Guidelines on the data protection aspects related to the collection of employees' COVID-19 vaccination status

Published on 29th April 2021

Information and Data Protection Commissioner

CONTENTS Page

1. Introduction

This guidance is intended for employers based in Malta which act as controllers ('**employers'**) and intend to collect information about the COVID-19 vaccination ('**vaccine'**) status of their employees ('**vaccination status'**).

Information about the vaccination status is **data concerning health**, which under the GDPR (Art 9.1) constitute a **special category of personal data**. By nature, special categories of personal data are considered sensitive and merit enhanced protection and safeguards.

Within this context and taking into account that a **risk-based approach** must be adopted, employers which are desirous to collect information about the vaccination status shall conduct an **assessment** on the impact of the perspective processing activities. This is required to ensure adherence to the **data protection principles** of the GDPR (Art. 5) and overall compliance with data protection law. It is remarked that such assessment shall be conducted ***prior to*** the commencement of the processing operation.

Employers may refer to the guidance below, which explains how the data principles of the GDPR should be assessed whilst carrying out such assessment. Employers shall also keep in mind that, by virtue of the **principle of accountability**, they shall be responsible for and be able to demonstrate compliance with the data protection principles in their capacity of controllers.

It has to be remarked that in the event that, as a result of the aforementioned assessment, employers establish that the processing is likely to result in a **high risk** to the rights and freedoms of natural persons, then they are bound to carry out a fully-fledged **data protection impact assessment**, in accordance with the GDPR (Art. 35).

2. Lawfulness, fairness and transparency (GDPR, Art. 5.1.a)

2.1 Lawfulness

It is generally prohibited to process data concerning health (GDPR, Art. 9.1), unless an exemption applies (GDPR, Art. 9.2). In the employment context, the following exemptions may be appropriate:

i.	**the preventive or occupational medicine condition** (GDPR, Art. 9.2.h).

This condition is two-fold, and requires that the following conditions be fulfilled at the same time:

a. the purpose(s) for the processing shall be clearly selected amongst: preventive or occupational medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services; and
b. Union or Member State law or the contract with health professional subject to an obligation of secrecy on which the processing is founded are clearly individuated and documented;

ii.	**the public health condition** (Article 9.2.i).

For this legal basis to apply, the following requirements must co-exist:

a. the reasons for processing information must be identified in the **public interest** in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.
b. Union or Member State law must be in place to provide for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy. Such legal act must be clearly individuated and documented.

As a general rule, **consent** does not apply to situations where there is an imbalance of power between the controller and the data subjects, such in an employer-employee relationship. In the employment context, unless the circumstances of the case provide otherwise, consent is not considered to be **freely given** and thus does not represent a valid legal basis.

2.2 Fairness

Employers must make sure that by processing information about the vaccination status they do not engage in any potential **unfair, discriminatory or otherwise unjustified treatment** of employees. In the event that employers assess that the collection of the vaccination status is likely to produce negative consequences for employees, such as for example **infringement of human** and / or **fundamentals rights**, then the envisaged processing operation runs contrary to the principle of fairness and should not be carried out.

To conduct this assessment, employers should take into account, for example that:

i.	due to their age, health status or profession, certain individuals have been given priority in the vaccine distribution program. Therefore, other individuals may not have been yet vaccinated at the time of collecting the vaccination status for reasons over which they had no control; and
ii.	the vaccine is voluntary. Hence, individuals have the right to decide whether to take it or otherwise, and they should not be prejudiced or otherwise discriminated for their choice in this respect.

2.3 Transparency

Employers must ensure that employees are duly informed about the processing of information about their vaccination status in the manner prescribed by the law. This is to ensure that **full transparency** is maintained during the course of the processing activity and that the employees remain in **control** of their personal data.

This means that employers shall:

i.	draft and deliver to the employees data protection notices prepared in compliance with the GDPR (Art. 13 or Art. 14, for example in case the information is collected by a medical professional acting as processor); a read-and-sign approach is generally advisable; and
ii.	ensure that the information contained within such notices and directed to employees is provided free of charge, it is concise, easily accessible and easy to understand, using clear and plain language (GDPR, Art. 12).

3. Purpose limitation (GDPR, Art. 5.1.b)

The principle of purpose limitation establishes that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Employees shall assess and be able to demonstrate that they have a **clear, lawful compelling reason** to process their employee's vaccination status. In essence, employers can collect this information only in case they cannot achieve the same purpose without collecting the same information, or in a less intrusive manner. Hence, employers shall clarify and duly document what they intend to achieve by collecting information about the vaccination status *before* any concrete processing operation is discharged.

4. Data minimisation (GDPR, Art. 5.1.c)

Once determined the purpose(s) for processing information about the vaccination status, employers shall then assess what information is **adequate, relevant and limited** to what is necessary in relation to such purpose(s). This is of utmost importance in connection with the **fiduciary obligation** which exists between the controller and the data subjects.

When feasible, employers may consider collecting information about the vaccination status from employees without collecting copies of actual medical certificates, if not strictly necessary. Such key information may be combined with minimum identifiers to single out the employee concerned; any supplementary or additional information which is not required to conduct the processing operation and to achieve the pre-defined purpose(s) of such activity shall not be collected.

5. Accuracy (GDPR, Art. 5.1.d)

Taking into account that obsolete data has no business value and could even result harmful, employers shall commit to keep the information they process about the vaccination status **accurate and up-to-date** and to rectify or erase without delay information which is inaccurate.

6. Storage limitation (GDPR, Art. 5.1.e)

Having defined the lawful ground and the purpose(s) for collecting the vaccination status, employers should establish for how long the information collected is necessary to serve to such purpose(s). Once that is established, employers should ensure that information about the vaccination status is kept in a form which permits identification of the employees only for the duration of the previously designated period.

7. Integrity and confidentiality (GDPR, Art. 5.1.f)

Giving due regard to the sensitivity of information about the vaccination status of employees, employers should assess the **security risk** posed by processing such information. After that, employers should select and implement **appropriate technical and organisational measures** to address the encountered risks. These measures may involve the mitigation, transfer, avoidance or retention of risks, and may include, for example, the implementation of the following controls:

i.	only authorised and designated individuals within the organisation should have the right to access information about the vaccination status. These rights are to be assigned on a need-to-know basis. As a consequence, in structured organisations, only certain individuals within certain departments (ex. HR) shall be entitled to process the information about the vaccination status;
ii.	such designated individuals should be made aware of the sensitivity of the information they are entrusted with, and should be instructed on how to report or escalate any personal data breach which may occur to such data;
iii.	information about the vaccination status should be kept confidential, stored in a secure environment and kept segregated from other information about the same individual; and
iv.	at the expiry of the retention period, the information (and any copy thereof) should be securely disposed of in an irreversible manner.