



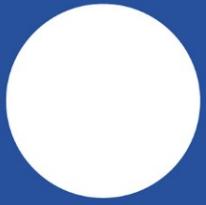
EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data
protection authority



Workshop on access control

EDPS-DPO meeting 14 December 2021

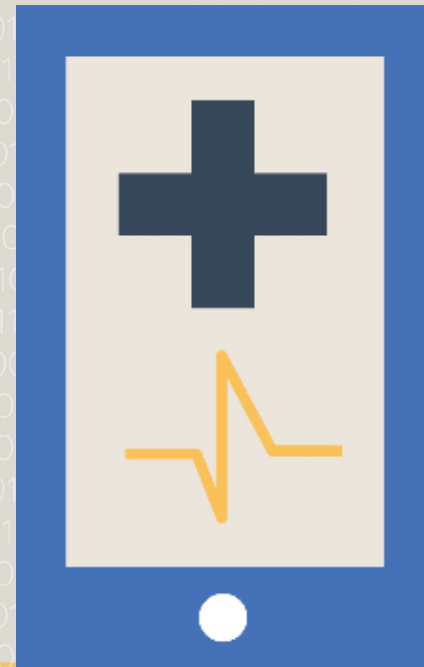


DISCUSSION POINTS

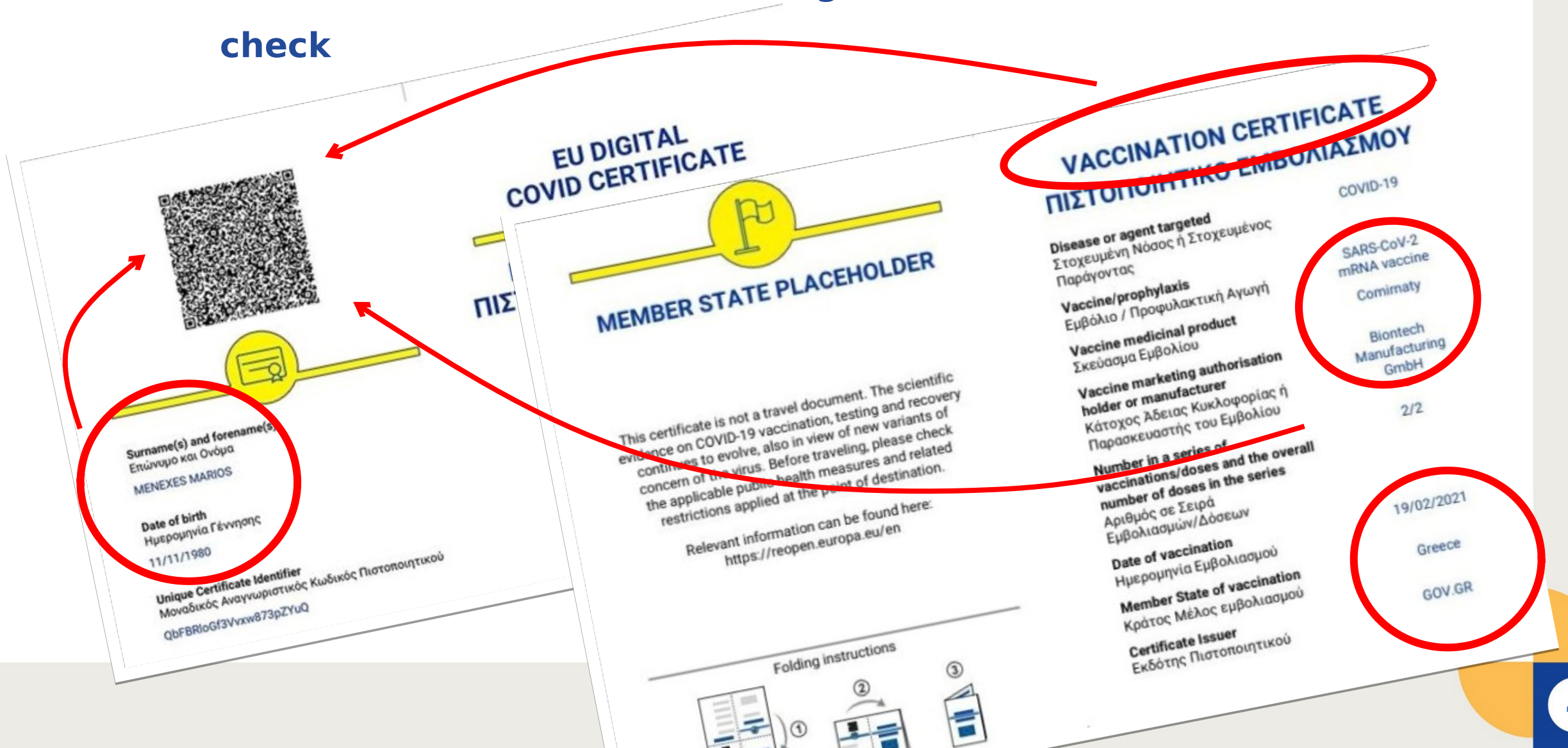
- **Digital verification with QR-scanning apps**
- **Interplay between national legislation and EUJs' privileges and immunities**

Digital verification via QR-scanning apps

- **Manual vs. digital verification**
- **Data controllership**
- **DPIA**



Personal Data accessible during manual Covid Certificate check



The image shows two overlapping EU Digital COVID Certificates. Red circles and arrows highlight specific fields where personal data is accessible during a manual check.

Left Certificate (EU Digital COVID Certificate):

- QR Code:** A large QR code is visible at the top left.
- Member State Placeholder:** A yellow circle with a flag icon and the text "MEMBER STATE PLACEHOLDER" is highlighted.
- Personal Data Fields (circled in red):**
 - Surname(s) and forename(s) / Επώνυμο και Ονόμα: MENEXES MARIOS
 - Date of birth / Ημερομηνία Γέννησης: 11/11/1980
 - Unique Certificate Identifier / Μοναδικός Αναγνωριστικός Κωδικός Πιστοποιητικού: QbFBRioGf3Vnxw873pZYuQ

Right Certificate (Vaccination Certificate / ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΕΜΒΟΛΙΑΣΜΟΥ):

- Title:** VACCINATION CERTIFICATE / ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΕΜΒΟΛΙΑΣΜΟΥ (circled in red)
- Disease or agent targeted / Στοχευμένη Νόσος ή Στοχευμένος Παράγοντας:** COVID-19
- Vaccine/prophylaxis / Εμβόλιο / Προφυλακτική Αγωγή:** SARS-CoV-2 mRNA vaccine
- Vaccine medicinal product / Σκεύασμα Εμβολίου:** Comirnaty
- Vaccine marketing authorisation holder or manufacturer / Κάτοχος Άδειας Κυκλοφορίας ή Παρασκευαστής του Εμβολίου:** Biontech Manufacturing GmbH
- Number in a series of vaccinations/doses and the overall number of doses in the series / Αριθμός σε Σειρά Εμβολιασμών/Δόσεων:** 2/2
- Date of vaccination / Ημερομηνία Εμβολιασμού:** 19/02/2021
- Member State of vaccination / Κράτος Μέλος εμβολιασμού:** Greece
- Certificate issuer / Εκδότης Πιστοποιητικού:** GOV.GR

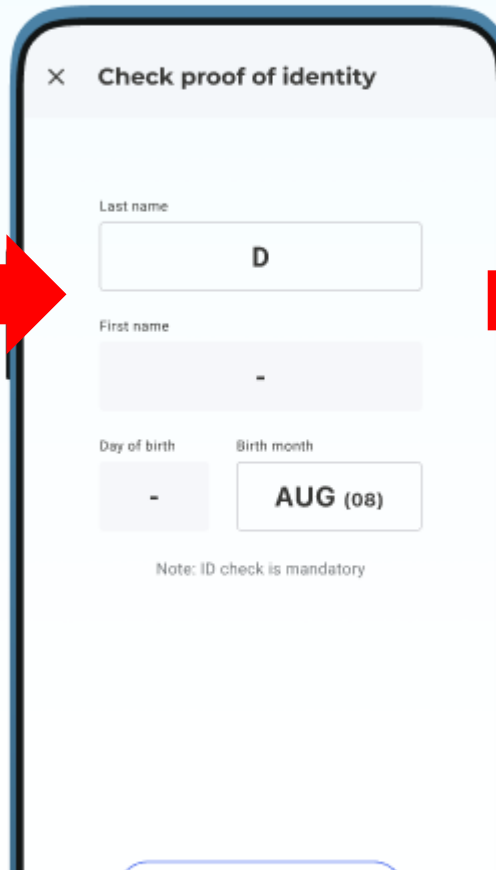
Folding instructions: 1, 2, 3

Personal Data accessible with Covid Certificate QR Code

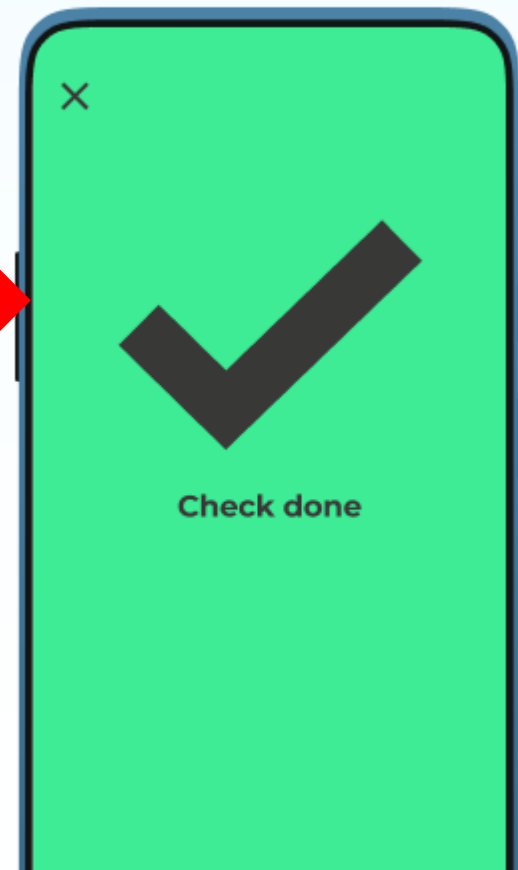
ver Scan the visitor's QR code



Check if the details in the QR code are the same as those on their identity document

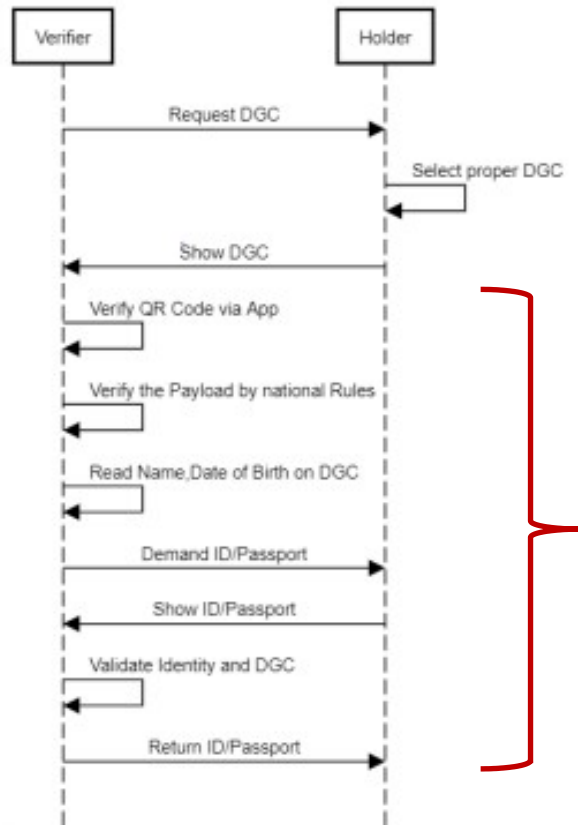


Are the details correct? Then the visitor is allowed to enter



How does digital verification work?

Offline DGC Verification



Processing of personal data locally on the app



- Name & date of birth
- Certificate type (v, t, r)
- Vaccination certificate details (type of vaccine, date, etc.)
- Test certificate details (type of test, date, etc.)
- Recovery certificate details (validity, etc.)

Source: EC Green Pass technical specs (apps)

https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_v4_en.pdf

Source: EC Green Pass technical specs (schema)



Comparison

	Manual Verification	QR Code Verification
Included Dataset	Entire dataset	Entire dataset
Requires additional ID verification	Yes	Yes
Visible Dataset	Entire dataset	validity and parts of) name, birthdate
Personal Dataflows	None	Local processing within the verification app (offline)
Technical safeguards	None	Digital signature verification, Expiry verification
Design across countries	Various	Standardised
Fake fabrication	Scanner/phone camera + MS Word	Hack or bribe doctor/pharmacy/health ministry
Processing of personal data	No	Yes



Who is the controller ?

Who is the controller of the processing that takes place in the mobile application: the EUI or the national government that has set-up the mobile app concerned?

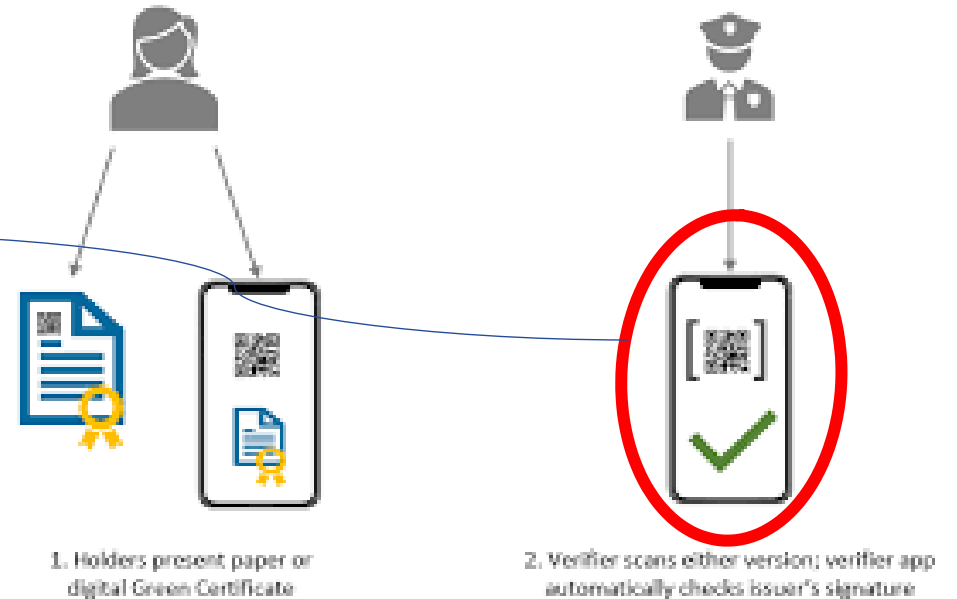
- **Article 10(6) Regulation 2021/953**

“The authorities or other designated bodies responsible for issuing the certificates referred to in Article 3(1) shall be considered to be controllers as defined in point (7) of Article 4 of Regulation (EU) 2016/679.”



Who is the controller ?

- In the light of what scanning a QR code technically implies (signature check, local storage on EUI device, local validation of certificate) EUIs are processing personal data as controllers for the purpose of access control.





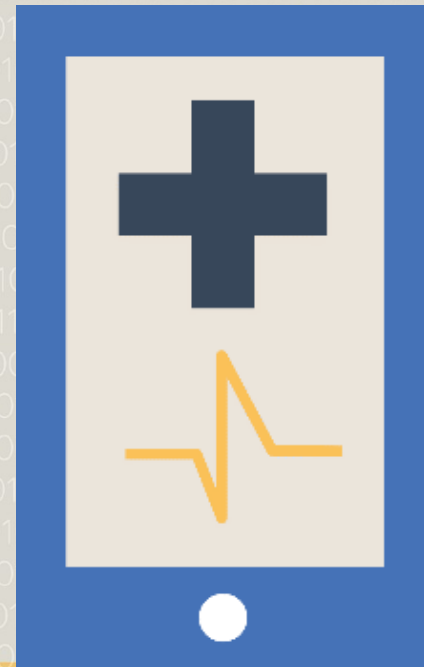
Data protection risks

What are the data protection-related risks of the use of a digital verification app?

Do we need a DPIA?



Interplay between national law and EUIs' privileges and immunities





To what extent is an EUI obliged to follow national law if the latter mandates employers to impose COVID certificate checks?

- Look at Seat Agreement
- Do EUIs need to conduct a necessity and proportionality assessment? If yes, to which extent?



Other points for discussion

- Differentiated application of access controls to staff & non-staff?
- Necessity and proportionality assessment
- Reimbursement of costs of tests (relevant for the necessity and proportionality assessment of the measure)
- others?



Differentiated application of access controls to staff & non-staff?

- How to define ‘non-staff’?
- Interplay between EU rules and national legislation (e.g. external contractors covered by national law?)
- **Necessity and proportionality:** what compelling reasons might justify a differentiated application of controls?
- **Controls for visitors only?** Necessity and proportionality considerations will be specific to each EUI: no. of visitors, nature of visits (e.g. individuals/small groups or larger events)?

“The legal basis for processing EU Digital COVID Certificates of non-staff could be similarly established by Article 1e(2) of the Staff Regulation 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” (Return to Workplace Guidance)



Necessity / proportionality: Criteria ?

How to carry out the necessity and proportionality assessment that would precede COVID certificate checks as access controls? What criteria, thresholds?





Necessity

What do the EDPS Guidelines suggest ?

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.



Who reimburses tests?

Current **JSIS** rules:

“IF prescribed by a doctor AND carried out by an approved medical provider Covid-19 tests will be reimbursed”

<https://myintracomm.ec.europa.eu/coronavirus/Pages/faq.aspx#healthcareandtesting>

Costs of tests for unvaccinated staff should be factored into proportionality assessment



DPOs' relevant questions

- (...)
- (...)
- (...)



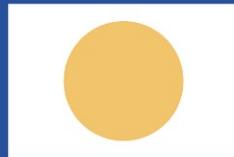
Reporting

1. Key messages from EDPS
2. Experience & challenges in EUIs
3. Best practices & next steps



EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data
protection authority



@EU_EDPS



European Data
Protection Supervisor



EDPS