Question for written answer E-005053/2021/rev.1
to the Commission
Rule 138
Tineke Strik (Verts/ALE)

Subject: Privacy and cybersecurity concerns regarding the EU Digital COVID Certificate

Fraudulent COVID-19 certificates are reportedly on offer online in France, Poland and North Macedonia, among others. Moreover, in the Netherlands, facial recognition software is reportedly being linked to COVID-19 certificates to enter festivals. COVID-19 certificates issued by Togo and Singapore contain extra data fields on the certificates, such as social security number or gender, but the addition of these data fields is prohibited at EU level under the Digital COVID-19 Certificate Regulation and the limitative list of data fields in its annex.

1. Does the Commission have information on whether the issuance of fraudulent certificates is caused by fraudulent employees at issuing authorities, and whether the abovementioned states have revocation mechanisms in place (revocation lists using the unique certificate identifier) to ensure that these fraudulent certificates can be revoked, or if the circulation of fraudulent certificates is caused by cybersecurity issues around the public key infrastructure, which would require the private keys to be revoked?

2. What is the Commission doing to assess, promote and guarantee the highest privacy standards and data minimisation when the EU certificates are used in Member States?

3. How is the recognition and acceptance of these certificates reconcilable with the Digital COVID-19 Certificate Regulation and in line with the principle of data minimisation?