EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

9 August 2021

EDPS Guidance on Return to the Workplace

and EUIs' screening of COVID immunity or infection status

edps.europa.eu

Executive Summary

Several EU Institutions, Agencies and Bodies ('EUIs') are considering 'Return to Workplace' strategies which include screening the COVID immunity or infection status of staff, contractors or visitors, as a means to mitigate the risk of workplace transmission. Such measures may foresee verifying EU Digital COVID Certificates, using antigen tests, or recording staff vaccination status.

The EDPS considers that the use of such measures requires caution and very careful assessment to ensure compliance with Regulation (EU) 2018/1725 ('the Regulation') and to minimise the impact on individuals' rights and freedoms. Lawfulness may depend in part on the national legislation of the host Member State and the EDPS urges EUIs to ensure their actions are in line with domestic legislation, the latest public health guidance and recommendations of the relevant national Data Protection Authority.

EUIs considering the use of antigen testing or EU Digital COVID Certificates should verify whether their use would fall under the scope of the Regulation: manual verification of a test result or of a paper or digital COVID certificate, without further registration or recording would not qualify as processing of personal data under the Regulation. Verification of antigen tests or COVID certificates involving the scanning of a QR code or followed by registration or recording of results would be subject to the restrictions required under Article 10 of the Regulation. In principle, the legal basis for such processing could be provided by Article 1(e)(2) of the EU Staff Regulations supplemented by an executive decision of an EUI providing for adequate measures to safeguard the fundamental rights and interests of the data subject.

Given the current voluntary nature of COVID vaccinations in the EU, and without prejudice to the use of EU Digital COVID Certificates where appropriate, the EDPS considers that there is no legal basis for EUIs to request proof of vaccination status from individuals. EUIs may however collect aggregated, anonymised staff vaccination data to support workplace risk assessments. In this respect, the analysis of aggregate staff vaccination data may be an essential first step before considering more privacy-intrusive measures.

EUIs must undertake a careful necessity and proportionality assessment to justify the implied interference with individuals' fundamental rights to private life and data protection. Processing of data related to antigen testing would only be justified in specific employment settings where the risk of exposure by staff would be particularly high and where the working environment makes it impossible to resort to less intrusive measures. Processing of EU Digital COVID Certificates in the workplace should only be considered once EUIs have discarded other alternative, less privacy intrusive measures and according to strictly defined parameters. Use should only continue as long as the exceptional circumstances justifying this processing persist and should be subject to regular reassessment.

In general, EUIs should avoid verification procedures which record or retain personal data unless considered absolutely necessary and provided by law. Mandatory verification of certificates as a means to grant access to the workplace should not be based solely on automated processing and should allow for meaningful human involvement during the verification process.

Contents

EDPS Guidance on Return to the Workplace and EUIs' screening of COVID immunity or infection status

1. INTRODUCTION

As vaccine programmes accelerate across the EU, and COVID-related restrictions are gradually lifted, EU Institutions, Agencies and Bodies ('EUIs') are devising 'Return to the Workplace' strategies to bring staff back onto premises while protecting the health of employees.

In the context of return strategies, some EUIs are considering initiatives to screen employee immunity or infection status, as a means to mitigate the risk of workplace transmission, e.g. by filtering access to buildings, or meetings. Proposed techniques include the use of antigen tests, recording of staff vaccination status, or making use of the EU Digital COVID Certificate.

Health and safety legislation requires employers to take reasonable steps to reduce workplace risks. However, these initiatives can constitute a serious interference with the rights to data protection and private life, and their application may raise the risk of discrimination.

The EDPS considers that the use of such measures, which may imply processing of sensitive health data for determining access to the workplace, requires very careful assessment, to ensure that their use by EUIs is lawful and to minimise the impact on individuals' rights and freedoms. Such assessments should necessarily be linked with EUIs' wider workplace risk assessments, and take into account multiple evolving factors, including the epidemiological situation, data regarding vaccination and immunity rates, and the latest public health regulations and guidance.

The EDPS recognises the challenges that employers face when seeking to balance their obligations to protect their workforce and meet their general duty of care towards employees while respecting fundamental rights and freedoms. In this context, the EDPS has decided to issue guidance on the use of antigen tests, vaccination status data, and EU Digital COVID Certificates by EUIs to help ensure appropriate protection of individuals' rights to data protection and privacy and compatibility with Regulation 2018/1725[1] ('the Regulation') where applicable. This guidance should be considered in the context of ongoing scientific, legal and societal developments in the context of the COVID-19 pandemic.

[1] *Regulation (EU) 2018/1725 of the European Parliament and of 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, p. 39).*

2. EUIs' RETURN TO WORKPLACE STRATEGIES AND INTERPLAY WITH NATIONAL LAW

Before considering the use of intrusive measures in the context of return to workplace strategies, EUIs must first assess whether such measures can be applied in the national legal setting of their host Member State: whether national legislation expressly provides for, or obliges, a measure, or whether it is prohibited under the host's national law.

The EDPS recalls that, while EUIs enjoy privileges and immunities vis-à-vis the EU Member States, those privileges and immunities cover only those areas necessary for the specific functioning of EU institutions and bodies.[2] Should EUIs intend to deviate from the host's national legal regime, they should first assess whether a divergence is permitted according to the specific headquarters or establishment agreements concluded with the Member State concerned.[3]

Furthermore, the EDPS recommends that EUIs take into account the most recent guidance and recommendations of the Member States' national health authority and the legal interpretations provided by national data protection supervisory authorities.

3. EUIs' PROCESSING OF COVID VACCINATION STATUS

EUIs considering the possibility to collect individuals' (including staff, non-staff or visitor) vaccination data must refer to the national law of the host Member State.

Currently, the COVID vaccine is voluntary in all EU Member States. By extension, it seems that with the exception of certain specific sectors such as health and social care, vaccination may not be considered a compulsory safety measure in national legislation. An employer's request to staff to inform or provide proof of vaccination status may undermine the voluntary nature of national vaccine policies in the EU and the principle of autonomy which foresees the right of competent adults to make informed decisions about their own medical care.

Vaccination status constitutes sensitive health data, and its processing may represent an interference with the right to data protection and intrusion into the right to private life as protected under the Charter of Fundamental Rights of the European Union. Such an intrusion would be further exacerbated if employees feel obliged to account for their reasons for foregoing or delaying vaccination (e.g. a serious underlying health conditions, or pregnancy). It could prove difficult to safeguard the confidentiality of such information if such data were used to organise staff presences. Moreover, employers' processing of vaccination data, if used to apply differential treatment to staff, raises risks of discriminatory treatment under Article 21 of the Charter (for instance on the basis of health status).

---

[2] *Protocol (No 7) on the privileges and immunities of the European Communities, OJ C 115/266, 9.5.2008.*

[3] *The Protocol on the privileges and immunities of the European Union is usually implemented by the establishment or headquarters agreement concluded between the EUI and the host state. This agreement defines areas of Member State law that do not apply to the EUI. Exceptions from Member State law include, among others, tax law, employment and welfare law, data protection law. Furthermore, EUIs are autonomous regarding their internal organisation and administration (exception from budgetary and procurement laws).*

The collection of personal vaccination data by EUIs will therefore likely constitute an unnecessary and disproportionate processing, for which there is, at the current time, no clear legal basis under EU or national law. This is likely to remain the case unless COVID vaccinations become mandatory in EU Member States. As a matter of national health policy, this is a decision typically taken at the level of national parliaments, subject to the scrutiny and accountability mechanisms usually required for any measure imposing serious restrictions on individual freedoms. Therefore, the EDPS considers that measures for the collection of vaccination data should not be arbitrated at the level of individual EUIs.

Therefore, and without prejudice to the use of EU Digital COVID certificates, the EDPS strongly advises EUIs to avoid directly asking employees for their personal vaccination status as well as processing such information, regardless of whether such a request is made on a mandatory or voluntary basis.

4. USE OF AGGREGATED VACCINATION DATA

Before EUIs consider, in the context of their return to the workplace strategy, the use of intrusive measures such as antigen testing or processing health data in the form of EU Digital COVID Certificates, they shall, in line with the principle of data protection by design and data minimisation, consider the use of aggregated health data. Aggregated health data that does not allow to link health information to individuals can be considered anonymous[4] and does not fall within the scope of the Regulation. Examples for such aggregated health data include:

- The percentage of staff members that or were vaccinated against COVID-19 within a given time period.
- The percentage of staff members without vaccination against COVID-19 or unknown vaccination status.

The medical services in possession of the vaccination status could be tasked with preparing such aggregated health data. To ensure aggregated data is anonymous, the data should always relate to groups of individuals that are large enough to exclude that insiders can use them to deduce health data about their colleagues.

The medical service may not have accurate and up to date information on the vaccination or recovery status of individuals that received health care treatment independently from the medical service. If EUIs want to encourage their staff to inform the medical service about their vaccination or recovery status to receive more accurate aggregate data, they must ensure that such updates are handled only by medical staff and processing is based on free consent.

EUIs may also consider using surveys in order to have an overview of the percentage of vaccinated and unvaccinated employees. Such surveys should be voluntary and anonymous. EUIs should consider whether the IT survey tool they are relying on guarantees anonymity (even if such a tool does not collect names or email addresses it may collect IP addresses). Free

[4] *See also Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques. 10 April 2014.* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

text questions should be avoided unless strictly necessary as free text responses may identify individuals.

If it is possible to trace data to the survey respondent in any way, then the survey is personalised and will be subject to the Regulation. In such cases, EUIs must ensure that participation is based on the free consent of individuals, by clarifying that participation is voluntary and clearly explaining the purpose of the survey and how the EUI intends to use the data that it collects. Surveys need to comply with the principle of data minimisation and only collect the information that is strictly necessary.

The use of aggregated vaccination data can be an important factor in EUIs workplace risk assessments when devising return to the workplace strategies and should be an essential first step before considering more intrusive measures such as antigen testing or processing of EU Digital COVID Certificates.

5. EUIs' USE OF ANTIGEN TESTING

Antigen tests, also known as Rapid Antigen Detection Tests (RADTs) or lateral flow tests, are a new category of faster, cheaper, though less accurate, COVID tests, which detect the presence of viral proteins (antigens) to identify a COVID infection. Antigen tests can be employed at point-of-care and entail a nasal swab, mixed with a solution and applied to a hand held testing device, giving a result in less than 30 minutes.

EUIs considering using such tests, for screening employees or filtering access to premises, must first assess whether their application is lawful. If no legal basis is provided under the national law of the host Member State, then the legal grounds for their use must be established under EU law.

5.1. Legality of antigen testing outside the scope of the Regulation

EUIs should consider how they intend to use antigen tests and whether this constitutes processing of personal data. If verification of test results is only visual (e.g. displaying the testing device or result at the entrance to a building or meeting, no scanning of a QR code), and is not accompanied by any recording or documentation of results, then the EDPS considers that this does not comprise processing of personal data and falls outside the scope of the Regulation.[5]

However, even without recording test results, antigen tests constitute a physical intervention and the request by an employer to undergo such a procedure in order to access a place of work or participate in a work event, constitutes an interference into the fundamental right to private life protected under Article 7 of the Charter. The measure would therefore be subject to the legality, necessity and proportionality conditions laid down in Article 52(1) of the Charter.

[5] *As defined under Article 2(5) of the Regulation. Such use of tests does not involve a processing of personal data "*wholly or partly by automated means*", and that in the absence of recording of results, this cannot be considered as "a processing other than by automated means of personal data forming part of a filing system or are intended to form part of a filing system".*

An assessment of the necessity and proportionality of imposing antigen tests on employees should take into account the impact on employees of an invasive, uncomfortable procedure, and the frequency with which staff may be subjected to this procedure. The risk stemming from false negatives and false positives, in particular when leading to isolation and quarantine measures, also needs to be assessed in such situations, taking into account that the efficacy of antigen tests are largely limited to detecting infection involving high viral loads and are significantly less effective in detecting low symptom/asymptomatic cases.[6]

When assessing which specific circumstances, physical workplace environment, or group of staff, may justifiably be subject to antigen testing, EUIs should consider the latest public health guidance and recommendations relating to the use of antigen tests. The Council Recommendation on a common framework for the use and validation of rapid antigen tests of 22 January 2021, lays down five situations and settings in which the use of antigen tests in a general context could be considered.[7] These include COVID-19 diagnosis among symptomatic cases, testing contacts of confirmed cases, managing outbreak clusters, screening in high-risk areas and in epidemiological situations or areas where the proportion of test positivity is high.

Additional EU and WHO guidance on the use of antigen testing in the workplace generally recommend their use in high-risk employment sectors (e.g. health and social care, prisons, and other frontline workers in high transmission environments) in contexts of high infection prevalence or for managing outbreaks of clusters where alternative risk mitigation measures cannot be used.[8]

Guidance by the ECDC and EU-OSHA also states that antigen tests can complement, but not replace, occupational health and safety measures and existing non-pharmaceutical interventions (NIPs). Moreover, the EDPS recalls that establishing the necessity of a measure that interferes with individual rights and freedoms requires first demonstrating that other less intrusive measures cannot be relied upon.

5.2. Legality of antigen testing subject to the Regulation

Recording of antigen results should be avoided unless deemed strictly necessary for the purpose of the measure. If an EUI assesses, under the conditions of legality, proportionality and necessity set out above, that the imposition of antigen tests is justified for a specific, well-defined, occupational situation, then in most cases documenting results would not be necessary for the objective of screening entry to a workplace or work event.

---

[6] *The ECDC and EU-OSHA recommend to exercise caution in the use of antigen tests in the workplace in low prevalence (low infection) settings "*as the use of RATDs could result in a high number of false positive test results*". ECDC/EU-OSHA Technical Report on Considerations on the use of rapid antigen detection tests for SARS-CoV-2 in occupational settings, 6 May 2021.* https://www.ecdc.europa.eu/en/publications-data/considerations-use-rapid-antigen-detection-including-self-tests-sars-cov-2

[7] *Article 6, Council Recommendation on a common framework for the use and validation of rapid antigen tests and the mutual recognition of COVID-19 test results in the EU (2021/C 24/01).*

[8] *ECDC/EU-OSHA Technical Report on Considerations on the use of rapid antigen detection tests for SARS-CoV-2 in occupational settings, 6 May 2021.* https://www.ecdc.europa.eu/en/publications-data/considerations-use-rapid-antigen-detection-including-self-tests-sars-cov-2*; Commission Recommendation of 18.11.2020 on the use of rapid antigen tests for the diagnosis of SARS-CoV-2 infection, Brussels, 18.11.2020 C(2020) 8037:* https://ec.europa.eu/health/sites/default/files/preparedness_response/docs/sarscov2_rapidantigentests_recommendation_en.pdf*; WHO/ILO Policy Brief, Preventing and mitigating COVID-19 at work, 19 May 2021:* https://apps.who.int/iris/handle/10665/341328

In cases where test results are systematically recorded as part of a filing system, or verification takes place via the scanning of a QR code, this operation would constitute processing of personal data and must meet the conditions for lawfulness under Article 5(1) of the Regulation.

In addition, as antigen test results are health data, processing would be subject to the conditions laid down in Article 10(2) of the Regulation.

Consent (article 10(2)(a) of the Regulation) will, in the majority of cases, not offer a valid legal ground for processing of personal data resulting from antigen tests given the employment context and the inherent power imbalance between employer and employee, even if an EUI is considering offering antigen testing on a voluntary basis. Similarly, consent is unlikely to constitute a valid legal ground for processing of antigen test results of non-staff (e.g. cleaning personnel, security guards, visitors). In order to qualify as free consent, antigen tests would need to take place in a separate location from the workplace and with no possibility for employers to identify who has and who has not undergone a test.

The EDPS considers that, as a measure intended to protect the health and safety of staff, Article 10(2)(b) may provide an appropriate ground for lawful processing of personal data related to antigen testing. By the same rationale, the requirement for a legal basis of the processing could potentially be satisfied by Article 1e(2) of the Staff Regulations, which provides that: *"[o]fficials in active employment shall be accorded working conditions complying with appropriate health and safety standards at least equivalent to the minimum requirements applicable under measures adopted in these areas pursuant to the Treaties."*[9]

In order to further establish the lawfulness of antigen testing in a given context, EUIs must be able to demonstrate the necessity and proportionality of such a measure in relation to its aim. Based on the considerations set out above (see section 4.1), it is unlikely that a compulsory and indiscriminate, systematic screening of employees by an EUI could be lawful. Rather, antigen tests may be justified for certain well defined, limited employment settings, where the risk of exposure by staff is assessed to be particularly high, and where the specificity of the working environment makes it unfeasible to resort to less intrusive risk mitigation measures.

In such cases, the legal basis should be supplemented by an executive decision of an EUI, agency or body, providing for suitable and specific measures to safeguard the fundamental rights and interests of the data subject. The decision should make a clear and compelling case that the processing of personal data related to antigen testing in a specific, well-defined occupational setting is necessary to protect employees' health against the risk of infection; clearly define the scope of application and staff members concerned, and specify a time period for implementation with a sunset clause to ensure that any imposed testing is temporary and subject to compulsory review.

In cases where an EUI assesses that the processing of personal data related to the antigen testing of non-staff, such as external contractors, is necessary, the legal basis could similarly be established by Article 1e(2) of the Staff Regulations supplemented by an executive decision of an EUI which provides suitable and specific measures to safeguard the fundamental rights and interests of the individuals concerned. The executive decision should be further

[9] *Article 1e(2) of the Staff Regulations could also provide an adequate legal basis for antigen testing of non-staff (contractors, trainees, visitors) where deemed necessary and proportionate for an EUI to comply with health and safety obligations towards its staff.*

complemented by an agreement signed between the EUI and the non-staff employer, specifying the above-mentioned measures.

Any EUI executive decision or agreement with a non-staff employer should set out the necessary safeguards to minimise the impact on data subjects, including:

- Use of systems and procedures which limit the recording of results;
- Clear and fair protocols in case of invalid or positive results;
- Provision of full information to employees and non-staff concerning how and why their health data will be processed, length of storage, who will have access to it;
- Technical and organisational measures to ensure security and confidentiality of the processing.

6. USE OF EU DIGITAL COVID CERTIFICATES

The EU Digital COVID Certificate entered into application in all EU Member States as of 1 July 2021. Its purpose is to facilitate the safe free movement of citizens within the EU during the COVID-19 pandemic.[10] The certificate features an inter-operable and machine-readable QR code and is available in paper format or via smartphone applications. The certificate provides proof that a person has either been vaccinated against COVID-19, received a negative test result or recovered from the virus.

6.1. Legality

The primary objective of the EU Digital COVID Certificate Regulation is the facilitation of the free movement within the EU during the COVID-19 pandemic for EU citizens and third-country nationals staying or residing legally in the EU. For any other purpose, the EU Digital COVID Certificate Regulation stipulates that a national law must explicitly provide a legal basis for data processing.[11] In the case of EUIs, national law should be interpreted within the meaning of Article 1(e)(2) of the EU Staff Regulations supplemented by an executive decision of an EUI providing for adequate measures to safeguard the fundamental rights and interests of the data subject as further elaborated below.

EUIs considering the use of the certificates as a means to mitigate the risk of workplace infection should refer to the national legislation of their host Member State to ascertain

---

[10] Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic; Regulation (EU) 2021/954 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) with regard to third-country nationals legally staying or residing in the territories of Member States during the COVID-19 pandemic.

[11] Recital 48 of the Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic.

whether the legal basis for the implementation of the system at national level permits this use, and refer to national health guidance regarding the use of certificates in employment settings.

6.2. Lawfulness under EU law

Whether, and how, certificates fall under the scope of the Regulation, will depend on how EUIs intend to use them. The EDPS distinguishes between the following scenarios:

1) An EUI intends to systematically record certificates or the information they contain as part of a filing system;
2) An EUI intends to put in place a digital verification of certificates involving the scanning of a QR code (with or without recording the data they contain);
3) An EUI intends to put in place a manual verification of certificates involving checks of printed, paper copies or manual checks of the digital certificate.

Scenarios (1) and (2) would constitute processing of personal data as defined by Article 2(5) of the Regulation and must meet the conditions for lawfulness under the Regulation.

Scenario (3) would not fall under the scope of the Regulation, however, the requirement to share confidential medical information in an employment setting (and the obligation to undergo a PCR or antigen test in order to access physical work spaces that this use implies) constitutes an interference into the fundamental right to private life protected under Article 7 of the Charter. The measure would therefore be subject to the legality, necessity and proportionality conditions laid down in Article 52(1) of the Charter and EUIs must undertake a careful assessment to gauge whether such an intrusion could be lawfully justified (refer to section 4.1 and section 5.3 below).

6.3. Use of EU Digital COVID Certificates subject to the Regulation

Use of EU Digital COVID Certificates as described in scenarios (1) and (2) above fall under the scope of the Regulation.

Comprising three sub-certificates attesting either vaccination status, a COVID PCR/antigen test result, or evidence of a prior COVID infection, the EU Digital COVID Certificates contain sensitive health data and their processing must meet the stricter threshold for legality under both Article 5(1) and Article 10 of the Regulation.

The EDPS considers that, as a measure intended to protect the health and safety of staff, Article 10(2)(b) may provide an appropriate ground for the lawful processing of EU Digital COVID Certificates, as may Article 10(2)(g) or 10(2)(i), particularly if national legislation and public health guidance mandate a more widespread use of certificates. For processing of certificates based on consent, see section 6.6. below.

A legal basis for the processing could potentially be provided by Article 1e(2) of the Staff Regulations. However, as a general health and safety related provision, it is unlikely to satisfy

the requirements of lawfulness under the Regulation nor that required by the EU Digital COVID Certificate Regulation.[12]

In order to meet this threshold, EUIs would be required to adopt an executive decision which defines the scope, extent and purpose of the processing and lays down clear safeguards for limiting the impact on the fundamental rights of data subjects.

The legal basis for processing of EU Digital COVID Certificates of non-staff could be similarly established by Article 1e(2) of the Staff Regulations supplemented by an executive decision of an EUI, and complemented by an agreement between the EUI and the non-staff employer, providing suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

Any EUI executive decision establishing the processing of EU Digital COVID Certificates should include a sunset clause requiring its regular, compulsory review, and provide the justifications for the necessity and proportionality of the processing.

The aim of re-purposing certificates for use in an employment context would be to reduce the risk of transmission and protect employees from infection. To assess the necessity of this measure, EUIs should take into consideration the full range of parameters underlying occupational risk assessments in the context of the pandemic, including infection prevalence in the general population; transmission dynamics in the workplace concerned (including existence of clusters); and the exposure risk of staff.

The latter may be determined via the collection of aggregated staff vaccination data (see section 4 above) and this step should be an essential pre-condition before considering processing of EU Digital COVID certificates. EUIs must be able to demonstrate that relying on less intrusive controls, such as organisational arrangements to ensure physical distancing, sanitary precautions and other risk mitigation measures is not feasible/not sufficient to protect the health of staff.

Proportionality requires addressing the impact on individuals' fundamental rights posed by processing EU Digital COVID certificates: this includes the interference with the right to privacy implied by any potential obligation for unvaccinated employees to undergo a PCR or antigen test in order to access their place of work. Any mandatory return to workplace strategy which relies on the verification of EU Digital COVID Certificates could only be justified once all staff members concerned have received the offer of full vaccination. This would ensure that differential treatment is not unfairly imposed on trainees and younger staff members, and should also be taken into consideration should the future validity of certificates be tied to the administration of 'booster' vaccination doses.

Depending on how verification is performed (i.e. where manual verification takes place or where personal data contained in QR codes is recorded), certificates may disclose confidential medical information and allow inferences to be drawn about whether an individual is

[12] *Recital 48 of the EU Digital COVID Certificate Regulation stipulates that: "Member States may process personal data for other purposes, if the legal basis for the processing of such data for other purposes, including the related retention periods, is provided for in national law, which must comply with Union data protection law and the principles of effectiveness, necessity and proportionality, and should contain provisions clearly identifying the scope and extent of the processing, the specific purpose involved, the categories of entity that can verify the certificate as well as the relevant safeguards to prevent discrimination and abuse, taking into account the risks to the rights and freedoms of data subjects."*

vaccinated or unvaccinated. The effect may be to undermine the voluntary nature of vaccination (see section 3 above) and expose employees to potential stigmatisation, and eventual workplace discrimination.

Furthermore, priority should be given to privacy friendly technical solutions (see section 6.5 and 6.6. below).

In light of the above, the EDPS considers that the lawful use of digital COVID vaccination certificates in the context of EUI return to work arrangements should only be considered after discarding alternative, less privacy intrusive measures (such as aggregated vaccination data), and according to strictly defined parameters. Use should only continue as long as the exceptional circumstances justifying this processing (relevant epidemiological parameters, outbreak of clusters, high exposure risk of staff and inability to mitigate risks via other NPIs) persist and must end as soon as those circumstances no longer apply. Regular reassessment is imperative.

6.4. EU Digital COVID Certificates and automated individual decision-making

The EDPS notes that certain uses of EU Digital COVID Certificates may, depending on their practical application, qualify as an automated individual decision-making subject to Article 24 of the Regulation. This could be the case for instance if digital verification of certificates involving the scanning of a QR code is used to automatically filter access to a workplace.

This could qualify as an automated individual decision-making process with significant effects similar to legal effects. In that regard, the EDPS notes that there is currently no Union Law, as per Article 24(4), authorising the verification of health status based solely on automated processing to allow or deny access to EUIs premises on health and safety grounds. Hence, a fully automated verification system would only be lawful on a voluntary basis, with the data subjects' explicit consent under Article 10(2)(a) of the Regulation.[13] Given that, in principle, consent usually cannot provide a valid ground for lawfulness in an employment context, and would not be applicable to the case at hand, EUIs should not rely on fully automated systems that link the scanning of QR codes to granting access to workplace premises.

This means in practice that verification of EU Digital COVID certificates applied on a mandatory basis should not be based *solely* on automated processing, and should provide for meaningful human involvement during the verification process.[14] Meaningful human involvement in this context implies the possibility for someone who has the authority and competence to step in during the verification procedure and assess the specific situation of the data subject and to advise him/her accordingly or override the automated decision. This may occur for instance if an employee claims that the automated reading of the data is erroneous.

---

[13] *See Orientations from the EDPS: Body temperature checks by EU institutions in the context of the COVID-19 crisis, 1 September 2020:* https://edps.europa.eu/data-protection/our-work/publications/guidelines/orientations-edps-body-temperature-checks-eu_en

[14] *According to EDPB Guidelines, "[t]o qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision." EDPB Guidelines on Automated individual decision making and profiling for the purposes of Regulation 2016/679 (WP251rev.01), 6 February 2018, p. 21.*

6.5. Operational aspects of processing EU Digital COVID certificates

Where the processing of EU Digital COVID certificates meets the threshold for lawfulness, necessity and proportionality, specific and appropriate safeguards should be applied, as required by Article 10 of the Regulation.

EUIs should consider the need to carry out a data protection impact assessment (DPIA), under Article 39 of the Regulation, in order to ascertain risks and mitigating measures at all stages of the processing.[15] Digital verification of staff certificates as a means to grant access to an EUI's premises will almost certainly require a DPIA, in accordance with Article 39(3)(b) of the Regulation, as this implies the processing on a large scale of special categories of data.

Data protection by design and default must be applied in accordance with Article 27 of the Regulation, ensuring that only the minimum amount of data is processed and privacy-friendly technologies are used.

In particular, EUIs should envisage verification procedures that avoid recording and retention of personal data, in line with the principle of data minimisation, and in accordance with the EU Digital COVID Certificates Regulation, which intends for the decentralised verification of digitally signed certificates without further processing of data.[16] The operation should be limited to verification and no technical trace of verification should remain once carried out.

The use of certificates should be limited to the specific purpose identified (e.g. screening access to a workspace) and not be deployed for any other not compatible purpose. Data should not be transferred to any other EUI or external recipients unless necessary and specifically provided by law.

In line with the principle of transparency, and the provisions laid down in Chapter 3 of the Regulation, staff and non-staff concerned should be informed well in advance (preferably consulted) on the intention to use EU Digital COVID Certificates within the context of return to workplace measures. They should be informed how verification will work, what data will be processed, who will have access to it, and where to direct any queries or objections regarding the processing.

Data subjects should also be informed of the procedures for requesting the controller (i.e. the national authority responsible for issuing the certificate) to issue a new certificate if the personal data contained in the original certificate are not or are no longer accurate or up to date.[17]

---

[15] See Decision of the European Data Protection Supervisor of 16 July 2019 on DPIA Lists issued under Articles 39(4) and (5) of Regulation (EU) 2018/1725.

[16] See Recitals 48 which states that "Where the certificate is used for non-medical purposes, personal data accessed during the verification process are not to be retained, as provided for in this Regulation". See also Recital 52 and Article 10(3) of the Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic.

[17] Article 3(4) of the Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic.

6.6. Additional remarks on facilitating consent-based EUIs' processing of EU Digital COVID Certificates

EUIs may explore the use of consent for the processing of individuals' health data to support data-driven return to the workplace strategies. However, the EDPS advises EUIs to apply extreme caution, and to carefully assess whether consent is freely given. This is difficult to achieve in the employment context. If there is no possibility for the staff (or non-staff) member to refuse his/her consent, this does not qualify as consent under Article 5(1)(d) of the Regulation.

In this context, privacy enhancing technologies may be applied to enable individuals, on a voluntary basis, to scan their EU Digital COVID Certificates on entry to a building. This processing would not be linked to granting access, but would aim to provide a guide as to the proportion of individuals that are in possession of a valid COVID certificate (and therefore represent a low infection risk) on a given day.

Given the free consent of individuals, EUIs could process their health data encoded in QR codes, near field communication (NFC) tags or other carriers that allow for the use of privacy-enhancing technologies and as such complement organisational with technical data protection safeguards. Such privacy-enhancing technologies encompass for instance zero-knowledge proofs, edge computing, homomorphic encryption, and blind signatures.

Health data processed based on consent should at best not be retained or transferred, but immediately aggregated and/or anonymised.

Organisational and technical safeguards can help that consent is obtained in a free manner:

- Pressure on individuals to provide (unfree) consent is relieved when feedback does not allow to distinguish between individuals that expressed consent and those who did not and their health data is immediately anonymised and aggregated.
- Considering the imperfect nature of COVID-19 tests, vaccinations and immunity through recovery that provide security often only up to a given probability (for example p of at best 95%), EUIs could leverage a back to office strategy that is permissive/tolerant towards individuals without known or with insufficient vaccination or test status up to given threshold (e.g. $100\% - p = 5\%$). This approach can help to reduce the pressure on a small minority that does not provide consent.
- Only informed consent is valid consent. Consequently, data subjects must receive easy to understand and concise information on the envisaged processing.

To comply with the right of access, the data subject shall be given the tools to access their health record, in particular if the record is embedded in a QR code, NFC tag or otherwise encoded or not readable.

7. CONCLUDING REMARKS

Given the current voluntary nature of COVID vaccinations in the EU, and without prejudice to the use of EU Digital COVID Certificates where appropriate, the EDPS considers that there is no legal basis for EUIs to request proof of vaccination status from individuals. EUIs may however collect aggregated, anonymised staff vaccination data to support workplace risk assessments. In this respect, the analysis of aggregate staff vaccination data may be an essential first step before considering more privacy-intrusive measures.

The EDPS recalls that EUIs must undertake a careful necessity and proportionality assessment to justify the implied interference with individuals' fundamental rights to private life and data protection.

Processing of data related to antigen testing would only be justified in specific employment settings where the risk of exposure by staff would be particularly high and where the working environment makes it impossible to resort to less intrusive measures.

Processing of EU Digital COVID Certificates in the workplace should only be considered once EUIs have discarded other alternative, less privacy intrusive measures and according to strictly defined parameters. Use should only continue as long as the exceptional circumstances justifying this processing persist and should be subject to regular reassessment.