EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

EDPS OPINION ON A PRIOR CONSULTATION REQUESTED BY [...]

on the online assessment with remote invigilation in the context of the recruitment

(Case 2021-0747)

1. PROCEEDINGS

On 27 July 2021, the European Data Protection Supervisor (EDPS) received a request for prior consultation under Article 40 of Regulation (EU) 2018/1725[1] ('the Regulation') regarding the online assessment with remote invigilation in the context of the recruitment.

The request for prior consultation sent by [...] contained the DPIA and the following supporting documents:

- The threshold assessment
- The record of processing activities – notification
- The legitimate interest assessment on covering the capture of video data in the provision of remotely invigilated exams prepared by [...] (the processor).

According to Article 40(2) of the Regulation, the EDPS is to issue his Opinion within a period of up to eight weeks of receipt of the request for consultation, with a possible extension by six weeks. The period has not been extended in this case.

Taking into account that this period may be suspended[2] until the EDPS has obtained any further information that he may have requested[3], the deadline within which the EDPS shall issue his Opinion in this case is **7 October 2021.**

---

1 Regulation (EU) 2018/1725 of the European Parliament and the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ, L 295, 21.11.2018, pp. 39-98.

2 Article 40(2) of Regulation 2018/1725.

3 In the present case, the deadline was suspended for 30 days: from 6 August to 5 September 2021.

2. DESCRIPTION OF THE PROCESSING

After the outbreak of the COVID-19 pandemic, [...] has taken a range of measures to avoid spreading the virus. In this context, selection procedures are carried out remotely, including written/practical tests. [...] considers remote recruitment as a necessary precaution to reduce the increased risk of virus contamination by avoiding meetings with participants at the [...] Headquarters, including (external) candidates.

[...] would like to conduct remote tests in the context of selection procedures by having the candidates supervised by an external proctor during the examination. Such services will be provided by an external contractor [...], acting as a processor. [...] considers that a remote invigilation of the tests in the recruitment process would guarantee the security, fairness and integrity of the selection process.

The external provider ([...], based in [...]) will receive in advance the names and contact details (name, date of birth, place of birth, ID/ passport number, gender, email address and phone number) of the candidates that are shortlisted and invited to take part in a remote selection procedure that consists of a written/practical test and an interview. Further identification of the candidates would take place on the date of the invigilated test via video (candidates are requested to show ID proof). The invigilator will monitor the candidates during the remote test through two video streams, i.e. a video from the webcam and a video that is captured from the candidate's computer screen. Then [...] will pseudonymise the candidates' written test and send them to the [...] Recruitment and Selection Team, together with a decoding file for candidate identification and a report on the execution. [...] would provide the video recording to [...] only upon [...]'s instructions. The documentation provided does not indicate in which circumstances [...] would ask for the video recording.

The written tests collected in the invigilated remote testing, the decoding file for candidate identification, the report on the execution and the video monitoring (if applicable) will be kept in [...]'s archives for at least four full calendar years and up to a maximum of five years as from the year the candidates are informed about the outcome of the selection procedure. This retention period is also serving the situation when the European Ombudsman is dealing with a complaint submitted against a selection procedure (which can be made within two years of the date on which the facts on which a complaint is based came to the attention of the person lodging the complaint).

[...] will pseudonymise all personal data processed, with the exception of the video data (if applicable) and the invigilation reports (including on possible cheating and malpractice), at the acknowledgement of receipt by [...] of the remote written tests answers. [...] will hold all video records (if applicable) and invigilation reports for a period of 6 months after which they are deleted. The [...] application and data are hosted on [...]. According to [...], the [...] application and data servers are located in the AWS datacentre in [...]. All [...] data are held in the EU and are subject to EU data protection laws.

Access to the remote tests, decoding files and reports will be limited to authorised [...] HR personnel. Selection Committee members will be given access to documents on a need-to-know basis and in accordance with their nomination to participate in individual selection procedures. In principle, Selection Committee Members will have access only to the pseudonymised tests. Data may be also disclosed on a need-to-know basis to other [...] teams ([...]), the European Ombudsman, the Civil Service Tribunal and the European Data Protection Supervisor.

3. PRIOR CONSULTATION PURSUANT TO ARTICLE 40 OF THE REGULATION

3.1. The threshold assessment and the DPIA

The online assessment with remote invigilation represents a substantial change in the recruitment process of [...]. [...] conducted a threshold assessment of the risks generated by this new processing, which resulted in the following criteria triggering the need for a DPIA[4]:

- Systematic and extensive evaluation of personal aspects or scoring, including profiling and predicting:

  'Like traditional proctoring, online proctoring involves a proctor who observes the test-taker in order to confirm their identity, answer any questions they may have, and to prevent, identify, and/or report cheating and malpractice. (...);

- Automated-decision making with legal or similar significant effect: processing that aims at taking decisions on data subjects:

  'Online proctoring uses student authentication, secure exam browsers, activity detection and flagging as ways of ensuring that the test results are as authentic as physically proctored test results. These are all automated decisions that have an effect on the data subjects.'

- Systematic monitoring: processing used to observe, monitor or control data subjects;

  '(...) a candidate will be supervised by a proctor during the testing element of the procedure, to guarantee the security, fairness and integrity of the selection process';

- Data concerning vulnerable data subjects: situations where an imbalance in the relationship between the position of the data subject and the controller can be identified:

  'There is imbalanced relationship between employer-employee/job applicant'.

- Innovative use or applying technological or organisational solutions that can involve novel forms of data collection and usage:

[4] Criteria from Annex 1 to the EDPS decision of 16 July 2019 on DPIA lists issued under Articles 39(4) and (5) of Regulation 2018/1725.

'(...) online proctoring is a new tool that involves new forms of data collection and usage.'

The DPIA identified high risks for the candidates, namely that 'the systematic and extensive evaluation that is performed during the remote invigilated testing may result in the legal effect that a candidate may be removed from the selection procedure in case it is established that they have cheated'. However, [...] has not clearly assessed the actual risks to the rights and freedoms of candidates of the processing at stake (remote invigilation of exams) and how the processing could affect the persons concerned against the data protection principles.

The DPIA further identifies a number of mitigating measures by [...] and [...] mainly concerning the access control, security and technical measures. In additional explanations provided in the course of the consultation with the EDPS, [...] clarified that the candidates will be provided with detailed information how the invigilated tests are organised, how their data will be processed and about the need to remove any information/items from their backgrounds and to close all applications on their computers that may lead to the disclosure of sensitive or other personal data not necessary for the processing operation. The EDPS takes note that [...] did not introduce in the DPIA any differentiation between the level of risk before and after the introduction of mitigating measures.

3.2. Need for prior consultation pursuant to Article 40 of the Regulation

Article 40(1) of the Regulation provides that the controller is to consult the EDPS prior to processing where a DPIA under Article 39 indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in view of the available technologies and costs of implementation.

Despite the measures identified by [...] and [...] to mitigate those risks, the DPIA concludes that the risk cannot be mitigated by reasonable means and at the same time points out the need to balance the risk for the candidates subject to the online recruitment and the risk of spreading of COVID-19 virus by reducing travelling and physical contacts that are involved in testing at the [...] headquarters. However, [...] did not explain in details why those risks could not be successfully mitigated.

3.3. Scope of the Opinion

The Opinion of the EDPS on this prior consultation **only concerns the high risks generated by the data processing in the course of the online assessment with remote invigilation in the context of the recruitment and the mitigating measures envisaged by [...], as described in the notification** of [...] and appended documentation.

This Opinion will focus on key aspects in this respect that raise issues of compliance with the applicable data protection legal framework or otherwise merit further analysis.

The EDPS trusts that the data processing is otherwise compliant with the Regulation, including the stipulations of the contract between [...] and its processor, notably as regards the location of the data processed on behalf of [...] in the EU/EEA.

The EDPS expects to be consulted on any significant update of the DPIA as a result of a substantial modification of the personal data processing operations at stake.

4. LEGAL AND TECHNICAL ASSESSMENT

4.1. Identification and mitigation of the risks in the DPIA

The EDPS welcomes that the DPIA generally follows the template structure of the DPIA report provided for in the EDPS Accountability toolkit[5]. However, as already pointed out in the point 3.1 of this opinion, [...] identified one of the criteria to conduct a DPIA listed in Art. 39 of the Regulation ('the systematic and extensive evaluation') as high risks, while:

- the circumstance that 'the systematic and extensive evaluation that is performed during the remote invigilated testing may result in the legal effect that a candidate may be removed from the selection procedure in case it is established that they have cheated' is inherent to any kind of exam invigilation and not to online invigilation;
- the controller should rather assess primarily the risks to the rights and freedoms of candidates generated by the remote invigilation (e.g. privacy intrusion, discrimination possible chilling effect due to the stress of being under surveillance, etc.), how this new processing could affect these rights and freedoms against the data protection principles and what is the possible impact on the persons affected, both in terms of likelihood and severity.

As the next step of conducting the DPIA, the controller should identify the mitigating measures and conduct a subsequent assessment to check whether the processing still poses a high risk to the rights and freedoms of data subjects, which cannot be mitigated by reasonable means in the controller's opinion[6]. If this is the case, the controller should consult the EDPS in accordance to Art. 40 of the Regulation. In the present case, as already pointed out, the DPIA concludes that the risks cannot be mitigated by reasonable means but not explicitly explain why.

[5] Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies, available at https://edps.europa.eu/node/4582_en.

[6] Please check the example on p. 25 Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies, available at https://edps.europa.eu/node/4582_en.

Therefore, the EDPS recommends that [...] improve the DPIA by identifying properly all risks for the rights and freedoms of candidates, as well as how the remote test invigilation could affect these rights and freedoms against the data protection principles, and clearly indicate in the DPIA the likelihood and impact of those risks before and after the introduction of the mitigating measures envisaged.

4.2. Lawfulness of the processing

In the DPIA, [...] states that the data of candidates in the context of the online recruitment with remote invigilation will be processed on the basis of Art. 5(1)(a) of the Regulation because the processing is necessary for the performance of a task carried out in the public interest on the basis of EU law ([...] Regulation[7] or other legal instruments concerning condition of employments in the EU bodies and agencies[8]). [...] indicates as well Art. 5(1)(b) of the Regulation as a legal basis, however it is not appropriate as none of the above mentioned legal acts requires [...] to specifically process the data of the candidates in the online recruitment with remote invigilation.

At the same time, [...][9] and [...][10] claim that they will process the data of the candidates also on the basis of Art. 5(1)(d) of the Regulation and that the candidate will give consent to the processing of his or her personal data in the context of the online recruitment with remote invigilation by sending his/her application and by acknowledging the data protection notice and information provided in advance of the remote invigilation test.

The EDPS considers that in case of the online recruitment with remote invigilation, consent is not a valid legal basis. Art. 3(15) of the Regulation stipulates that *consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.* A consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent. If the consequences of consenting undermine individuals' freedom of choice, consent would not be free[11].

[7] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation ([...]) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.
[8] [...]
[9] [...] Record of processing activities.
[10] The legitimate interest assessment on covering the capture of video data in the provision of remotely invigilated exams prepared by [...].
[11] Please check the EDPB Guidelines 05/2020 on consent under Regulation 2016/679.

In this specific case, there is a clear imbalance of power in the relationship between the potential future employer (controller) and the candidate (data subject). The candidate will have no real alternatives to accepting the online assessment with remote invigilation in the context of the recruitment organised by [...]. A lack of consent would mean that the candidate could not take part in the recruitment at all. Consent could be considered as freely given only when [...] would give the candidate a practicable alternative like a possibility to come for an interview or a test on the [...] premises, which, in the context of the COVID-19 outbreak, may not be always possible.

In light of the above, the EDPS recommends that an exclusive legal basis for processing of candidates' data in the context of the online recruitment with remote invigilation be Art. 5(1)(a) of the Regulation. However, [...] should continuously monitor any developments related to the COVID-19 pandemic, in particular any significantly decreased levels of associated health risks, in order to ensure that the necessity to carry out online recruitment with remote invigilation remains established.

In view of Art. 5(1)(a) of the Regulation as the legal basis for processing, Art. 23 of the Regulation applies, providing for the data subjects' right to object which should be clearly mentioned in the [...]'s record of processing activities as well as in the data protection notice that must be made available before the candidate applies. The EDPS underlines that processing can take place despite an objection from the data subject related to his or her particular situation if [...] demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the candidates, for example related to specific circumstances arising from the pandemic.

Moreover, as further developed below (section 4.3), the processing will involve the processing of sensitive data, which requires a specific ground for lawfulness under Article 10 of the Regulation.

4.3. The risk of disclosing personal information of sensitive nature

This risk of disclosing personal information of sensitive nature, including special categories of personal data as defined in Art. 10 of the Regulation and its impact on data subjects (such as discrimination) was not considered in the DPIA. It is reasonable to expect that the candidate might accidentally open an application running on background, receive a notification (e.g., e-mail client) or the background of a room can show e.g. religious symbols, which might reveal some personal information to the invigilator during the capture of video or the screen sharing during the test. Such risk is in most cases of accidental character, with an exception of the data subjects' racial or ethnic origin, which may be revealed systematically and requires a legal basis under Art. 10(2) of the Regulation. In this regard, [...] could look into Art. 10(2)(g) of the Regulation, which allows for processing of special categories of data, provided that it is 'necessary for reasons of substantial public interest, on the basis of Union law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard

the fundamental rights and the interests of the data subject' or into Art. 10(2)(i) of the Regulation, which allows for processing of special categories of data, provided that it is 'necessary for reasons of public interests in the area of public health, such as protecting against serious cross-border threats to health [...], on the basis of Union law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject'.

The risk of disclosing personal information of sensitive nature, including special categories of personal data, should be properly assessed by [...] and linked it in the DPIA with the mitigated means preventing such excessive collection of data. In additional explanations provided in the course of the consultation with the EDPS, [...] clarified that the candidates , before they take the tests, will be provided with detailed information about the need to remove any information/items from their backgrounds and to close all applications on their computers that may lead to the disclosure of sensitive or other personal data not necessary for the processing operation, [...] plans also to delete footage of a candidate in case an excessive collection occurs, without indicating precisely how they would proceed. Such information on the mitigating measures should be complemented in the DPIA.

The EDPS recommends updating the DPIA to consider the risk of disclosing sensitive data or data of a highly personal nature during the invigilated exam, to identify the mitigating means and to identify a legal basis under Art.10(2) of the Regulation for the processing of data on racial or ethnic origin.

4.4. Automated decision-making

[...] indicates in the DPIA that the online proctoring uses student authentication, secure exam browsers, activity detection and flagging to ensure that the test results are as authentic as physically proctored test results. All these activities are identified by [...] as automated decisions that have an effect on the data subjects, i.e. a possible exclusion from the selection procedure in case these processes establish that they have cheated. However, in the documentation [...] does not make any reference to the automated individual decision-making on the basis of Art. 24(2)(a) of the Regulation or to the controller's obligations from Art. 24(3) of the Regulation, which would apply in this regard, should any decision in the process be 'solely' based on automated processing. However, as explained in the part on the description of the processing, it seems that all decisions taken in the process of invigilation are entirely based on a human intervention by an invigilator or the [...] Selection Committee.

Thus, the EDPS recommends updating the DPIA to make it clear that no decision based solely on automated decision is made during the online recruitment with remote invigilation. If [...] concludes that in fact some decision will be 'solely' based on automated processing, than the DPIA should be complemented with a reference to Art. 24(2)(a), in particular establishing the relevant necessity, and Art. 24(3) of the Regulation. The latter one requires as well to identify and record the degree of any human involvement in the decision-making process and at what

stage this takes places[12]. Additionally, in such case the data subjects should be informed, in accordance with Art. 15(2)(f) of the Regulation, about the logic involved in the automated decision-making, if any, as well as the significance and the consequences of such processing.

4.5. Video recording

In documentation provided, [...] states that the invigilator monitors the candidates during the remote test through two video streams, i.e. a video from the webcam and a video that is captured from the candidate's computer screen. [...] explains[13] that [...] may record the written test and provide the video recording to [...] only upon [...]'s instructions, while [...] states[14] that they record all exams, but the client can ask them not to record the exam in specific cases. However, none of the provided documents clarifies in which situations may [...] request [...] to record (or not to record) the exams and to provide the recordings to [...].

Therefore, the EDPS recommends that [...] further describe in the DPIA in which situations [...] should be instructed to proceed with the recording of the video from the candidate and to provide it to [...]. This information should also be provided to the candidate prior to the exam.

The DPIA should also indicate that the video capture of the screen gets stored together with the webcam footage as currently only the webcam footage is mentioned in this context in the documentation.

4.6. Pseudonymisation

In documentation provided, [...] states that [...] will anonymise the candidates' written tests and send them to [...]. From the description of this process, it seems that [...] will rather pseudonymise[15] the test, so it cannot be attributed to a specific candidate, and will send separately a decoding file for candidate identification. If the tests were anonymised, [...] could not trace them back to the candidate which would defeat the purpose of the recruitment.

Therefore, the EDPS recommends correcting the term used and referring to 'pseudonymisation' instead of 'anonymisation'.

[12] Please check WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, endorsed by the EDPB.
[13] [...] Record of processing activities.
[14] The legitimate interest assessment on covering the capture of video data in the provision of remotely invigilated exams prepared by [...].
[15] See Art. 3(6) of the Regulation.

5. CONCLUSION

The EDPS has made recommendations to ensure compliance of the processing with the Regulation.

The EDPS expects that **[...] implements these recommendations (summarised below) and provides documentary evidence** of this implementation before commencing the online recruitment with remote invigilation within **three months** of this Opinion:

1. identify all risks for the rights and freedoms of candidates and indicate in the DPIA the likelihood and impact of the risks before and after the introduction of the mitigating measures;

2. continuously monitor any developments related to the COVID-19 pandemic in order to ensure that the necessity to carry out online recruitment with remote invigilation remains established;

3. refer solely to Art. 5(1)(a) of the Regulation as the legal basis for processing of candidates' data in the context of the online recruitment with remote invigilation;
4. update the DPIA to clarify whether Art. 24(2)(a) of the Regulation will be applicable to the intended processing ;
5. update the DPIA to consider the risk of disclosing sensitive data or data of a highly personal nature during the invigilated exam and to identify the mitigating means and to identify a legal basis under Art.10(2) of the Regulation for the processing data on racial or ethnic origin;
6. describe in the DPIA in which situations [...] should be instructed to proceed with the recording of the video from the candidate;
7. refer in the record of processing activities to a correct term 'pseudonymisation' instead of 'anonymisation'.

Done at Brussels on 5 October 2021

[e-signed]

Wojciech Rafał WIEWIÓROWSKI