services or by bodies/authorities.

The Commission services ensure transparency by adhering to the conditions regarding information provision and data subject rights outlined in Articles 15 to 24 of Regulation (EU) 2018/1725. The privacy statement published on the Arachne homepage confirms the compliance of data processing activities in Arachne with the aforementioned articles. Data subjects are informed about their rights and the process to exercise them through a privacy statement published on the ARACHNE website, which is publicly available: https://ec.europa.eu/social/BlobServlet?docId=25704&langId=en

- The safeguards have undergone assessment and approval in the DPIA, specifically in section "2.1.6 Purpose limitation", stating that.

✓ The purposes for data processing have been clearly identified and documented.

✓ The details of the purposes of processing have been sufficiently referenced to in the Privacy statement.

✓ The processing is regularly reviewed, and where necessary the documentation and the Privacy statement is updated.

✓ If personal data is intended to be used for a new purpose, it is ensured that this is compatible with the original purpose or specific consent is taken for the new purpose, in accordance with the principle of purpose limitation under the GDPR/EUDPR. If the new processing activity is not compatible, specific consent from the data subject must be obtained before proceeding.

It is important to highlight that any party, subject to the GDPR, is obligated to comply with the general data protection rules. In practical terms, this means that data from Arachne must only be processed for the purpose for which it was collected. Should there be a need to use this data for another purpose, the controller intending to process it has the responsibility to ensure lawful processing in line with the GDPR/EUDPR. The controller must carefully assess the legal basis for such processing, which may include seeking explicit consent from the data subject or ensuring that the new purpose is legally compatible with the original one. This approach reinforces the overall commitment to data protection and upholds the trust of data subjects in the handling of their personal data.

9. *Are there any user restrictions for an authority using the system, and how are they regulated? For example, concerning the purpose of processing or the types of data the agency is allowed to process.*

Arachne offers granular access to different categories of data recipients and implements robust access control measures. Only a limited number of users designated by bodies/authorities have the ability to upload data into the system, while others have restricted read access. Additionally, certain users have restricted write access for cases within the context of case management workflows. Bodies/authorities are granted access solely to the data pertaining to their operations. Access to the system is facilitated through the Commission EU Login personal username and password, linked to an Arachne account, and requires the use of a 2-factor authentication method. New users must create an EU Login account to access Arachne. EU Login is used for authentication, while Arachne accounts provide access to specific programmes/plans and features.
Arachne provides detailed access control measures tailored to different user roles and responsibilities.

10. *What other security measures are in place, and how are they regulated?*

An IT Security Plan (SP) has been drafted following a risk assessment based on the IT Security Risk Management (ITSRM) Methodology and based on ITSRM SP template proposed by DIGIT. This ITSRM Methodology follows the recommendations emphasized in the Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 [CD2017/46]. The security plan contains a complete IT security Risk assessment. A description of the identified risks, the implemented security measure

and an IT security implementation plan was performed according the ITSRM Methodology and related standards and was approved by the ARACHNE Steering committee in July 2021. Security measures put in place include access permissions; physical security measures; ensuring the security of IT channels; encryption of personal data; review of security measures; data breach handling mechanisms and maintenance of software.

All data uploaded by bodies/authorities are encrypted, secured, and transferred to the Commission services for processing. No data is transmitted outside the Commission's premises, and service providers do not have access to the uploaded data. The entire data processing process, including data validation, enrichment, and risk calculation, occurs within the Commission's premises.

The accuracy principle is maintained through data verification during collection and regular verification to ensure data accuracy. Arachne's processing of personal data adheres to fundamental principles such as data minimization, storage limitation, and additional technical safeguards like encryption during data transfer and storage. These measures ensure personal data protection by design.

Furthermore, the principles of proportionality, necessity, and integrity were evaluated in the DPIA and validated by the Commission's Data Protection Officer on July 22, 2022.

11. *What information can be obtained merely by accessing the system, and what information is exclusively available through specific searches? For instance, are there any screenshots from the system that could illustrate this?*

Data search outcomes in Arachne vary depending on the specific information sought. Arachne aggregates data from four sources (Member States, Orbis, WorldCompliance and VIES – see details below), and accessibility depends on the nature of the source data.
The information used in Arachne is sourced from bodies/authorities and official channels, including publicly available information and data from the VIES system, as well as external databases such as Orbis and World Compliance. Risk indicators are derived from predefined mathematical formulas using all available data.

For instance, legal affiliations and connections between entities are available through the Orbis database. This includes group structures of companies, which can be accessed by all users, even if the entities are not directly involved in projects.

Example:
Arachne uses Orbis data to identify legal affiliations between entities involved in projects, along with their managers, owners, and associated individuals. This information is used in calculating risk indicators like 'Links between beneficiaries and contractors'. However, detailed indicator scores and information used for calculations are only accessible to users with specific access rights for the relevant projects.
In the risk analysis for Arachne, which is available to the Data Protection Officer (DPO), it is stated that authorities will be granted access to personal data on a "need to know" basis through a "role-based approach." Could the Commission elaborate on what this entails, for example, regarding permissible searches in the system and how it is regulated? Do case handlers have their own control and access to the data, or are they provided upon request? Does your response apply to all data or does it vary depending on the category of data?

Personal data is accessed on a need-to-know basis which means that users have restricted access to specific data, depending on the users' access rights and on the source of the data.

The names of individuals (and associated birthdates) are retrieved form 3 different sources:

- Operational data from bodies/authorities: names + birthdates of related people of a project or key experts of a contract. If birthdates are provided by the bodies/authorities, these dates are only used for matching[1]* purposes. This to reduce the number of 'false positive' matchings* (avoid matching* with people having the same name but with different birthdate).
- Orbis: Names, birthdates, active and inactive roles of official representatives (Board of directors / Owners / partners / managers) of the companies.
- World Compliance: Names, birthdates, other personal data of individuals appearing on the PEP lists, Sanction and enforcement list and in Adverse Media. The World Compliance database data is provided to the Arachne user for information, only if a matching* occurs and can be retrieved by the Arachne user who has access to the project or contract data via the details of the risk indicators.

12. *Concerning flagged items and other outcomes of the risk analysis, could the Commission provide clarification on the extent to which authorities have access to the underlying data that serves as the basis for these flags?*

All the data used for the calculation of each risk indicator, as well as the indicator definition, is available in pop-up windows which are available by clicking on the risk indicator score. Authorities have access to the underlying data that serves as the basis for the flags in ARACHNE to varying extents, depending on the source of the data and the user's access rights:
- Operational data from Member States: Authorities have access to project data, contract data, expenses, and entities involved in these projects (beneficiaries, project partners, contractors, subcontractors, service providers, consortium members), as well as people involved in these projects (related people and key experts), including beneficial owners. This access is limited to the projects associated with the programmes/plans the user is associated with.

- Orbis: Authorities have full access to comprehensive economic information on companies, their financial statements, and official representatives (Board of directors/ Owners/ partners/ managers) of the companies.

- WorldCompliance: Access to data from WorldCompliance, such as PEP lists, sanction lists, enforcement lists, and adverse media, is available through risk indicators. This means that data from WorldCompliance is accessible only for projects uploaded to ARACHNE, provided the user has access rights.

- VIES: Access to VAT numbers for companies from the VIES system is available through risk indicators, meaning data from VIES is accessible only for projects uploaded to ARACHNE.

The risk indicators themselves, which are derived from predefined mathematical formulas using all available data, are accessible only for projects uploaded to ARACHNE and only to users with the appropriate access rights for the relevant projects.