EDPB Documents

Report on the use of SPE external experts

16 April 2024

Contents

INTRODUCTION

The Support Pool of Experts (SPE) is a pilot project established under pillar 2 of the EDPB 2021-2023 strategy (supporting effective enforcement and efficient cooperation between national supervisory authorities)[1].

The SPE provides support in the form of expertise for investigations and enforcement activities of common interest to supervisory authorities ("**SAs**") and enhances cooperation/solidarity by reinforcing and complementing the strengths of the individual SAs and addressing operational needs.

This report focuses on the main initiatives conducted as part of the Support Pool of Experts since it started.

Since the beginning of the SPE program, thirteen projects have been launched, among which nine are finished. The SPE projects that are ongoing and not yet fully finalised are not included in this report.

In addition, the report recalls the applicable procedure for the call for expression of interest and the procedure to launch a project with an external expert.

This report does not cover other enforcement cooperation related initiatives, although some of them may fall in the scope of the SPE such as collaboration on strategic cases, CEF actions, investigation priorities, or the EDPB secondment programme.

[1] Its Terms of Reference (https://edpb.europa.eu/sites/default/files/files/file1/edpb_document_supportpoolofexpertstor_en.pdf) were adopted by the EDPB plenary in December 2020 and the project plan was adopted in December 2021.

1. THE NETWORK OF SPE CONTACT POINTS WITHIN SAS

In order to coordinate the work of the SPE, a list of SPE contact points was set up at the end of 2021. The group have met regularly since then. It is coordinated by the EDPB Secretariat and includes participants from SAs.

Among others, the SPE contact points:

- follow all information on SPE activities,
- discuss and propose ongoing and future SPE projects, in particular they identify specific needs in enforcement cases that will require SAs' experts or external experts support,
- identify SAs operational needs for national investigations with respect to the SPE,
- share enforcement experiences and good practices between SAs,
- analyse provided enforcement documentation/solutions,
- disseminate information within the respective SAs,
- develop common methodologies regarding IT knowledge and more specific legal issues and encourage the creation of new methodologies harmonising approaches on inspections and enforcement.

2. THE SPE CALL FOR EXPRESSION OF INTEREST AND CONTRACT PREPARATION

Following a call for expressions of interest "***Establishment of a List of Individual Experts for the implementation of the EDPB's Support Pool of Experts***" in February 2022[2], a reserve list of external experts was set up. The SPE consists of qualified experts in areas such as IT auditing, website security, mobile OS and apps, IoT, cloud-computing, behavioural advertising, anonymization techniques, cryptology, AI, UX design, Fintech, Data science, digital law, etc. They may assist SAs on different stages of their investigation and enforcement activities in the field of data protection.

An electronic application procedure[3] was designed, in compliance with the EUDPR[4].

Candidates are invited to apply in one or two fields of expertise: ***Legal expertise in new technologies*** and/or ***Technical expertise in new technologies and information security***. Each of the two fields is divided into sub-fields of expertise (see annex I of the call for expressions of interest), covering the topics on which EDPB may need external expertise.

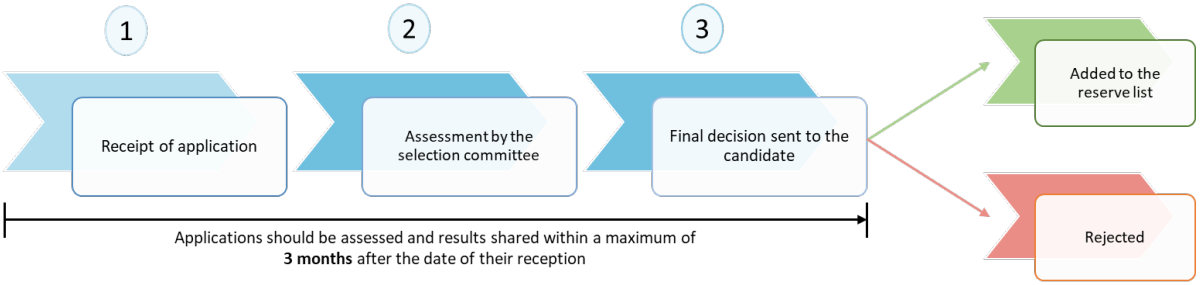
The list of experts ("reserve list") compiled as a result of this procedure was valid for two years from the dispatch of the notice, i.e. until the beginning of 2024. The validity of the call for expressions of interest and the list of experts has been extended in 2023 for two years. **It is now valid until 10 February 2026**.

Interested parties can apply at any time prior to the last three months of validity of the list. Following the extension of the validity of the list of experts, applications will be possible until 10 November 2025.

At the end of 2023, 504 experts are present on the reserve list. During this period, the Secretariat received 702 applications from potential external experts. Once candidates had expressed their

[2] https://edpb.europa.eu/system/files/2022-02/call_for_expressions_of_interest_support_pool_of_experts.pdf
[3] https://ec.europa.eu/eusurvey/runner/PoolOfExperts
[4] https://edpb.europa.eu/system/files/2022-02/SPS_Support%20Pool%20of%20Experts_external_final_0.pdf

interest online, the selection procedure was implemented in accordance with applicable procurement rules:



The Call for Expression of Interest of the Support Pool of Experts in figures:

	2022 - 2023
Applications received	702
Selection committee's meetings	8
Candidates added to the reserve list	504 (72%)
Split of the reserve list by confirmed field(s) of expertise:	
Legal expertise	355 (70%)
Technical expertise	129 (26%)
Technical & legal expertise	20 (4%)

The reserve list can then be used to propose a specific project to a candidate, depending on the EDPB's needs and whether a specific profile matches these needs:

- When a project is planned, Terms of Reference are drafted. They describe the specific work to be done, the requirements to be taken into account (especially regarding languages) and the deliverables to be prepared. This proposal is commented by the SAs participating in the SPE initiative and validated by a panel including the Chair and Deputy Chairs.

- Based on those Terms of Reference, the most qualified experts are selected for the project (in full respect of the principles of non-discrimination, equal treatment and absence of conflict of interest) according to "8.1.2 Criteria for the selection of individual experts" and "8.4.3 Convocation" of the Call for expression of interest.

- Starting with the most qualified, selected experts are contacted to enquire about their availability and willingness to participate in the project. If all parties agree then a contract is signed, if not the next most qualified expert is contacted.

3. ENHANCING TRANSPARENCY OF SPE PROJECTS

The EDPB website includes a section dedicated to the Support Pool of Experts, in particular to explain the objective and applicable procedure but also to respond to experts' questions[5]. It has been updated to take into account the questions received since the start of the SPE.

Since the beginning of the SPE program, thirteen projects have been launched, among which nine are finished. These projects are managed (individually or jointly) by a lead SA, Expert Subgroup or

[5] Available at https://www.edpb.europa.eu/support-pool-experts-spe-programme_en

Taskforce, or by the EDPB Secretariat. Depending on the concerned project, the entity having the leading role may be more or less involved in the drafting of the deliverable(s). In some projects, this entity may provide significant input and feedback regarding the deliverable(s).

The EDPB already published the results of several projects:

- One-Stop-Shop thematic case digest - Right to object and right to erasure by Prof. Alessandro MANTELERO (see section 4.1)
- One-Stop-Shop thematic case digest - Security of Processing and Data Breach Notification by Prof. Eleni KOSTA (see section 4.2)
- EDPB Website Auditing Tool by Dr. Jérôme GORIN (see section 4.3)
- AI Auditing by Dr. Gemma GALDON CLAVELL (see section 4.4)
- Standardized Messenger Audits by Pr. Mathieu CUNCHE (see section 4.5)
- DPO training[6] by Dr. Tihomir KATULIC (see section 4.6)
- AI risks - Optical Character Recognition (OCR) & Name Entity Recognition (NER) by Isabel BARBERA GARCIA (see section 4.7).

It is important to note that while the above deliverables are made publicly available on the EDPB's website, the views expressed in these documents are only those of their authors (i.e. the SPE experts) and do not reflect the official position of the EDPB. The EDPB does not guarantee the accuracy of the information included in these documents. Neither the EDPB nor any person acting on the EDPB's behalf may be held responsible for any use which may be made of the information contained in these deliverables. Some excerpts may be redacted from these deliverables as their publication would undermine the protection of legitimate interests, including, inter alia, the privacy and integrity of an individual regarding the protection of personal data in accordance with Regulation (EU) 2018/1725 and/or the commercial interests of a natural or legal person.

A specific disclaimer is included in each of the deliverables made public.

The deliverables of two additional projects will remain only accessible to EDPB members for the moment. The first one relates to an authority's audit lab. The second one was a project carried out with the aim of fostering the development of certifications as a tool for transfers of personal data by complementing the list of certification criteria specific to transfers set out in the EDPB Guidelines 07/2022 on certification as a tool for transfers, with concrete examples (and where relevant counter-examples) for each criterion.

Finally, the SPE program was used by one national SA to obtain support from an external expert in the context of an enforcement action. The details of this case, including the deliverable, are confidential (i.e. only accessible to the requesting SA).

[6] Partial publication, the questions and answers of the exams won't be communicated.

4. FINALIZED AND PUBLISHED SPE PROJECTS

4.1. OSS case digest on the right to object and to erasure

by Prof. Alessandro MANTELERO

- OSS Case digest available on the EDPB website: erasure https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/one-stop-shop-case-digest-right-object_en
- Summaries of decisions in the process of being published in the OSS EDPB register in 2024

The EDPB has created a Register of one-stop-shop (OSS) decisions (i.e. Art. 60 GDPR), which is publicly available on its website[7], and currently populated with the text of OSS decisions and, in some cases, with a summary thereof. To render information on final decisions taken in one-stop-cases more readily available, and more accessible to all the Members of the EDPB and practitioners (e.g. lawyers, data protection officers), the EDPB launched the "One-Stop-Shop case digests".

Such case digests complement the Register of OSS decisions by
1. selecting and presenting the most important decisions on a given theme; and
2. providing an overview and aggregate results of relevant decisions on this theme.

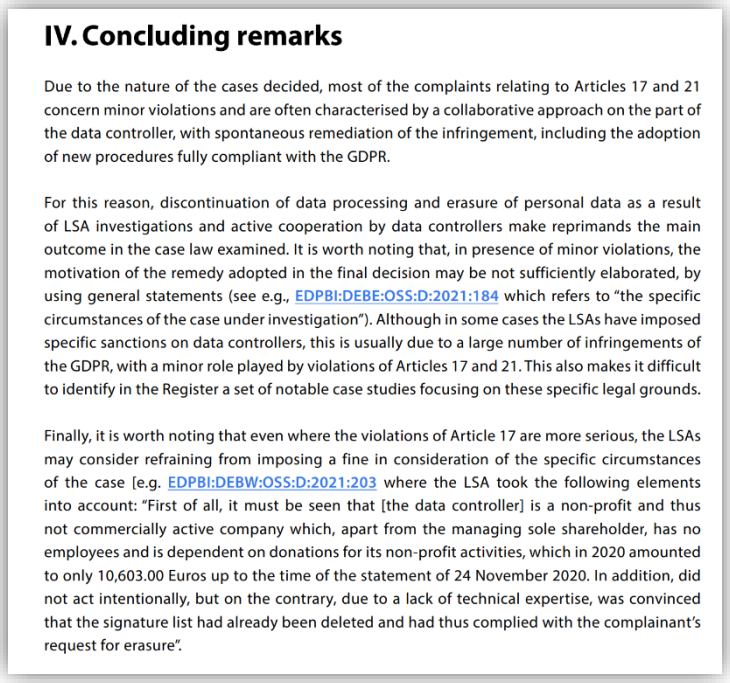
The first OSS case digest on "right to object and right to erasure" **was produced in 2022** by an external legal expert, Prof. Alessandro MANTELERO, and **published** on the EDPB website **in February 2023**. Extracts of this case digest were also included in the EDPB annual report for 2022[8].

This document provided an analysis of **170 decisions relating to Articles 17 and 21 GDPR**, adopted by SAs pursuant to Article 60 GDPR (One Stop Shop Decisions). SAs cooperate a lot on the exercise of the right to object and the right to erasure and they reach consensus through the OSS decisions. Therefore, this case digest analysed the conclusion of SAs in these OSS decisions and gave some takeaways for these decisions. More specifically, this case digest offered insights on the interpretation and application of the above GDPR provisions by DPAs in many diverse scenarios, e.g. the right to object to direct marketing or when an individual wishes to erase their account or profile data online.

For example, this case digest analysed how SAs assessed the internal processes put in place by data controllers to handle requests from individuals exercising their rights to object or right to erasure. In particular, SAs assessed whether these processes were compliant with GDPR requirements or not. The report underlined, regarding decisions on Article 17 GDPR, that the most serious procedural shortcomings concerned the absence of a specific procedure to deal with erasure requests, while the most frequent case concerns delays in the erasure process due to poor internal organization or technical malfunction. Regarding Article 21 GDPR, the report showed that most cases reveal deficiencies in the internal procedure adopted to deal with data subjects' requests (accuracy of the procedure, internal communication, timeframe for processing requests, etc.). The case digest also analysed the types of corrective measures issued by DPAs, the most common one being a reprimand.

[7] https://www.edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en
[8] EDPB Annual Report for 2022, section 6.1.3.1, available at https://www.edpb.europa.eu/system/files/2023-04/edpb_annual_report_2022_en.pdf

The case digest targeted two types of audience, namely SAs and their case handlers, but also organisations themselves.



IV. Concluding remarks

Due to the nature of the cases decided, most of the complaints relating to Articles 17 and 21 concern minor violations and are often characterised by a collaborative approach on the part of the data controller, with spontaneous remediation of the infringement, including the adoption of new procedures fully compliant with the GDPR.

For this reason, discontinuation of data processing and erasure of personal data as a result of LSA investigations and active cooperation by data controllers make reprimands the main outcome in the case law examined. It is worth noting that, in presence of minor violations, the motivation of the remedy adopted in the final decision may be not sufficiently elaborated, by using general statements (see e.g., EDPBI:DEBE:OSS:D:2021:184 which refers to "the specific circumstances of the case under investigation"). Although in some cases the LSAs have imposed specific sanctions on data controllers, this is usually due to a large number of infringements of the GDPR, with a minor role played by violations of Articles 17 and 21. This also makes it difficult to identify in the Register a set of notable case studies focusing on these specific legal grounds.

Finally, it is worth noting that even where the violations of Article 17 are more serious, the LSAs may consider refraining from imposing a fine in consideration of the specific circumstances of the case [e.g. EDPBI:DEBW:OSS:D:2021:203 where the LSA took the following elements into account: "First of all, it must be seen that [the data controller] is a non-profit and thus not commercially active company which, apart from the managing sole shareholder, has no employees and is dependent on donations for its non-profit activities, which in 2020 amounted to only 10,603.00 Euros up to the time of the statement of 24 November 2020. In addition, did not act intentionally, but on the contrary, due to a lack of technical expertise, was convinced that the signature list had already been deleted and had thus complied with the complainant's request for erasure".

Lastly, the external expert also drafted summaries of 15 selected OSS decisions focusing on the points of law that are discussed in each case. Those summaries are in the process of being published in the public register of the EDPB website in 2024.

4.2. OSS case digest on security of processing and data breaches

by Prof. Eleni KOSTA

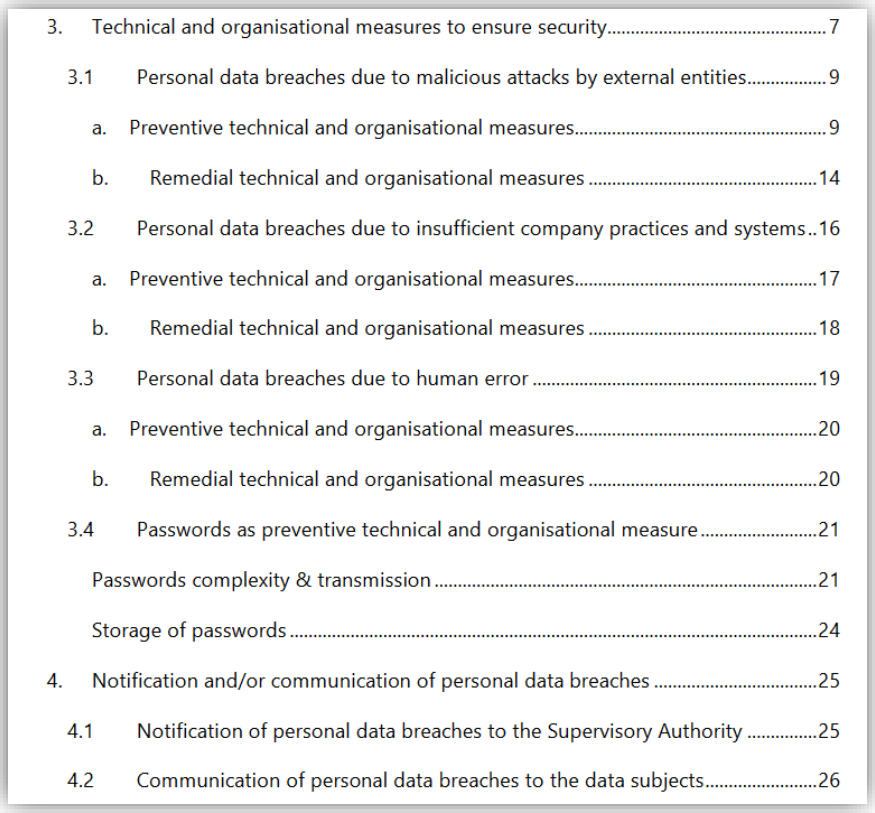
- OSS Case digest available on the EDPB website: https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/one-stop-shop-case-digest-security_en
- Summaries of decisions in the process of being published in the OSS EDPB register in 2024

A second OSS case digest was launched in 2022 on security and data breaches and completed at the end of November 2023.

An external legal expert, Prof. Eleni KOSTA, drafted a case digest based on 90 decisions for which supervisory authorities cooperated with one another under the one-stop-shop mechanism in the field of security of data processing and data breach notifications[9]. More specifically, these decisions relate to Articles 32 (security of processing), 33 (notification of a personal data breach to the supervisory

[9] The EDPB's public register with the one-stop-shop final decisions is available at https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-article-60-final-decisions_en. Annex 1 to the case digest lists the decisions relied upon and provides the link to the redacted decisions, which are available on the EDPB's public register.

authority) and 34 GDPR (communication of a personal data breach to the data subject). All of these decisions were adopted between January 2019 and June 2023. The case digest also refers to the available guidance at EU level, and in particular, EDPB Guidelines 9/2022 on personal data breach notification under GDPR and Guidelines 01/2021 on examples regarding personal data breach notification. Relevant cases before the Court of Justice of the EU, as well as decisions and guidance adopted at national level are mentioned, such as national guidance on the use of robust passwords and secure authentication channels.



SAs often applied Articles 32, 33 and 34 GDPR altogether in their decisions, given that the occurrence of a data breach is in most cases linked to the implementation of security measures. Many decisions relate to data breaches caused by malicious attacks, insufficient internal practices and IT systems or human error. As a result, the case digest offers insights on the interpretation and application of these GDPR provisions by SAs in all of these diverse scenarios.

More specifically, SAs carried out analyses of the technical and organisational measures implemented - both before the occurrence of a data breach (through preventive measures) and after such occurrence (through remedial or mitigating measures). Despite the fact that the SAs analysed the relevant security measures on a case-by-case basis taking into account the specifics of the affected data processing, conclusions can still be drawn regarding whether certain security measures are considered sufficient by SAs. For instance, several SAs examined the establishment of proper access control mechanisms based on the individual authentication to access specific data. Lack of such clear access control mechanisms led various SAs to find violations of Article 32 GDPR. Other decisions show similarities in the conclusions reached by SAs, for example regarding the storage and encryption of passwords, and the recording of logs.

This case digest analyses the findings of SAs in very diverse scenarios, such as in the event of ransomware, compromised hardware or accounts and accidental disclosures of personal data. It creates a rich pool of analyses of different security incidents, along with the corresponding security

measures that SAs found to be appropriate or not in the specific context. As a result, the case digest constitutes a useful tool for SAs and their case officers when assessing similar cases. The decisions mentioned also enable organisations to grasp which preventive security measures they may choose to implement when processing personal data and/or which remedial measures to adopt following a personal data breach. All the decisions referred to in the case digest are accessible via the EDPB's public register and the links to these decisions are included in the report.

Lastly, the external expert also drafted **summaries of 15 selected OSS decisions** focusing on the points of law that are discussed in each case. These summaries are in the process of being published in the public register of the EDPB website in 2024.

4.3. Website auditing tool

by Dr. Jérôme Gorin

- **Version 1.1.2** published as Free and Open Source Software under EUPL 1.2 Licence, available at https://code.europa.eu/edpb/website-auditing-tool

Several supervisory authorities already use tools or methodologies to inspect websites. However, those tools are either very limited or require advanced technical skills both to be used and to analyse the collected evidence.

In 2022, the EDPB launched a project to develop a user-friendly and documented tool for website inspections, building on the Website Evidence Collector[10] (WEC) with an external expert: Dr. Jérôme GORIN.

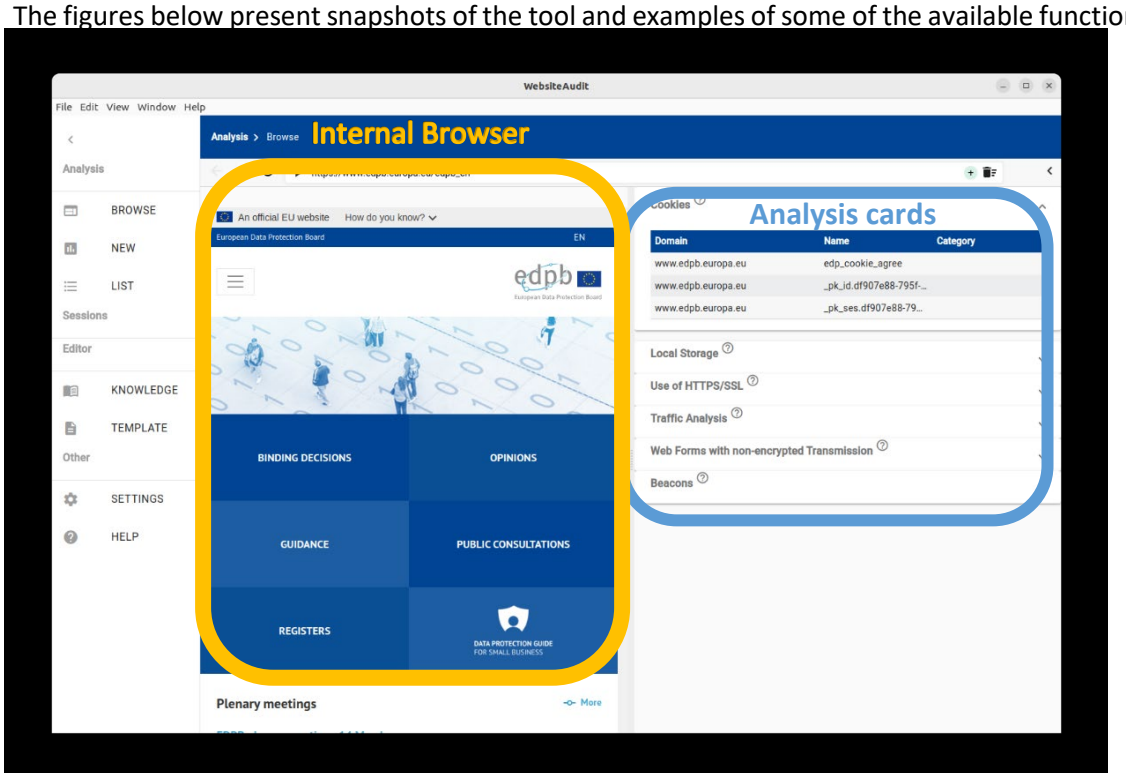
The EDPB website auditing tool makes it possible to collect evidence, classify data and generate reports regarding trackers that are being used by websites. It is packaged on Windows, MacOS and GNU/Linux (.deb) and offers a user friendly graphical interfaceIt integrates a browser that helps to assess at a glance whether or not a website collects or stores information in a browser in a compliant way (i.e.by informing and seeking user consent when this is required). It allows to build a knowledge database of qualification of cookies to simplify the prequalification of those already known while the final decision on compliance / non-compliance stays in the hand of the auditor on a case by case basis. All evidence and reports can be stored and shared with colleagues. Finally, it also allows to analyse results from audit made with the WEC.

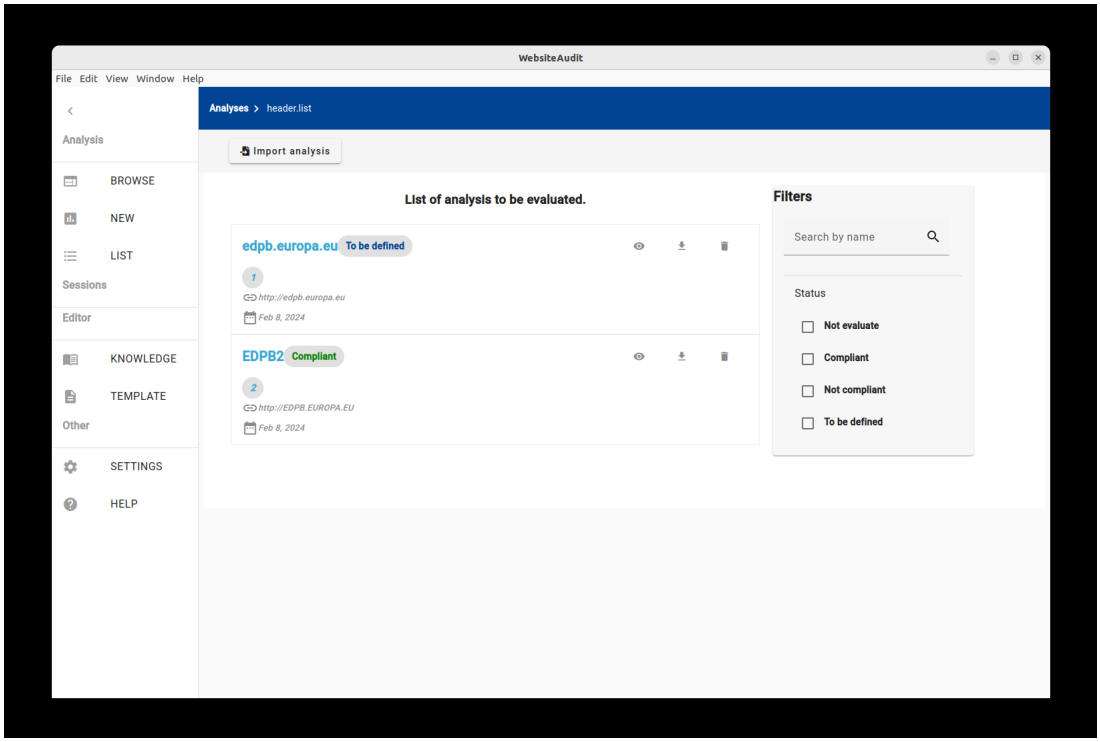
This tool (and its source code) was first made available to supervisory authorities. In particular, a presentation by the expert was then organized during an in-person bootcamp (please see Section 5.1, which touches upon this event).
Following the positive feedback of the EDPB members a new SPE project was launched in October 2023 to consolidate version 1 and develop new features in a version 2.

[10] Open source tool developed by EDPS: https://edps.europa.eu/node/5452_de

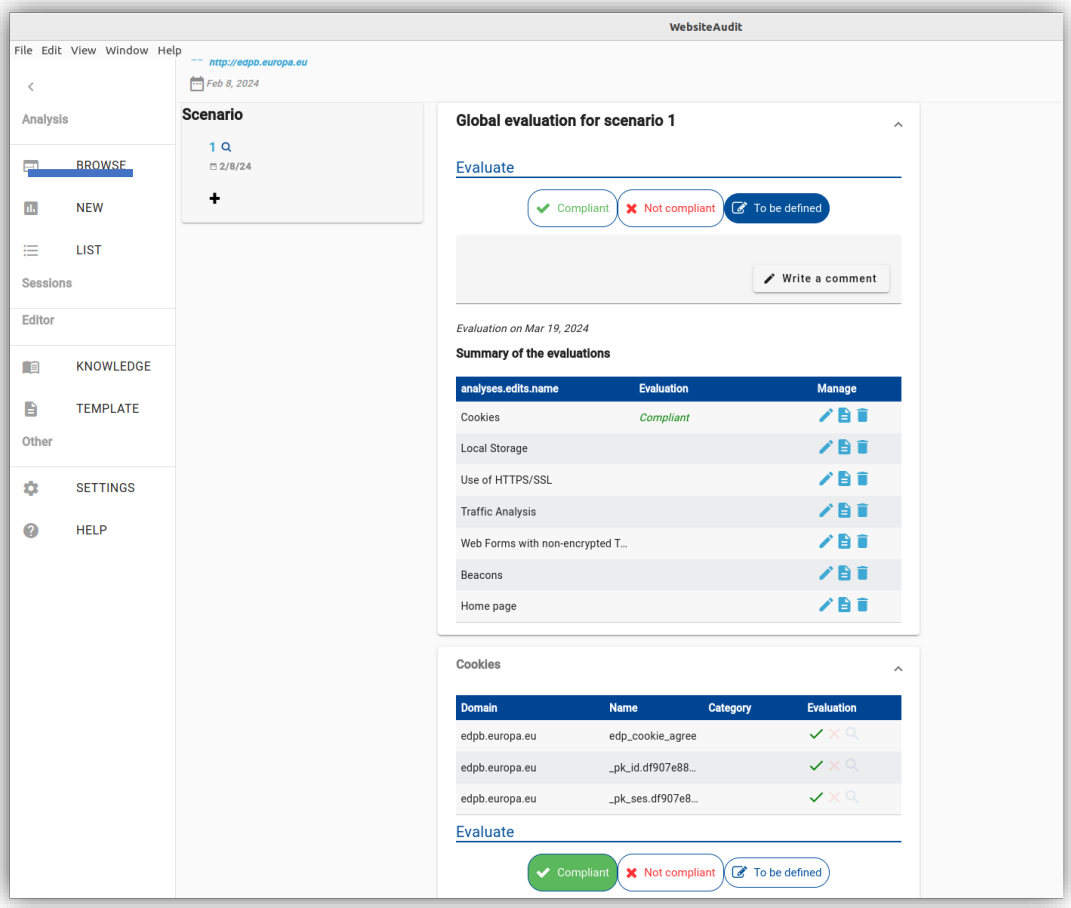
The consolidated version has been released and made public on 29 January 2024 (under EUPL 1.2+) on: https://code.europa.eu/edpb/website-auditing-tool[11].

The figures below present snapshots of the tool and examples of some of the available functionalities:





[11] News item "EDPB launches website auditing tool", available at https://www.edpb.europa.eu/news/news/2024/edpb-launches-website-auditing-tool_en



4.4. AI auditing

by Dr. Gemma GALDON

- Project available at: https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/ai-auditing_en

This project was proposed by the ES SA. With the upcoming legislation regarding data issues (in particular the AI Act), this **project aimed to map, develop and pilot practical GDPR tools in the field of AI**. **The objective was to help all parties understand and assess data protection safeguards in the context of the AI regulation in practice and in particular to help the ES SA to incorporate tools to inspect AI systems and define methods that can be required of third parties to comply with.**

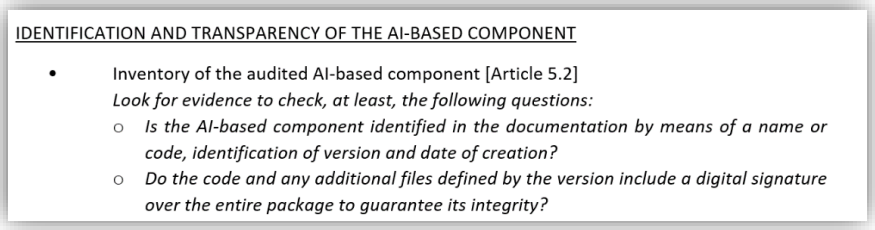
This project was completed in **February 2023** by the external expert Dr. Gemma Galdon and resulted in three deliverables:

- **Checklist for AI auditing.**

Methodologies and approaches were compared to produce a qualified assessment of the possibilities and shortcomings of algorithmic audits to identify and tackle data protection issues (including profiling, human intervention, etc.), as well as an algorithmic audit methodology (facilitating

inspections by supervisory authorities and contributing to the protection of rights, accountability and redress).

This first document proposes practical elements, like model cards and practical questions an auditor is advised to ask during an investigation.



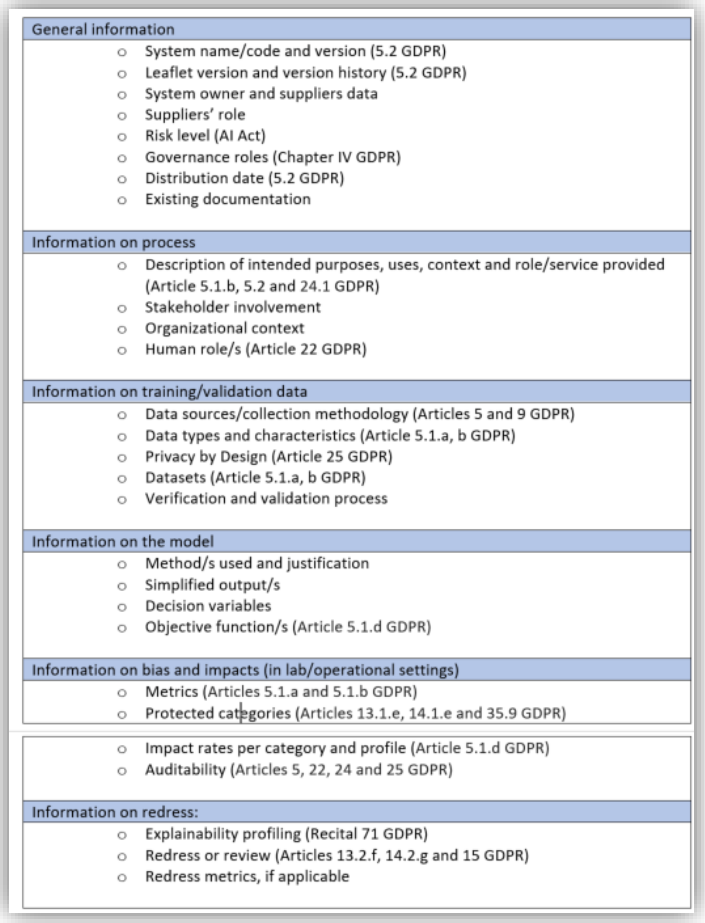
IDENTIFICATION AND TRANSPARENCY OF THE AI-BASED COMPONENT

- Inventory of the audited AI-based component [Article 5.2]
  Look for evidence to check, at least, the following questions:
  - *Is the AI-based component identified in the documentation by means of a name or code, identification of version and date of creation?*
  - *Do the code and any additional files defined by the version include a digital signature over the entire package to guarantee its integrity?*

The questions are organized around a practical objective for each step, as illustrated below:

- **Proposal for algorithmic leaflets.**

A concept "exported" from the medical domain, the Government of Spain recently proposed the first instance of these documents as a set of guidelines for algorithmic transparency in labor-related technologies.[12] This approach was applied to AI systems processing personal data.
The proposal is to build, for each algorithm a leaflet based on the following:



General information
○ System name/code and version (5.2 GDPR) ○ Leaflet version and version history (5.2 GDPR) ○ System owner and suppliers data ○ Suppliers' role ○ Risk level (AI Act) ○ Governance roles (Chapter IV GDPR) ○ Distribution date (5.2 GDPR) ○ Existing documentation
Information on process
○ Description of intended purposes, uses, context and role/service provided (Article 5.1.b, 5.2 and 24.1 GDPR) ○ Stakeholder involvement ○ Organizational context ○ Human role/s (Article 22 GDPR)
Information on training/validation data
○ Data sources/collection methodology (Articles 5 and 9 GDPR) ○ Data types and characteristics (Article 5.1.a, b GDPR) ○ Privacy by Design (Article 25 GDPR) ○ Datasets (Article 5.1.a, b GDPR) ○ Verification and validation process
Information on the model
○ Method/s used and justification ○ Simplified output/s ○ Decision variables ○ Objective function/s (Article 5.1.d GDPR)
Information on bias and impacts (in lab/operational settings)
○ Metrics (Articles 5.1.a and 5.1.b GDPR) ○ Protected categories (Articles 13.1.e, 14.1.e and 35.9 GDPR)
○ Impact rates per category and profile (Article 5.1.d GDPR) ○ Auditability (Articles 5, 22, 24 and 25 GDPR)
Information on redress:
○ Explainability profiling (Recital 71 GDPR) ○ Redress or review (Articles 13.2.f, 14.2.g and 15 GDPR) ○ Redress metrics, if applicable

[12] The Spanish Ministry of Labor interprets the scope of company obligations to provide information on algorithms | Garrigues

- **Proposal for EU algo-scores** (including methodology to produce scores and visualization of results).

As AI systems proliferate, there is a need to facilitate public awareness and understanding of how algorithmic systems work. The proposal draws from two existing methodologies of significant societal impact: the Nutriscore and A+++.

4.5. Standardized messenger audit

by Pr. Matthieu CUNCHE

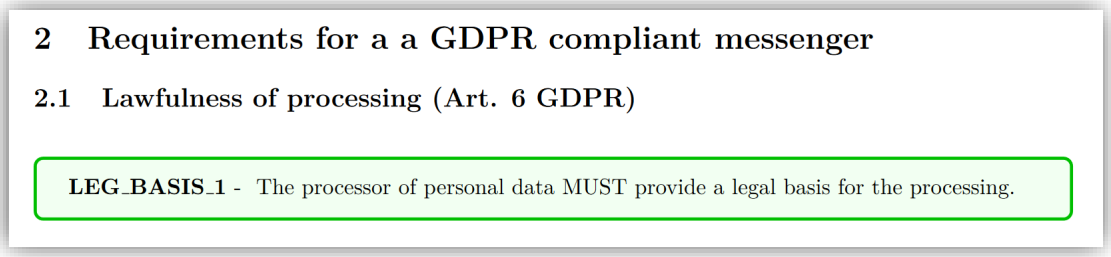
- Project available at: https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/standardised-messenger-audit_en

At the request of the DE SA (Federal), a project was launched with respect to the **audit of messenger services used within businesses**. The goal of this SPE project was to develop a test catalogue of mandatory, recommended, and optional requirements, which a GDPR-compliant messenger front end has to meet. This catalogue is primarily supposed to support supervisory authorities in their work, but companies may also be interested in it to review and improve on their product (once it is published).

The project was completed in November 2023 by the expert Dr. Mathieu Cunche, through two deliverables, namely a document explaining the frontend requirements and another one with respect to audit methodology. To produce these deliverables, the expert worked closely with the DE SA (Federal), which provided significant input and feedback.

The first document features a list of criteria. It is closely based on the structure and outline of the GDPR, for supervisory authorities to have an easier orientation to the respective requirements of the GDPR is ensured and a faster and more comprehensive overview of the requirements of the test criteria can be guaranteed. For each of these criteria, an audit methodology is explained in the second document.

For example, regarding Lawfulness of processing (Art. 6 GDPR), the first document “D1 - Frontend Requirements” provides for the following requirement:

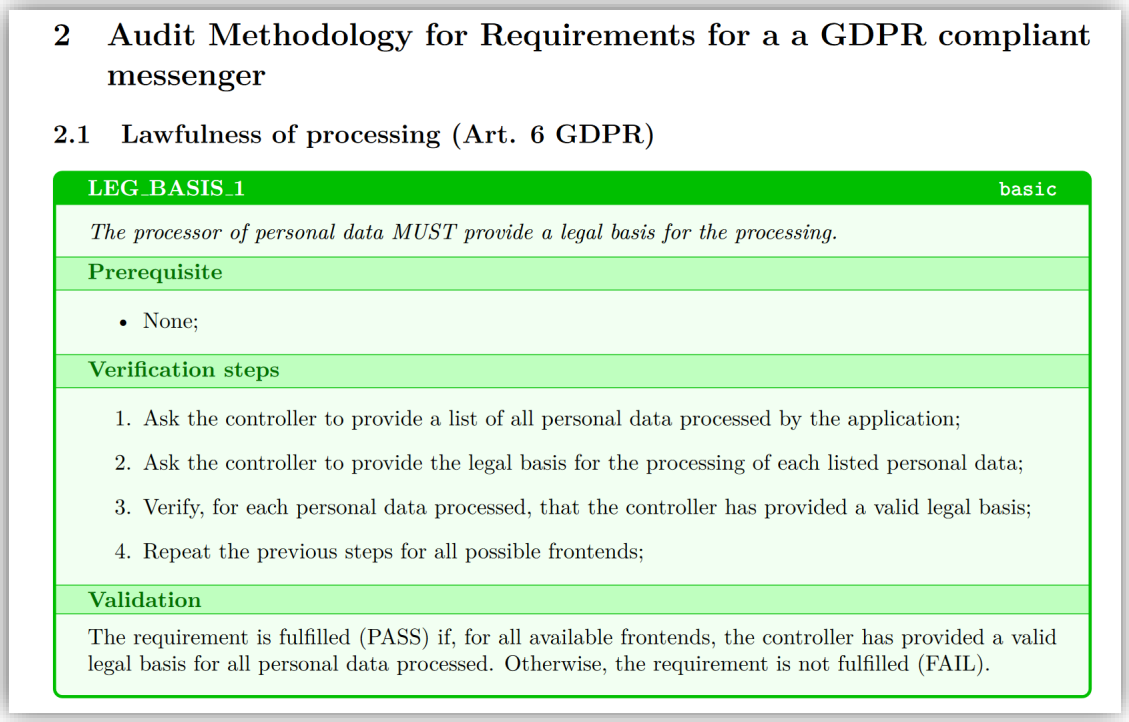


2 Requirements for a a GDPR compliant messenger

2.1 Lawfulness of processing (Art. 6 GDPR)

LEG_BASIS_1 - The processor of personal data MUST provide a legal basis for the processing.

In parallel, the second document “D2 - Audit Methodology” gives a practical methodology to audit the above requirement:



2 Audit Methodology for Requirements for a a GDPR compliant messenger

2.1 Lawfulness of processing (Art. 6 GDPR)

LEG_BASIS_1 basic

The processor of personal data MUST provide a legal basis for the processing.

Prerequisite

- None;

Verification steps

1. Ask the controller to provide a list of all personal data processed by the application;
2. Ask the controller to provide the legal basis for the processing of each listed personal data;
3. Verify, for each personal data processed, that the controller has provided a valid legal basis;
4. Repeat the previous steps for all possible frontends;

Validation

The requirement is fulfilled (PASS) if, for all available frontends, the controller has provided a valid legal basis for all personal data processed. Otherwise, the requirement is not fulfilled (FAIL).

4.6. DPO Training

by Dr. Tihomir KATULIC

- Project available at: https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/data-protection-officer-training_en

This project was initiated by HR SA. To improve the DPOs' knowledge, especially in hospitals and educational institutions, an SPE project was launched to train data protection officers in Croatia and raise the overall level of compliance of their organisations. More specifically, an extensive DPO training programme was designed in Croatian by an external expert, with training materials and Q&As for DPOs. The deliverables included presentations and exams for general training modules and modules that are specifically tailored for the health and educational sectors.

The deliverables have been finalised in December 2023. The external expert Dr. Tihomir Katulić gave training sessions to the staff of the HR SA and the HR SA will be able to use the training material for DPO training (more information is available at https://azop.hr/edpb-support-pool-of-expert-project-data-protection-training-programme-for-dpos-in-croatia/). DPOs in Croatia will be able to follow training sessions for free and take exams.

4.7. AI risks - Optical Character Recognition (OCR) & Name Entity Recognition (NER)

by Isabel BARBERA GARCIA

- Project available at: https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/ai-risks-optical-character-recognition_en

In the specific context of the development of AI, the EDPS asked to assess two types of AI systems, namely OCR and NER. OCR is a technology used to convert images or scanned documents containing text into machine-readable text. OCR technology enables the extraction of text from both physical paper documents and digital sources. NER is an information extraction technique employed in natural language processing (NLP)[13]. NER is used to identify named entities such as names, organizations and locations within a document and classify them into predefined categories.
The objective of this project was to help data controllers in their obligation to perform an assessment of data protection risks and, when necessary, to conduct a Data Protection Impact Assessment and to help data protection authorities to evaluate the validity and effectiveness of this assessment in the course of their investigations.

The two deliverables[14] (finalised in **September 2023** by the expert Isabel Barbera Garcia) identified **data protection and privacy risks posed by the procurement, development and use of those types of AI systems**. They then proposed how to assess **the likelihood and severity of the identified risks** and also suggested risk treatment options such as effective **mitigation tools or strategies**.

For both technologies, the expert identified specific data protection and privacy risks posed by the **procurement**, the **development** and the **use** of the specific technology.

For example, the first specific risk posed by procurement for OCR is, at first, described as follows:

Data Protection and Privacy Risks	Risk description	GDPR Impact	Examples	Risk applicable on service model provision
Insufficient protection of personal data what eventually can be the cause of a data breach	Safeguards for the protection of personal data are not implemented or are insufficient	Infringement of Art. 32 and Art. 5 (f) GDPR: Integrity and confidentiality and Art. 9, Special categories of personal data	OCR systems that process text containing personal data could be not properly secured. This could be the case if transmission of data is not secure, data are not stored encrypted or with an adequate access control mechanism.	SaaS cloud

[13] Natural language processing is an interdisciplinary subfield of linguistics, computer science, and artificial intelligence concerned with the interactions between computers and human language, in particular how to program computers to process and analyse large amounts of natural language data (Source: Wikipedia)

Then, its likelihood is assessed:

Data Protection and Privacy Risks	Risk factor	Risk description	Likelihood	Reasoning
Insufficient protection of personal data what eventually can be the cause of a data breach	- Insufficient security measures - Processing sensitive data - Large scale processing - Processing data of vulnerable individuals	Safeguards for the protection of personal data are not implemented or are insufficient	Low	The third-party suppliers we have reviewed, have implemented security measures such as secure transmissions, strong access control measures, and data encryption at rest. We, as user/customer have also strong security processes implemented internally.
Possible adverse	Low data	The output of the system could	Low	Though the impact would be high, we

Then its severity:

Data Protection and Privacy Risks	Risk description	Likelihood	Severity	Reasoning
Insufficient protection of personal data what eventually can be the cause of a data breach	Safeguards for the protection of personal data are not implemented or are insufficient	Low	Very significant	The documents contain very sensitive information, and a data breach could cause significant harm to the data subjects
Possible adverse	The output of the system could	Low	Very	Using the system for other purposes

and ultimately a global evaluation of the risk is proposed:

Data Protection and Privacy Risks	Risk description	Likelihood	Severity	Risk Level
Insufficient protection of personal data what eventually can be the cause of a data breach	Safeguards for the protection of personal data are not implemented or are insufficient	Low	Very significant	Very High

Finally, mitigation measures are suggested:

Data Protection and Privacy Risks	Risk Level	Mitigation measures	Feasibility Assessment	New risk Level after mitigation
Insufficient protection of personal data what eventually can be the cause of a data breach: safeguards for the protection of personal data are not implemented or are insufficient	Very High	The third-party vendor chosen must have implemented security measures such as secure transmissions, strong access control measures, and data encryption at rest and sufficient privacy design strategies[37] to protect the data. We will ask certifications[38] and results of a pentest[39] to the vendor. As controller we can also protect the specific sensitive data in the documents by applying pseudonimisation or anonymisation techniques after the data extraction. Depending on the different needs, we could implement default anonymisation or reversible data masking techniques, for instance allowing access to the unmasked data to certain people. If the OCR SaaS solution does not offer the possibility to implement these techniques[40], we could decide to look for a vendor that can offer them or implement them ourselves.	1. Cost of implementation: The implementation of pseudonimisation or anonymisation techniques after the data extraction would imply extra cost. 2. Impact on purpose of digitization and archiving: No 3. Impact on expectations of individuals: No 4. Impact on transparency and fairness of the processing: No	Low
Possible adverse	Very High	Unauthorised access to	1. Cost of	Low

5. SPE EVENTS

5.1. Bootcamp on website auditing

The EDPB Secretariat organised a **first in-person Bootcamp in Brussels to allow SAs' experts to exchange knowledge, best practices and test tools for website auditing**. **In total, 51 experts from 27 SAs met in Brussels on 12-13 June 2023.**

This topic was chosen to support SAs in analysing the complaints regarding cookies as well as the increasing number of investigations regarding trackers. It aimed to address a need of building common practices, enhancing the sharing of knowledge, but also of strengthening procedure robustness. During these two days, one SA presented the various types of trackers used online for advertising purposes and explained how it collects and manages digital evidence. Then three tools were presented to SAs: the Website Auditing Tool (see Section4.3), the EDPS Website Evidence Collector and the Baden-Wurttemberg's Website Evidence Tool.

5.2. Support Pool of Expert event for experts

The EDPB organised a first online event with the external experts of the Support Pool of Experts on 8 February 2024. The event was the occasion to inform them about what has been done since their inclusion on the list of reserve, obtain their feedback and facilitate discussions on the SPE program and projects.
For this occasion, the EDPB invited speakers that participated in SPE projects both from an SA's and an expert's perspective. The two hours program was followed by around 200 experts.

CONCLUSION

This report provides a brief overview of the SPE projects launched with the reserve list of external experts since the program has started. Many diverse projects have been launched, including a growing trend of projects on AI systems, which shows the eagerness of SAs to benefit from the use of external expertise, whether legal or technical - or both.