EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

March 2022

Report

Survey on COVID-19 related processing activities by EUIs

edps.europa.eu

Executive Summary

This report presents the findings of a survey conducted by the EDPS in 2021 of the Union institutions, bodies, offices and agencies (EUIs), regarding the processing activities and IT tools they have used to ensure business continuity during the COVID-19 pandemic and compliance thereof with Regulation 2018/1725 ('the Regulation'). The report comprises three parts: new processing operations implemented by EUIs, IT tools implemented or enhanced by EUIs to enable telework, and new processing operations implemented by EUIs in charge of public health-related tasks.

Part one of the report focuses on the main new processing operations introduced by EUIs in response to the pandemic: body temperature checks, manual contact tracing, COVID-19 tests and/or handling of results, and monitoring presence on EUI premises. The survey revealed that EUIs predominantly introduced 'basic body temperature checks', which, in contrast to automated checks, do not involve personal data processing. The EDPS welcomes this, and reminds EUIs that do employ automated checks to provide for meaningful human involvement. Regarding legal basis, EUIs erroneously relied on Articles 5(1)(b) and (e) of the Regulation. This was a persistent issue across all processing operations reported. Notably, for Article 5(1)(b) to apply, an EU law must specifically oblige the EUI to carry out the processing, and Article 5(1)(e) must concern interests essential to a person's life. The manual contact tracing operations reported appear largely compliant. That said, few EUIs conducted a DPIA for their processing despite the presence of several criteria triggering this, and few supplemented the lawfulness of processing targeting non-staff members with an executive decision providing for measures to protect the rights and freedoms of the data subject, as would be appropriate.

Regarding COVID-19 testing and/ or handling of results, the EDPS welcomes the fact that processing was mostly voluntary. The EDPS also notes that external contractors, which EUIs frequently used to carry out testing, should act as processors. In such as relationship, EUIs remain accountable for defining retention periods and should verify the deletion of data by contractors. Monitoring presence in EUIs' premises was the largest new processing operation reported. The EDPS identified no significant issues here, aside from a relatively low DPO involvement, considering that DPOs should be involved in all issues concerning personal data protection. Finally, EUIs reported on a variety of other new processing operations. These most commonly included processing related to COVID-19 vaccination campaigns, and access control measures other than body temperature checks and the monitoring of presence.

EUIs introduced and/ or modified a broad range of IT tools to ensure consistency in times of telework for a diverse set of specific purposes. These included tools to organise meetings and conduct selection procedures (new tools) and to introduce remote access features (modifications). Given the fact that several of the same tools were used by EUIs to ensure business continuity, the EDPS encourages EUIs to develop synergies to jointly negotiate data protection clauses with contractors.

Only one EUI reported that it had implemented COVID-related processing activities as part of its core business, and from the information made available, the EDPS identified no specific risks.

1. INTRODUCTION

A number of Union institutions, bodies, offices and agencies (EUIs) have implemented new processing operations to help to prevent against the spread of COVID-19 among their staff and visitors. Moreover, the COVID-19 outbreak forced many EUIs to switch their operations almost exclusively to telework, and the need for teleworking tools to maintain activities has grown dramatically in an extremely short timeframe. Finally, some EUIs have started carrying out new processing activities as part of their core business missions in public health.

In December 2020, the EDPS launched a survey on COVID-19 related processing activities by EUIs. With this survey, the EDPS aimed to map the processing activities and tools used by EUIs to ensure business continuity in times of COVID-19 and to gather information as to how EUIs comply with the data protection requirements under Article 8 of the Charter of Fundamental Rights of the European Union (the Charter) and Regulation 2018/1725[1] (the Regulation).

This report presents the main results of the survey, as well as the resulting EDPS' recommendations for EUIs. The recommendations cover mainly the following topics: lawfulness, records of processing operations, individuals targeted, categories of personal data processed, Data Protection Impact Assessments (DPIAs), DPO involvement, duration and review of the processing operations.

Beyond the report, the EDPS will use the survey's results to identify topics that may deserve specific guidance or that should be revisited. This would add to the orientations on the Reactions of EUIs as employers to the COVID-19 crisis (15 July 2010) on Body Temperature Checks (1 September 2020), on Manual contact tracing (2 February 2021) and the guidance on Return to the Workplace (9 August 2021). The EDPS shall also rely on the survey to conduct targeted audits and investigations.

The report reflects the state-of-play at the responding EUIs in late April 2021. At that time, vaccination was in its early stages, the EU-COVID-19 certificate was still in limbo, and telework was the rule for most EUIs. The dynamic evolution of the COVID-19 pandemic means EUIs must continually adapt their processes, and this report aims to support them in what appears now to be a long-lasting challenge, which will likely continue to have an impact even after the pandemic's end.

Our overall objective is to ensure that current and future processing operations related to or generated by the COVID-19 outbreak are compliant and respect people's right to privacy and data protection.

The EDPS is thankful to all stakeholders involved in replying to the survey and providing comprehensive feedback, and in particular the Data Protection Officers (DPOs).

---

[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, pp. 39–98.

2. OVERVIEW AND METHODOLOGY

The survey[2] was divided into three main parts:

- new processing operations implemented by EUIs following the outbreak of COVID-19;

- IT tools or solutions implemented or enhanced by EUIs to ensure business continuity in times of telework; and,

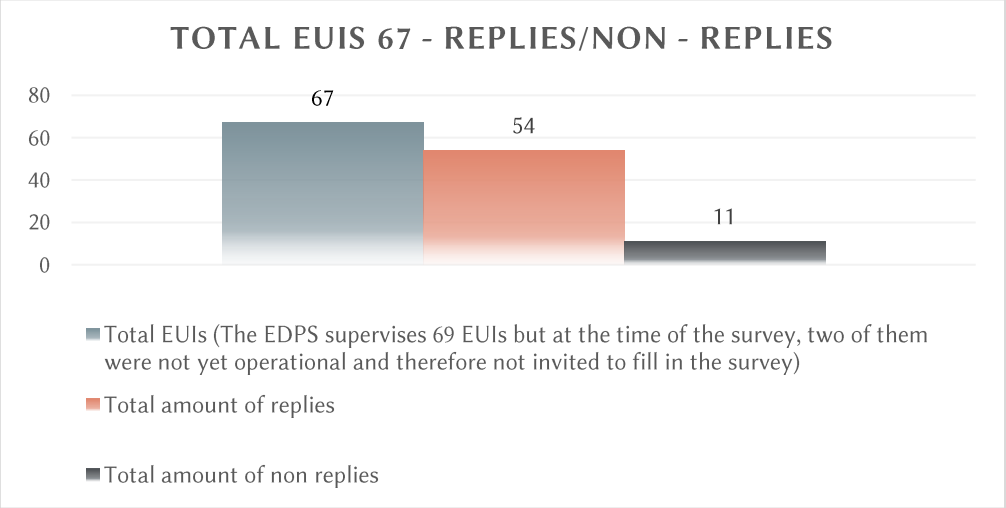
- new processing operations implemented by EUIs in charge of public health related tasks.

Each part included a broad range of questions. To ease the analysis of the results and the identification of patterns across the EUIs, the EDPS designed the survey so that the respondents did not always have the possibility to provide additional information in free text fields. At the end of the survey, EUIs were, however, given the opportunity to bring other matters to the EDPS' attention in the context of COVID-19 related data processing operations ("Any Other Business").

EUIs were invited to provide their replies by 31 March 2021, extended until 15 April 2021.

Out of 69 EUIs that are currently under the supervision of the EDPS, 56 responded to this survey by this date[3]. Some EUIs that cooperate closely submitted joint replies[4]. For this reason, the total number of replies received are 54. For the purpose of presenting statistics in this report, the EUIs that submitted one joint reply will be treated as one single EUI. Two of the 11 EUIs that did not respond to the survey were not yet operational at the time the survey was launched[5].

Table 1



[2] The survey questionnaire is appended to this report (Annex 1).
[3] The list of respondents is appended to the report (Annex 2)
[4] The European Investment Bank (EIB) and the European Investment Fund (EIF); the European central Bank (ECB) and the European Systemic Risk Board (ESRB).
[5] The European Public Prosecutor Office (EPPO) and the European Labour Agency (ELA).

The 54 replies referenced more than 300 processing operations or IT systems, which we analysed one by one, as follows:

The survey pre-identified four main new processing operations that EUIs may have implemented as part of their return to work strategy: body temperature checks, manual contact tracing, COVID-19 testing and/or handling of results, and monitoring presence in the EUI premises. The survey included specific questions to identify how EUIs process personal data in the context of these four processing operations. In this regard, the replies received by the respondents are, in principle, consistent, and transversal conclusions have been drawn.

The other processing operations reported proactively by EUIs are more diverse and vary from vaccination programmes to IT equipment delivery, online training or remote selection. We grouped them based on their similar features, identified patterns and drew conclusions. EUIs listed some processing operations without further detail, either under the "Any Other Business" section, or in free text fields elsewhere in the survey. As a result, the EDPS could not draw conclusions from these responses, which we accounted for only in the statistics.

The results of the survey on new or modified IT tools[6] provide a comprehensive mapping of these tools. They show the diversity of the tools and the different purposes for which they have been deployed, as well as the various underlying processing operations that take place by means of their use.

Generally, the report reflects the results that we believe are both relevant and helpful to share with our stakeholders and the public in general. This does not preclude the EDPS from following up on all results, of which we keep track in our records.

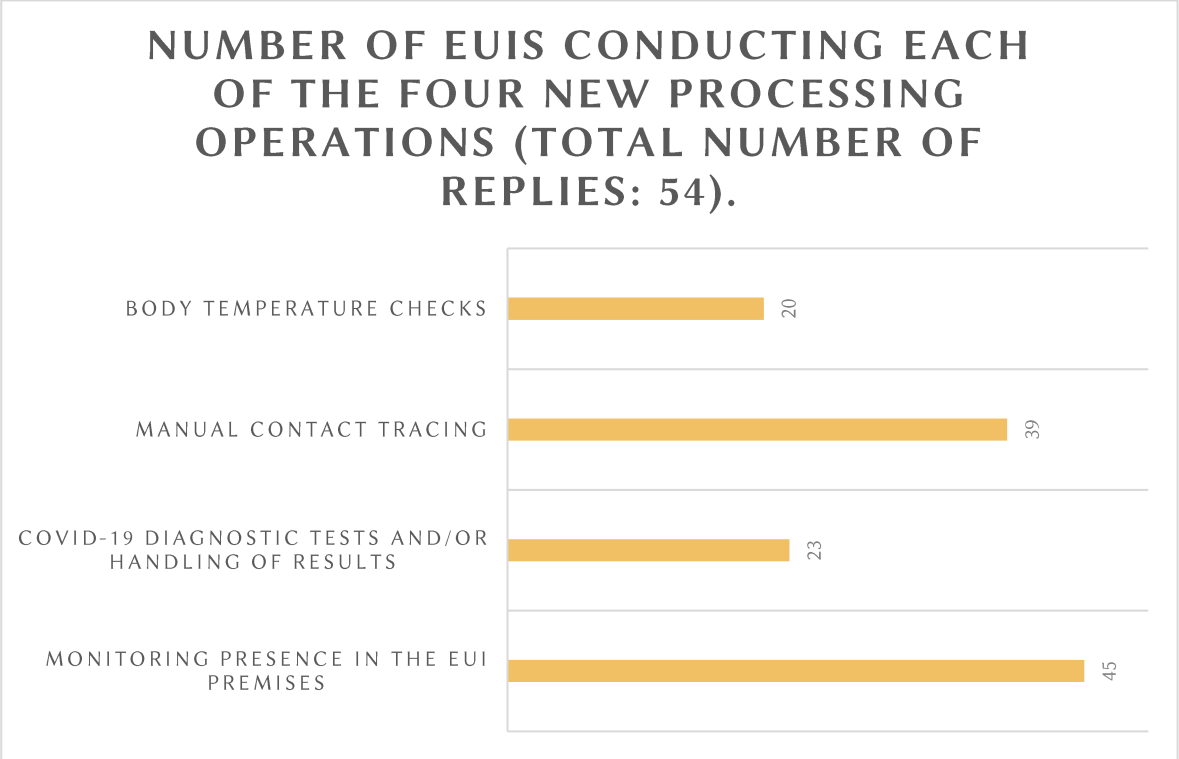
The report deals extensively with the main new processing operations generated by the pandemic (Section 3), and provides an overview of some additional processing operations (Section 4) and the use of IT tools in times of telework (Section 5). We also say a few words about the core business processing activities reported by one EUI in charge of public health (Section 6). In each section, the EDPS reports on the main results, conducts a legal analysis and makes recommendations where relevant.

[6] We left deliberately outside the scope of the survey the existing IT tools, as the goal was to identify the changes generated by the pandemic.

3. NEW PROCESSING OPERATIONS GENERATED BY THE PANDEMIC

In the survey form, the EDPS pre-identified four potential new processing activities. The below graph presents the results regarding the number of EUIs that implemented each of these.

Table 2



3.1. Body Temperature checks

Almost half of the responding EUIs (20 out of 54) introduced body temperature checks to filter access to their premises.

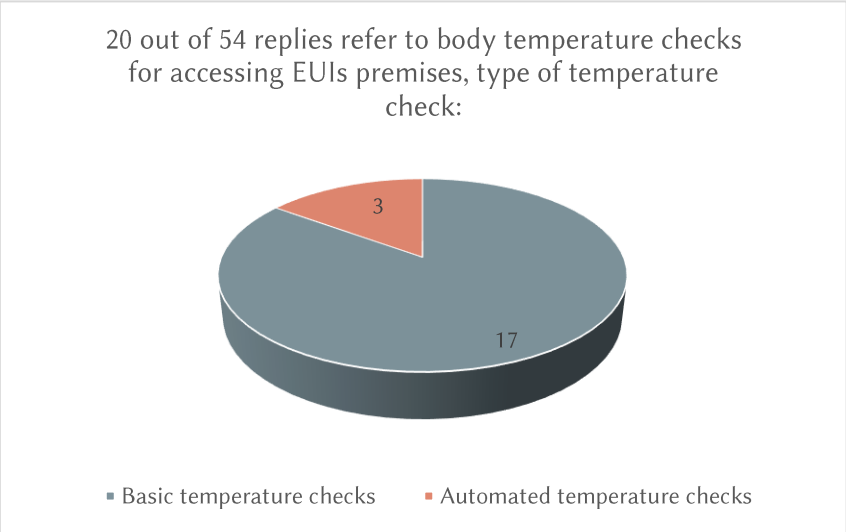
The majority of these EUIs (17 in 20) indicated that they operated 'basic temperature checks.' Basic temperature checks are designed to measure body temperature only, are operated manually, and are not followed by registration, documentation, or any other processing of an individual's personal data. Because basic temperature checks do not involve the processing of personal data, they are in principle not subject to the scope of the Regulation, provided that they are not followed by registration, documentation or other processing allowing to link such temperature checks to individuals.[7] Nonetheless, some EUIs filled in the survey and treated the activity as falling under

[7] EDPS Orientations on body temperature checks of 20 September 2020, pp. 4-5.

the scope of the Regulation, and the results presented in this section of the report should be read in light of this.

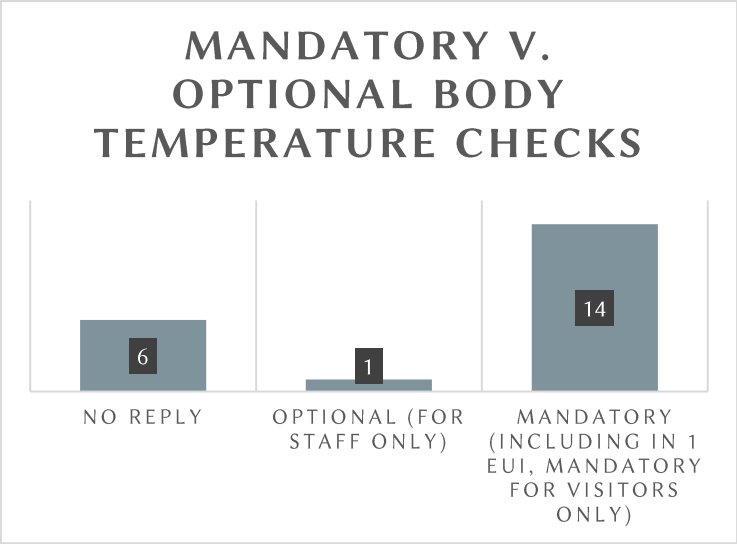
Three EUIs operated automated temperature checks using thermal scanning devices or thermographic cameras (either alone, or in combination with basic temperature checks). The use of automated digital means to detect body temperature falls under the scope of the Regulation, even when no registration/recording of information takes place, as these checks involve the processing personal data 'wholly or partly by automated means' within the meaning of Article 2(5) of the Regulation[8].

Table 3



As shown in the graph below, the majority of temperature checks were mandatory. This included all three automated temperature checks.

Table 4



[8] EDPS Orientations on body temperature checks of 20 September 2020, pp.5-6.

3.1.1. Main points of interest on body temperature checks

LAWFULNESS AND LEGAL BASIS

Article 5 of the Regulation provides for various grounds for lawfulness of data processing operations while Article 10 includes extra-requirements when special categories of data, such as health data, are at stake.

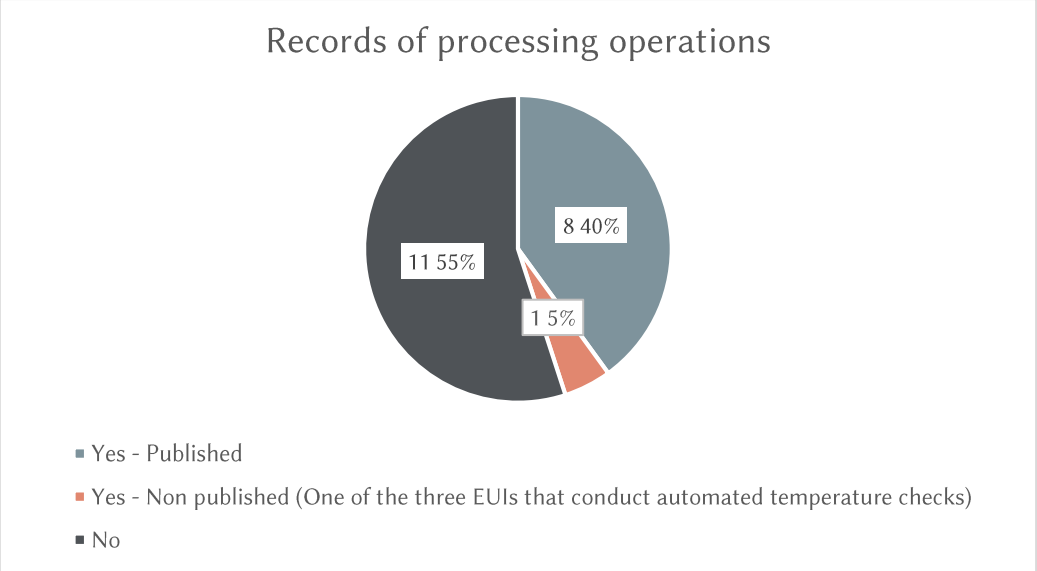
The majority of the EUIs relied on Article 5(1)(a) (task in the public interest), Article 5(1)(b) (legal obligation), Article 10(2)(b) (employment law) and/or Article 10(2)(i) (public interest in the area of public health) as a lawful ground for body temperature checks. A few indicated that they relied on Article 5(1)(e) or Article 10(2)(c) (vital interests of data subjects) and 10(2)(h) (preventive or occupational medicine).

Most of the EUI's rely on the Staff Regulations, notably Article 1(e)(2)[9], as the legal basis in Union law[10]. A few EUIs supplemented the lawfulness of body temperature checks with internal decisions - including one of the three EUIs that implemented automated temperature checks - while others also referred to national provisions on health and safety.

RECORDS OF PROCESSING OPERATIONS

As shown in the graph, the majority of the EUIs published a record[11] of processing operations for body temperature checks.

Table 5



[9] Article 1(e)(2) of the Staff Regulations provides that Officials 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.'

[10] A requirement under Article 5(2) of the Regulation.

[11] A requirement under Article 31 of the Regulation.

Individuals targeted, personal data processed

The categories of individuals targeted by the processing operations were staff members, visitors and external contractors intending to enter the respective buildings.

Most of the EUIs reported that they processed health data.

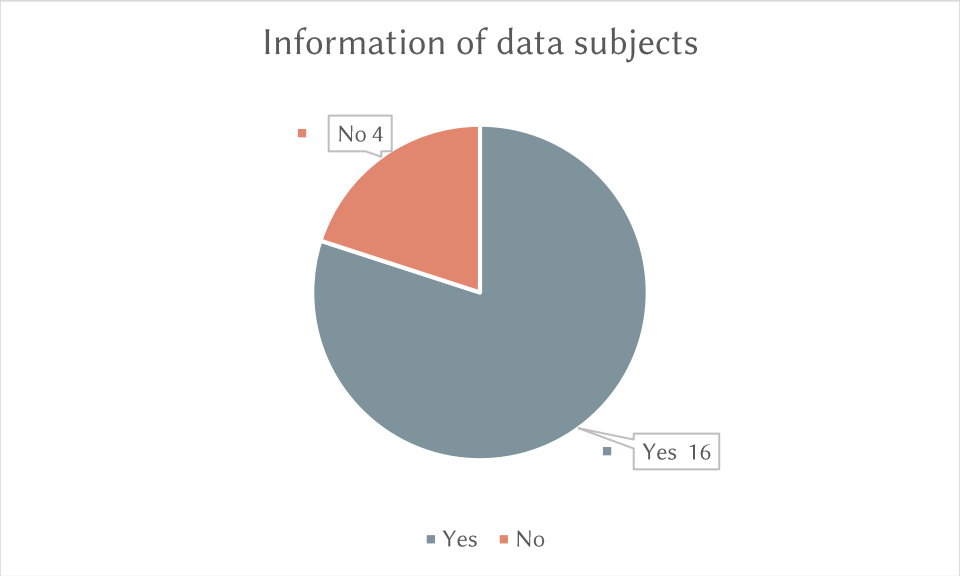
Data Protection Impact Assessments (DPIAs)

Two EUIs reported that they conducted a DPIA. The use of new technologies, processing of special categories of data on a mandatory basis, the imbalance of power between the controller and the data subject as well as the denial to grant access to the buildings in case of 'positive' measurements were listed as criteria that triggered a DPIA.

Information of data subjects

Most of the EUIs that introduced temperature checks, including basic ones, provided data subjects with information by means of publication of privacy statements on internal or external websites, and distinctive signs and information displayed at the entrances of the buildings.

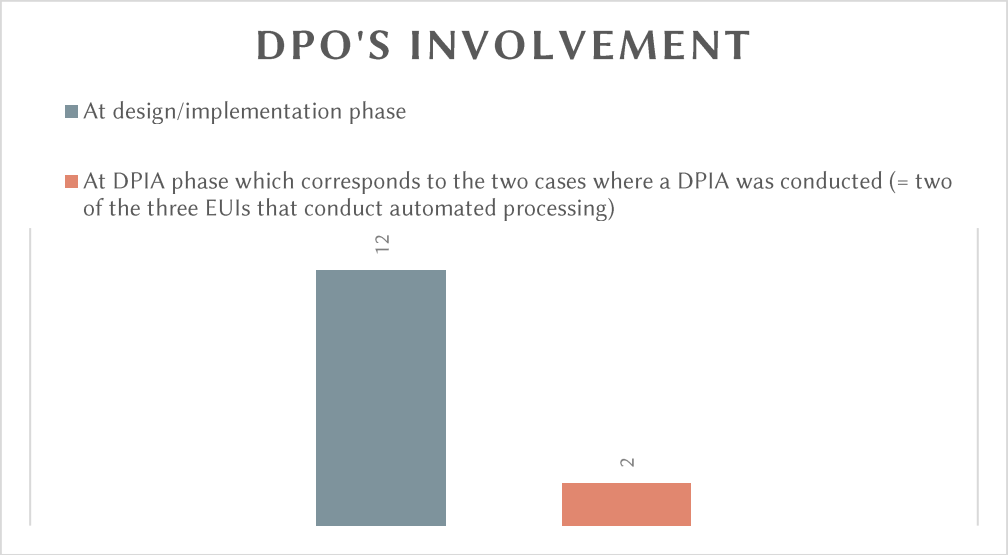
Table 6



DPO involvement

As shown in the graph, more than half of the EUIs actively involved their DPO in the context of this processing operation.

Table 7



DURATION OF THE PROCESSING

More than half of the EUIs indicated that they periodically reviewed the necessity to continue this processing operation in view of the evolution of the pandemic.

3.1.2. Legal analysis and recommendations on body temperature checks

The EDPS welcomes the fact that that the majority of the EUIs implement non-intrusive body temperature checking techniques that do not involve any processing of personal data. It is also noteworthy that in the vast majority of cases data subjects were provided with information on the temperature checks, irrespective of whether personal data was processed or not, which we welcome as well, as even basic temperature checks result in an interference into the fundamental right to private life protected under Article 7 of the Charter of Fundamental Rights of the European Union.

The EDPS has some suggestions to enhance compliance with the Regulation:

LAWFULNESS AND LEGAL BASIS

Article 5(1)(b) of the Regulation (legal obligation) applies only in cases where a legal provision laid down in Union law (and not only an internal decision of the EUIs themselves) requires EUIs to process personal data without any leeway in its implementation. This implies that the obligation itself must be sufficiently specific as to the processing of personal data it requires. However, there is no Union law provision that obliges EUIs to carry out body temperature checks. In this regard, Article 5(1)(b) is not an appropriate lawful ground for this processing operation.

Additionally, vital interests (Article 5(1)(e) and Art. 10(2)(c) of the Regulation) should be used only when the processing concerns interests that are essential for someone's life, for instance, in the context of first aid when the data subject is unconscious and hence, not capable of consenting. These lawful grounds are therefore also not appropriate.

Moreover, preventive or occupational medicine (Article 10(2)(h)) may only serve to process health data in the context of the provision of health services by health professionals[12]. Since temperature checks for the purposes of access control cannot be considered a health service, Article 10(2)(h) is not an appropriate lawful grounds.

Finally, regarding the legal basis for automated body temperature checks, EUIs should supplement the Staff Regulations with an executive decision providing for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.[13]

Use of automated tools and human involvement

The three EUIs that carried out automated temperature checks (either alone or in combination with basic temperature checks) seem to apply appropriate security and organisational measures, such as properly training the personnel in charge of the checks, abstaining from recording thermal images or carrying out a second measurement in case of 'positive' checks. However, it is not clear whether such processing provided for meaningful human involvement or not.

Notably, temperature checks applied on a mandatory basis should not be based solely on automated processing, and should provide for meaningful human involvement[14] at relevant stages of the check process. A fully automated temperature checks system would only be lawful on a voluntary basis, with the data subject's explicit consent under Article 10(2)(a) of the Regulation", which is doubtful in the employment context, both for staff members and externals that have to go to the EUIs premises for professional reasons.

Meaningful human involvement means that EUIs conducting automated checks should establish a follow-up procedure in the case of two consecutive 'positive' checks. In particular, the individual concerned should be given the possibility to benefit from a third measurement by a healthcare professional using another device. Human involvement may also mean that specific circumstances affecting the data subjects are taken into account and to allow for exceptional or compassionate decisions[15].

Duration of the processing

All EUIs implementing body temperature checks should regularly re-assess their necessity and proportionality, taking into account the evolution of the pandemic, and in particular as to the relevant of body temperature in the diagnosis of COVID-19. This includes EUIs implementing basic body temperature checks not covered by the Regulation, given the potential interference with the fundamental right to private life protected by Article 7 of the Charter.[16]

---

12 EDPS Guidelines concerning the processing of health data in the workplace by Community institutions and bodies, p. 8.
13 EDPS Orientations on body temperature checks of 20 September 2020, p 6.
14 EDPS Orientations on body temperature checks of 20 September 2020, p 6.
15 EDPS Orientations on body temperature checks of 20 September 2020, pp. 7-8.
16 EDPS Orientations on body temperature checks of 20 September 2020, p 5.

3.2. Contact tracing

On 2 February 2021, the EDPS issued orientations on manual contact tracing by EUIs in the context of the COVID-19 crisis[17]. In addition to other mitigation measures, such as teleworking, EUIs put in place manual contact tracing systems as part of their standard epidemiological toolkit. Such systems are implemented in order to trace people who have been in close contact with a person infected with COVID-19 with a view to prevent the spread of the contamination in the workplace.

The survey focused on manual contact tracing[18].

Approximately 3/4 of the EUIs (40[19] out of 54 replies), reported that they implemented manual contact tracing. The survey reveals that 29 respondents implemented manual contact tracing on a mandatory basis, nine did it on an optional basis, and one did not specify whether manual contact tracing was mandatory or optional.

3.2.1. Main points of interest on manual contact tracing

SCOPE

The vast majority of the respondents requested data subjects (mainly staff) to report on their positivity, as well on colleagues they were in contact with during the incubation period. The majority indicated that they also requested staff to report contacts with any infected persons.

Several respondents introduced manual contact tracing also for non-staff members, such as contractors or visitors to EUI premises by requesting them to report on positivity, as well as on staff members they were in contact with during the incubation period.

Manual contact tracing took place with a view to establishing lists of staff members infected or potentially infected, and where necessary of staff members who had contact with them in order to implement follow-up mitigation measures (e.g. disinfection of offices) to reduce the risk of infection of staff members.

LAWFULNESS AND LEGAL BASIS

Most of the respondents relied on Article 5(1)(a) (task in the public interest) and/or Article 10(2)(h) (preventive or occupational medicine). Other lawful grounds were also reported, as shown in the graph below.

The applicable Staff Regulations , notably Article 1(e)(2) (working conditions complying with appropriate health and safety standards) and Article 59 (management of medical leave), are the

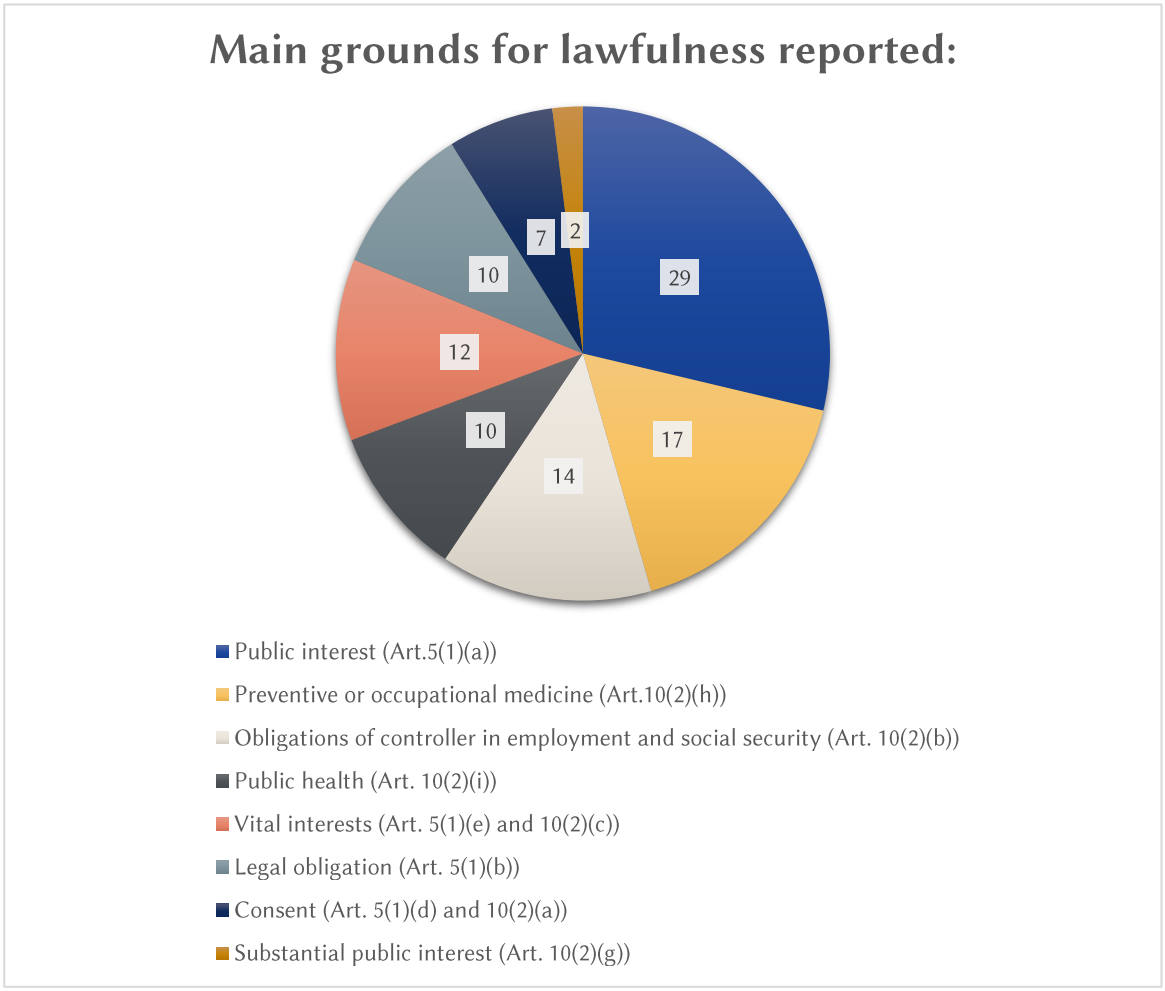
[17] The EDPS orientations on manual contact tracing by EUIs were published, while the COVID-19 survey was ongoing.

[18] Manual contact tracing should be distinguished from contact tracing with mobile applications due to its very different nature and data protection implications. An overview of the issues raised by contact tracing with mobile applications was published by the EDPS in May 2020: https://edps.europa.eu/sites/default/files/publication/20-05-08_techdispatch-tracing_en.pdf.

[19] It is to be noted that one EUI indicated that they did not conduct manual contact tracing, but pointed out that in case a staff member tests positive to COVID-19 while being present in the office up to 14 days prior to the test result, has to inform the EUI. In such an event, all staff members present in the office are informed and given further guidance, without disclosure of the name of the staff member who tested positive. The EUI in question did not provide further information on the processing at stake.

legal basis which most EUIs rely upon. Few EUIs supplemented the lawfulness of such processing with executive decisions, while others also referred to national provisions.

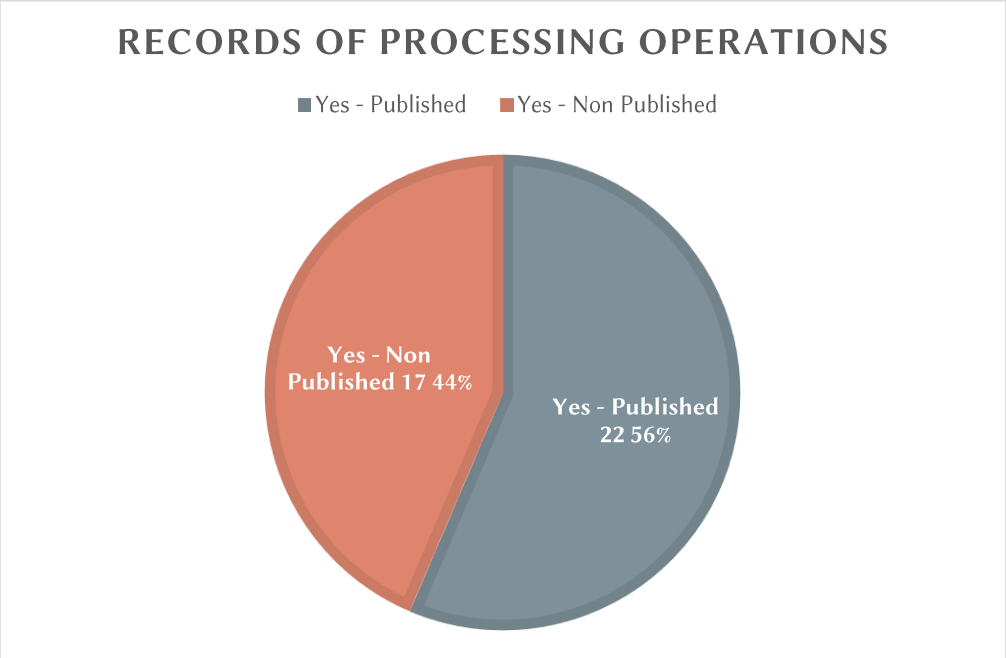
Table 8



RECORDS OF PROCESSING OPERATIONS

The majority of EUIs published a record of processing operations, as shown in the graph below:

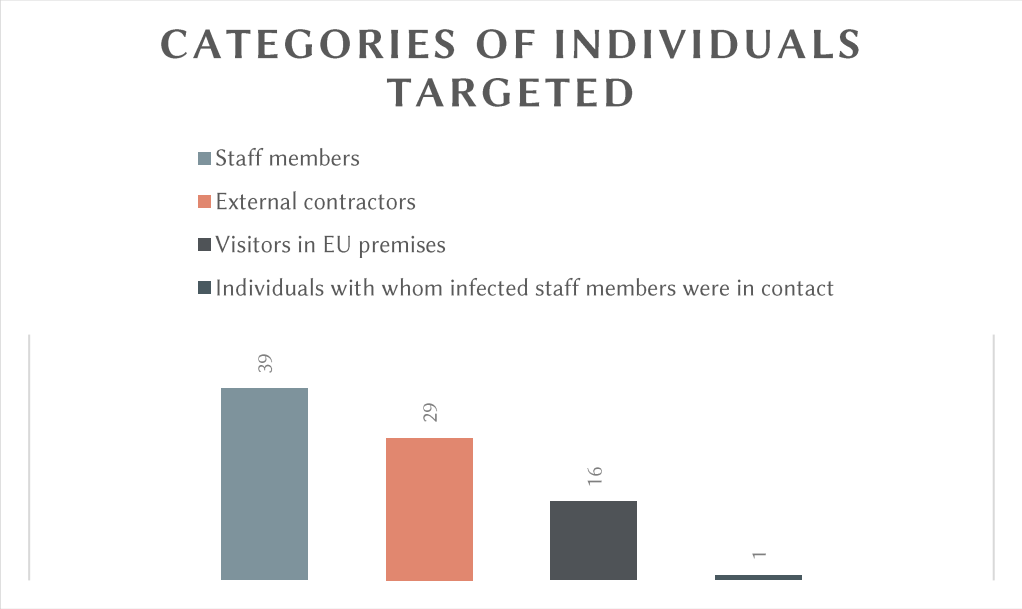
Table 9



INDIVIDUALS TARGETED, PERSONAL DATA PROCESSED

The individuals targeted by this processing operation are shown in the graph below:

Table 10

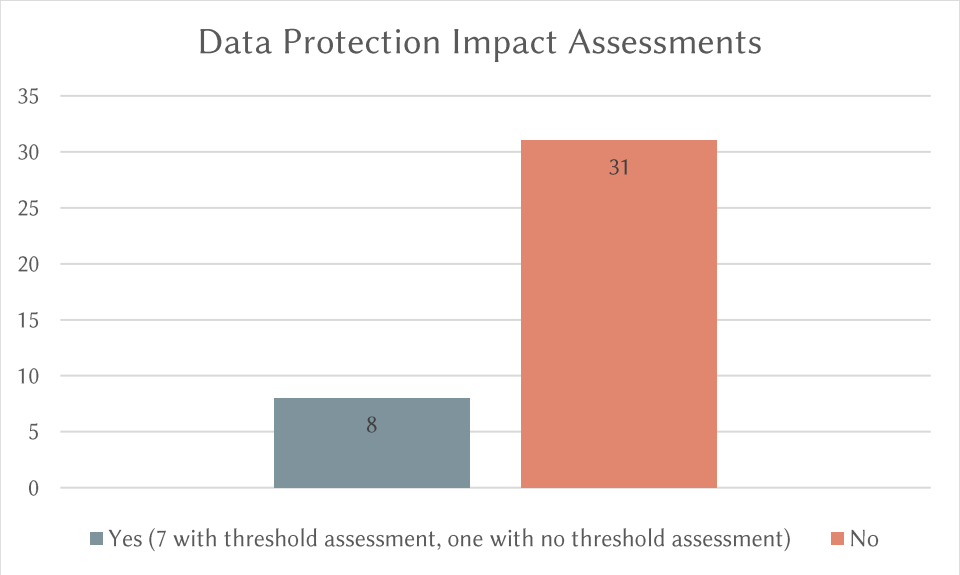


All but one EUIs that deployed contact tracing reported that they processed health data.

DPIAs

Eight EUIs reported that they conducted a DPIA or were in the process of conducting a DPIA at the time that they responded to the survey. The use of new technologies, processing of special categories of data, data processed on a large scale, and automated decision-making were listed as criteria that triggered a DPIA.

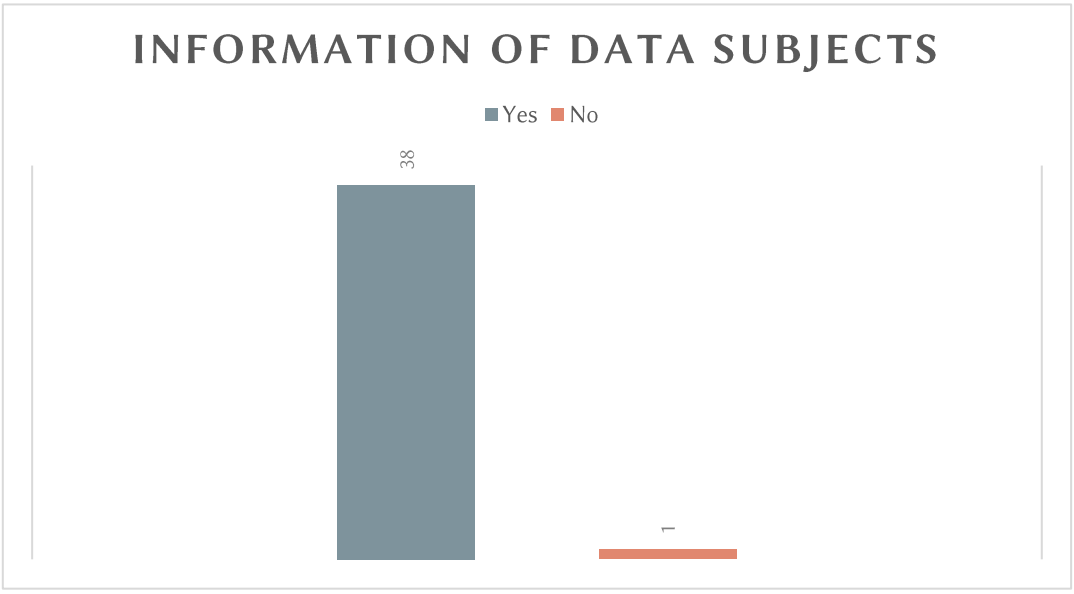
Table 11



Information of data subjects

The majority of the EUIs reported that they provided information to data subjects with regard to manual contact tracing, for example by means of publication of privacy statements on internal or external websites, e-mail communication to staff members, newsletters, and FAQs about contact tracing.

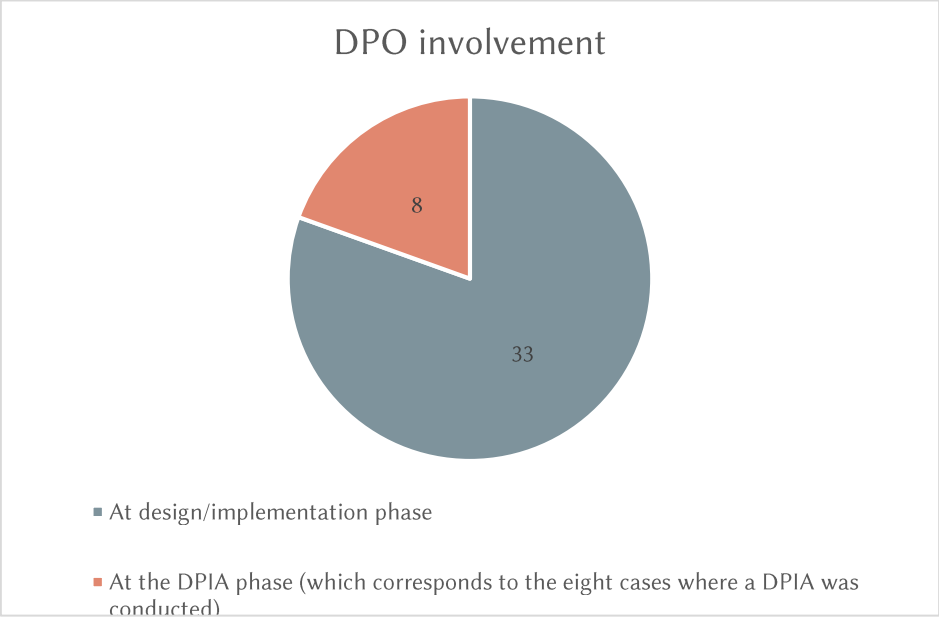
Table 12



DPO INVOLVEMENT

The majority EUIs actively involved their DPO, as shown in the graph below:

Table 13



RETENTION AND DURATION OF THE PROCESSING

The majority of the respondents reported that the processing operation was still ongoing when they filled in the survey. Concerning the applicable retention periods, a few EUIs reported that they keep data for a maximum of 14 days. However, most EUIs indicated a longer retention period or did not specify for how long personal data is kept.

More than half of the EUIs that implemented manual contact tracing, periodically reviewed the necessity to continue this processing operation in view of the evolution of the pandemic. Some EUIs introduced yearly reviews, or reviews in accordance with the applicable legislation or recommendations by the national health authorities.

3.2.2. Legal analysis and recommendations on manual contact tracing

The majority of EUIs seem to have put in place appropriate measures to ensure compliant processing of personal data in the context of contact tracing. For instance, in accordance with the data minimisation principle[20], EUIs do not process more data than necessary for the purpose of contact tracing, as, in principle, only those persons in close contact with the infected staff member are traced and monitored.

However, there seems to be some room for improvement on the following topics:

[20] Article 4(1)(c) of the Regulation.

PROCESSING OF PERSONAL DATA OF NON-STAFF MEMBERS

In accordance with Article 59(5) of the Staff Regulations, EUIs may process data of staff members who will generate a chain of contamination at the office (i.e. not members who are exclusively teleworking). They may also process data of the members of their household if the latter are suffering from a contagious disease (such as COVID-19)[21], if such information is disclosed by the staff member.

By contrast, EUIs do not have a legal basis, comparable to Article 59(5) of the Staff Regulations , to process health related data of non-staff persons who are not members of their household in its manual contact tracing operation[22]. Nevertheless, EUIs may inform these non-staff members that they have been in contact - in a work context - with a staff member who has been infected. The lawfulness of this limited processing of non-staff members' data lies in Article 5(1)(a) of the Regulation. Regarding a legal basis, Article 1(e)(2) of the Staff Regulations (working environment complying with appropriate health and safety standards) would be applicable, supplemented with an executive decision providing for suitable and specific measures to safeguard the fundamental rights and the interests of data subjects. Processing should be limited to informing the non-staff contacts and providing them with the contact details of local health authorities. EUIs must not collect any medical or health related information from non-staff members aside from the information required to contact trace their staff.

However, very few EUIs referred to the existence of such an executive decision, and several of them targeted non-staff members, such as visitors and/or or external contractors.

INDIVIDUALS TARGETED

Some EUIs reported that manual contact tracing concerned staff members "infected" or "potentially infected" by COVID-19. However, the wording "potentially infected" does not provide the necessary clarity to understand which individuals the processing aims to target. It is not clear whether "potentially infected" individuals are those who present certain symptoms and/or those who were in contact with a person who tested positive to COVID-19, etc. EUIs should ensure that they collect health data only from individuals with a confirmed COVID-19 diagnosis for the purposes of manual contact tracing[23].

GROUND FOR LAWFULNESS

Some EUIs reported that they relied on consent (Article 5(1)(d) of the Regulation) as a ground for lawfulness in the context of manual contact tracing. The targeted individuals were EUI staff members. Given the employment context of such tracing system, it is unlikely that consent would provide a valid or a relevant legal ground for the processing operation at stake, even when the internal rules in place provide that contact tracing takes place on a voluntary basis. Indeed, given the imbalance of power, even if the reporting is trust-based with no formal obligation to report, staff members may feel compelled to report their contamination.[24] Therefore, for staff members, the ground for lawfulness should be public interest (Article 5(1)(a)) and the obligations of EUIs as

---

[21] Article 59(5) covers medical leave of staff members, including 'if a member of his household is suffering from a contagious disease'.

[22] See EDPS orientations on manual contact tracing, p. 6.

[23] See EDPS orientations on manual contact tracing, p. 5.

[24] *See, mutatis mutandis,* the EDPB Opinion 3/2019 on the interplay between the Clinical Trial Regulation and the GDPR, § 20.

an employer (Article 10(2)(b) and (h)[25]). Consent could be a lawful legal basis when processing concerns non-staff members and is carried out on a true voluntary basis.

Our findings under Section 3.1.3 concerning the inappropriateness of the use of Articles 5(1)(b) (legal obligation) and 5(1)(e) (vital interest) as lawful grounds are applicable for COVID-19 testing and/or handling of results as well.

As already mentioned in the context of body temperature checks, the use of Articles 5(1)(b) (legal obligation) and 5(1)(e)/10(2)(c) (vital interest), as lawful grounds, is inappropriate for manual contact tracing as well.

DPIAs

EUIs reported 40 manual contact tracing procedures but only eight DPIAs were conducted. EUIs should conduct a DPIA when developing and implementing a manual contact tracing operation because of the special categories of data involved, the novelty of the activity, and the processing of personal data on a large scale[26]. In this vein, EUIs should carry out a DPIA before they implement a manual contact tracing system.

Information of non-staff members

In order to ensure the required information of non-staff members, EUIs should include a privacy statement in any written communication with these individuals to inform them that they have been in contact with a staff member tested positive. Also, when asked to fill in an access register or a meeting list, they should be clearly informed that these listings may be used for contact tracing[27].

Handling by health professionals and transmission to third parties

Even though the survey did not reveal significant shortcomings in this respect, we remind EUIs of the principles developed in the EDPS orientations on manual contact tracing[28]. The contact tracing-related data should remain under control and supervision of medical professionals. EUIs should inform contact persons of a person tested positive following a clear protocol limiting the amount of data to what is strictly necessary to achieve the contact-tracing goal. If EUIs need to transmit personal data to EUIs whose staff was in contact with an infected person, EUIs must ensure that the transmission is indeed necessary for the implementation of the contact tracing strategy[29]. Local health authorities that would request data from contaminated staff members should establish that the request fall within the scope of their legal duties to implement a contact tracing operation[30].

Retention and duration of processing

The data collected in the context of manual contact tracing should, in principle, only be stored for a maximum of 14 days. Afterwards, they should be deleted or securely destroyed in accordance

---

25 See EDPS orientations on manual contact tracing, p. 5.
26 See EDPS orientations on manual contact tracing, p. 7.
27 See EDPS orientations on manual contact tracing, p. 6.
28 pp. 7-9
29 Recital 21 of the Regulation.
30 Article 9(1)(a) of the Regulation.

with the storage limitation principle[31]. However, it seems that several EUIs keep personal data for longer periods without duly justified reasons. The EUIs concerned should review the applicable retention periods.[32]

Finally, EUIs are invited to reflect on the necessity and proportionality of manual contact tracing in addition to the contact tracing imposed by national authorities in light of the evolving sanitary situation.

3.3. COVID-19 testing and/or handling of results

This part of the survey was broad. It covered COVID-19 diagnostic tests, carried out either within the EUI, by another EUI, or outside of the EUIs, as well as the handling of test results by EUIs.

Around half of the EUIs (23 out of 54) reported that they carried out and/or handled the results of COVID-19 diagnostic tests, which included both PCR and antigen tests, as well as antibody tests, reported by one EUI.

The majority of these EUIs (15 out of 23) noted that testing and/or handling of results was voluntary, for example where staff requested tests to help them to meet the travel requirements to their country of origin. Eight EUIs noted that it was mandatory, for example to allow staff members who have tested positive to return to the office, to fulfil national travel requirements when travelling abroad in the context of a mission, to attend specific meetings, or when indicated by the medial advisor.

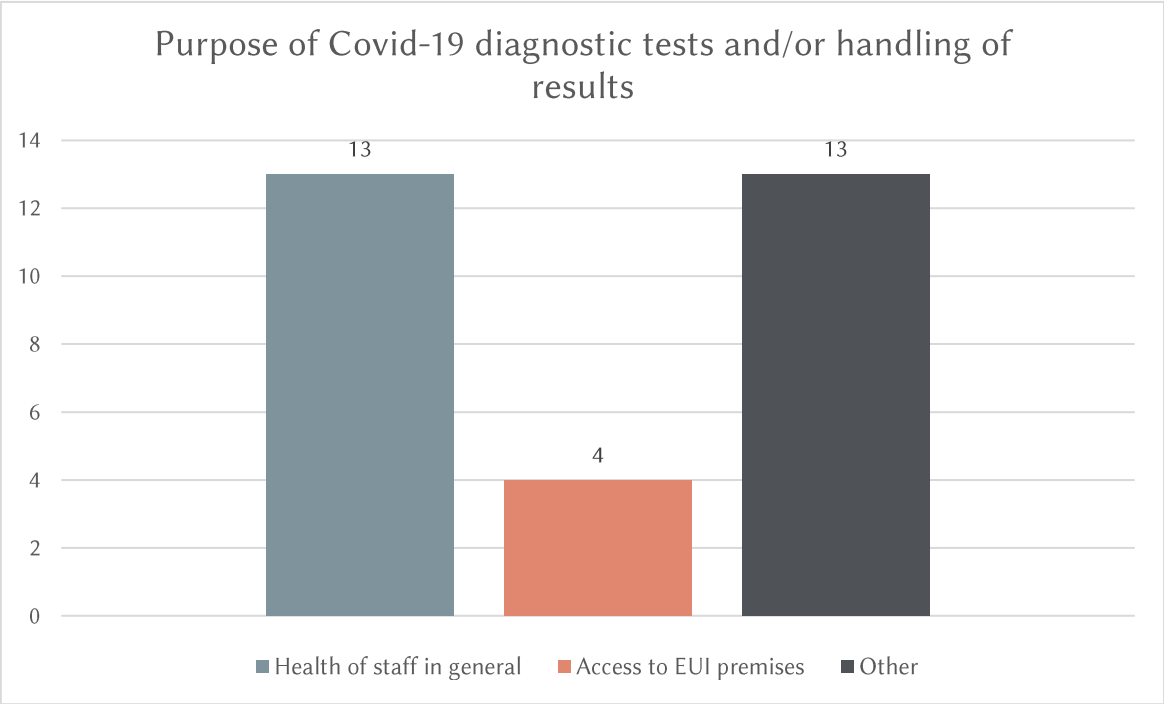
This processing operation overlaps with manual contact tracing, (Section 3.2.) which may take place where an individual tests positive for COVID-19, and access control (Section 3.4.), as EUIs may prevent individuals who have tested positive from entering their premises.

[31] Article 4(1)(e) of the Regulation.
[32] See EDPS orientations on manual contact tracing, p. 9.

3.3.1. Main points of interest on COVID-19 testing and/or handling of results

PURPOSES AND TYPE OF TESTING

Table 14



As shown in the diagram, most EUIs reported that they conducted tests and/or handled COVID-19 results to protect the health of staff in general. Those who answered 'Other', mostly tested or handled results to facilitate staff requests on a voluntary basis.

Of the four EUIs that conducted tests and/or handle results to control access to their premises, two indicated that they required staff members who had previously tested positive to present a negative test before they could return.

Testing was carried out within the EUIs (11 cases), externally, including at other EUIs (17 EUIs), or both (6 EUIs).

LAWFULNESS AND LEGAL BASIS

Most EUIs relied on Article 5(1)(a) (task in the public interest), followed by Article 5(1)(e) (vital interest), and Article 10(2)(i) (public interest in the area of public health).

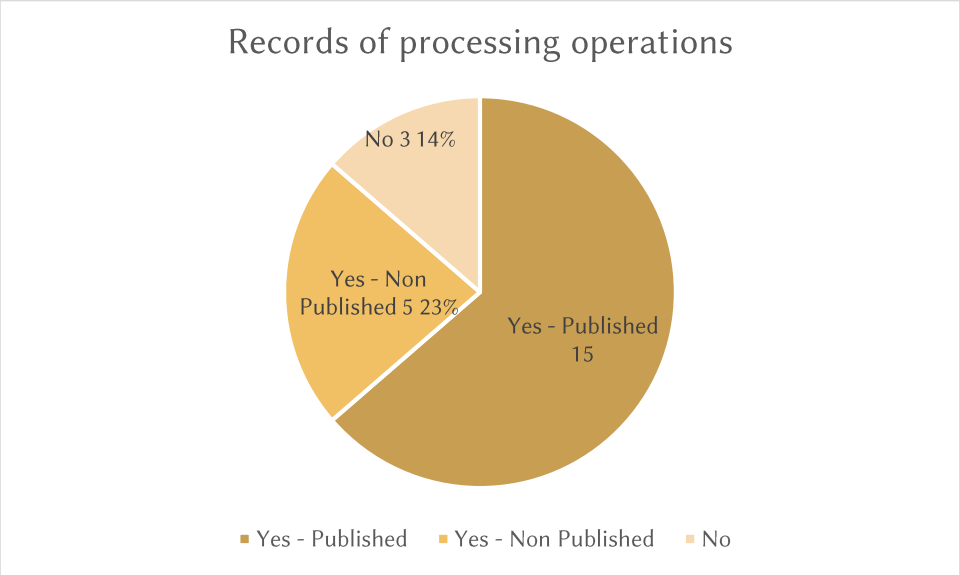
A few EUIs cited Articles 5 (1)(b) (legal obligation), 5(1)(d) and 10(2)(a) (consent), 10(2)(h) (preventive or occupational medicine), 10(2)(g) (substantial public interest), 10(2)(b) (employment and social security field), and 10(2)(c) (vital interests of data subjects).

Regarding legal bases in Union law[33] most EUIs referred to Article 1(e)(2) of the Staff Regulations .

RECORDS OF PROCESSING OPERATIONS

As shown in the graph, most EUIs published records of processing operations.

Table 15



INDIVIDUALS TARGETED, PERSONAL DATA PROCESSED, RECIPIENTS

All of the EUIs (23 out of 23) reported that they process health data and target staff members.

As shown in the graph, EUIs also targeted external contractors, visitors, as well as 'Other', which included family members, and individuals who accessed EUIs while presenting symptoms.

[33] Articles 5(1)(a), 5(1)(b), 10(2)(h) and/or. 10(2)(i)) of the Regulation.

Table 16

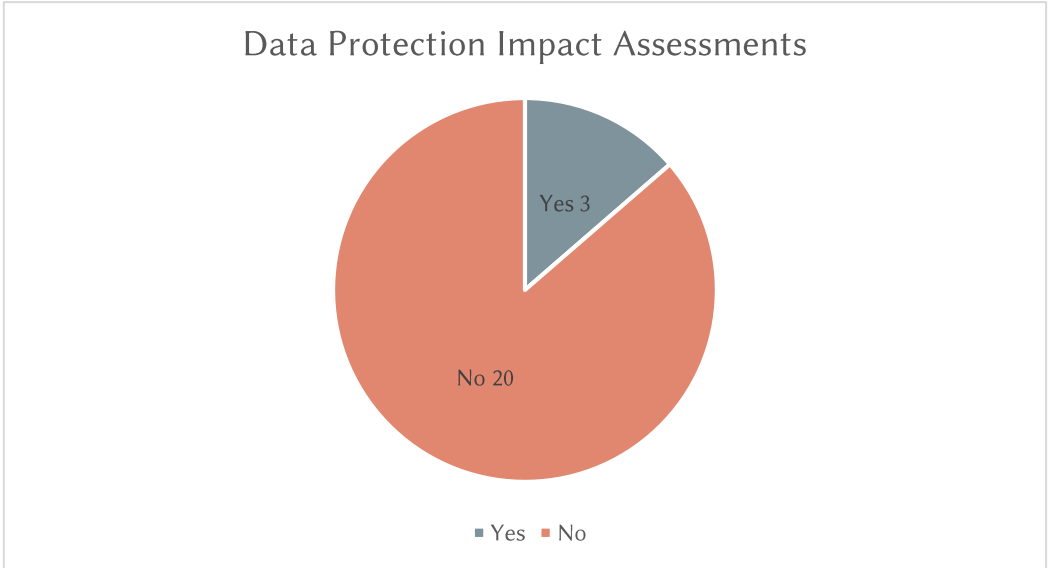
In most cases, the recipients of personal data processed during testing/ handling of COVID-19 results, are the EUIs medical services.

Other recipients included HR (to facilitate manual contact tracing where staff members test positive) security (for access control where staff test positive) and national health authorities in line with applicable national rules on contact tracing.

DPIAs

Three DPIAs were conducted for this processing operation. All were conducted following a threshold assessment, and criteria triggering the DPIA were: processing of special categories of data, processing of data on a large scale as well as innovative use of technological or organisational solutions were listed as criteria that triggered a DPIA.

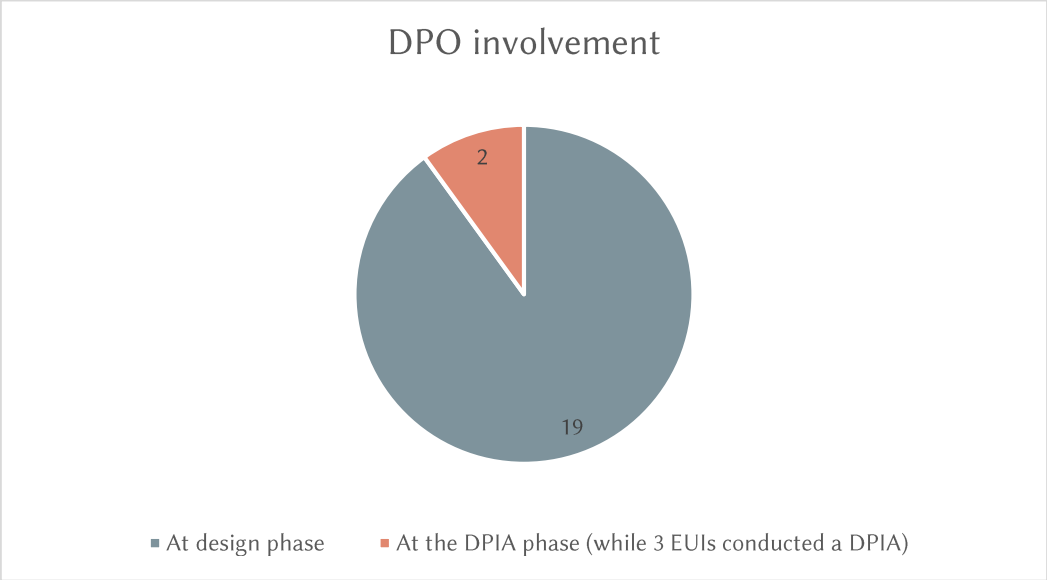
Table 17



DPO involvement

As shown in the graph, 19 EUIs involved their DPO in the design of the processing.

Table 18



External contractors (processors)

18 EUIs involved external contractors (processors) in the course of this processing operation. These mostly included external medical service providers, or external laboratories to analyse samples provided by the EUIs' medical services.

15 EUIs included data protection clauses in their contracts with external service providers.

Retention

EUIs deleted or securely destroyed data in line with their applicable retention periods for medical files. One EUI mentioned that deletion or destruction would take place in accordance with the contractor's retention period.

3.3.2. Legal analysis and recommendations on COVID-19 testing and handling of results

The EDPS welcomes the fact that in the majority of cases, COVID-19 testing by EUIs took place on a voluntary basis for staff members who wished to be tested. This testing was mainly to safeguard the health of staff members, considering that EUIs have a duty of care to their staff.

However, the EDPS would like to draw the attention of EUIs to the findings below and subsequent recommendations to ensure compliant processing in the context of COVID-19 testing and/or handling of results.

Grounds for lawfulness

Consent (Articles 5(1)(d) and/or Article 10(1)(a)) for COVID-19 testing and/or handling of COVID-19 results, may be a valid lawful ground despite the employment context when the following conditions are met: i) testing is purely voluntary, ii) it takes place at the request of the data subject, iii) EUIs act as facilitators by merely providing the testing facilities. In this context, EUIs may demonstrate that consent is freely given in accordance with Article 7(4) of the Regulation.

However, consent is not an appropriate lawful ground when EUIs conduct COVID-19 testing on a mandatory basis. Additionally, it is not appropriate where the handling of COVID-19 test results includes contact tracing by the EUI (see Section 3.2.2.).

Finally, our findings under Section 3.1.3 concerning the inappropriateness of the use of Articles 5(1)(b) (legal obligation) and 5(1)(e) (vital interest) as lawful grounds are also applicable for COVID-19 testing and/or handling of results.

DPIAs

In the context of COVID-19 testing and/or handling of results, special categories of personal data (health data) are usually processed on a large scale. This processing may be combined with follow-up measures taken by EUIs, such as limiting access to EUI premises. These criteria may trigger a DPIA especially when EUIs require their staff members to be tested on a mandatory basis. However, the number of EUIs that conducted a DPIA is quite low. EUIs are invited to check whether the processing operation at stake requires a DPIA in light of the EDPS Decision of 16 July 2019 on DPIA lists issued under Articles 39(4) and (5) of the Regulation. The EDPS guidelines of February 2018 on "accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation" may also prove useful as they provide guidance on how to conduct a DPIA.

Use of external contractors

The majority of EUIs engaged external contractors, such as laboratories or medical service providers, to carry out COVID-19 testing. Some EUIs reported that such contractors were controllers, while others mentioned that they were processors, and one EUI considered that the contractor was a joint controller. EUIs should have a clear understanding and make a clear decision about their role in relation to external contractors[34]. This choice should then be reflected in the contract.

In the present case, if an EUI engages an external private contractor to carry out COVID-19 testing on its behalf in the context of the execution of a service contract, it is advisable that the EUI be the controller and the external contractor be the processor[35].

Retention and duration of the processing

When EUIs engage a processor, the contract or other legal act under shall stipulate, among others, that the processor shall delete or return all personal data to the controller after the end of the

[34] See EDPS Guidelines on the concepts of controller, processor and joint controllership.
[35] See p. 23 of EDPS Guidelines on the concepts of controller, processor and joint controllership.

provision of services relating to processing, and delete existing copies unless Union or Member state law requires storage of personal data[36].

In this vein, it is not sufficient to rely on the retention periods set by the contractor to ensure that personal data is deleted. The EUIs remain accountable to define the retention periods and verify that the processor deletes the personal data in question, accordingly.

EU DIGITAL COVID CERTIFICATE AND NATIONAL HEALTH AND SAFETY RULES

The survey showed that a number of EUIs made COVID-19 testing and/or handling of results mandatory in the context of their return to work strategies. Since the entry into force of the digital COVID Certificate in July 2021, i.e. after the closure of the survey, some EUIs require staff members and externals to show a valid COVID Certificate to access their premises. We deal with this access control measure in Section 4.2.

3.4. Monitoring presence in EUI premises

Monitoring presence in their premises was the largest new processing operation among the EUIs (45 out of 54 replies).

For the majority of EUIs the monitoring of presence on their premises was mandatory. Only three stated it was optional.

Monitoring of presence in the EUI premises overlaps with manual contract tracing (see Section 2.2.), as indicated below.

3.4.1. Main points of interest

PURPOSES

Almost all EUIs reported they monitored presence to check occupancy rate (41 out of the 45 replies). In addition, approximately half of them stated that the processing was for contact tracing purposes.

'Other' purposes reported included ensuring business continuity during the pandemic, for example by providing appropriate protective material to persons entering the building.

LAWFULNESS AND LEGAL BASIS

Around 80% of the EUIs that stated that they were monitoring presence indicated a precise legal basis under Article 5 and/or Article 10 of the Regulation.

A significant majority of these relied on Article 5(1)(a) of the Regulation (task in the public interest). Article 5(1)(b) (legal obligation) and Article 5(1)(e) (vital interests) were also quite frequently cited.

[36] Article 29(3)(g) of the Regulation.

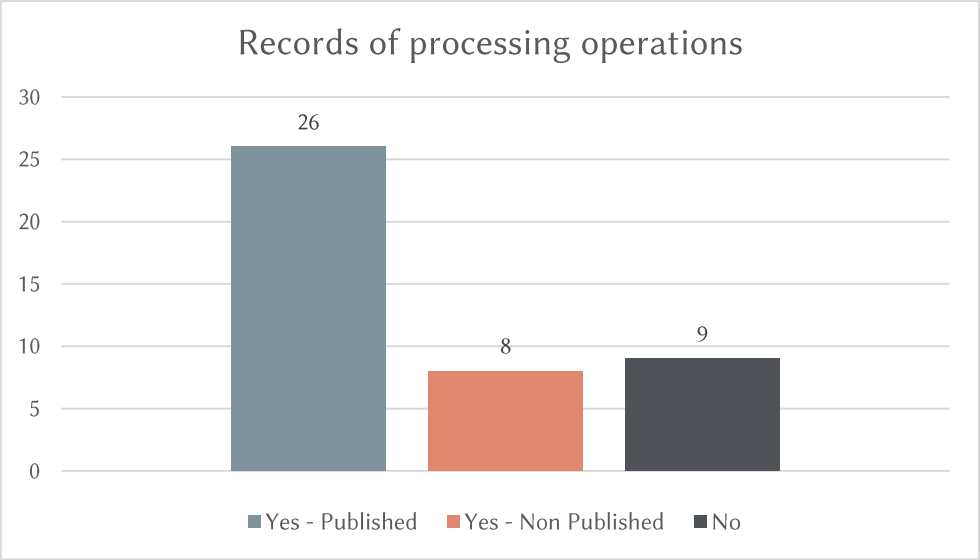
In relation to special categories of data, some replies cited Article 10(2) of the Regulation, including Article 10(2)(b) (employment and social security), Article 10(2)(h) (working capacity of employees, medical diagnosis etc.), and Article 10(2)(i) (public interest in the area of public health). One EUIs also referenced Article 10(2)(c) (vital interests, where the data subject is physically or legally incapable of giving consent) and Article 10(2) (g) (substantial public interest).

When the ground for lawfulness require a legal basis in Union law, EUIs mentioned mainly Article 1(e) of the Staff Regulations, but also Article 55, and Article 59. Some EUIs solely cited their internal rules.

Records of processing operations

As shown in the graph, most EUIs published records of processing operations.

Table 19

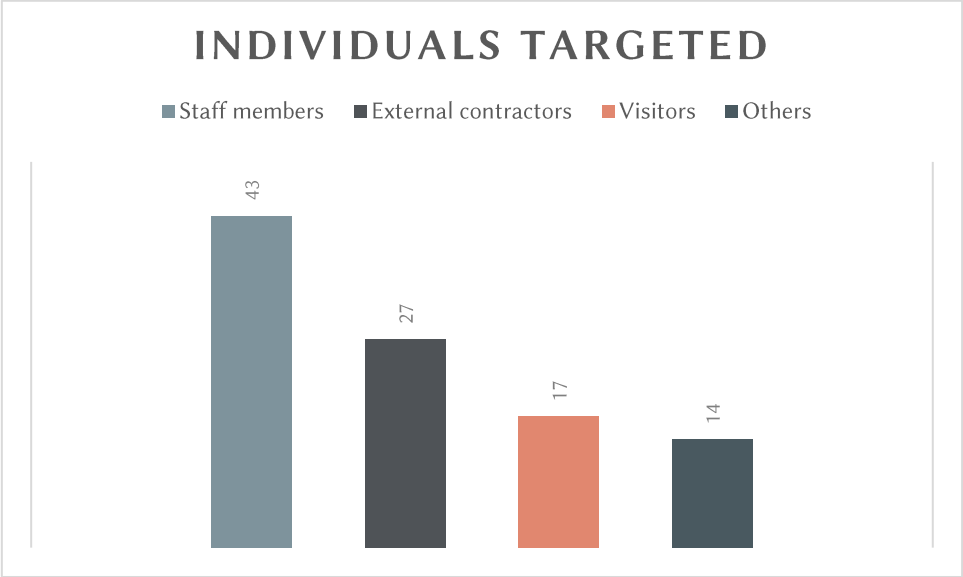


Individuals targeted, special categories of data

The individuals targeted by this processing operation are shown in the graph below.

Concerning the categories of personal data concerned, several EUIs mentioned that they process data concerning health.

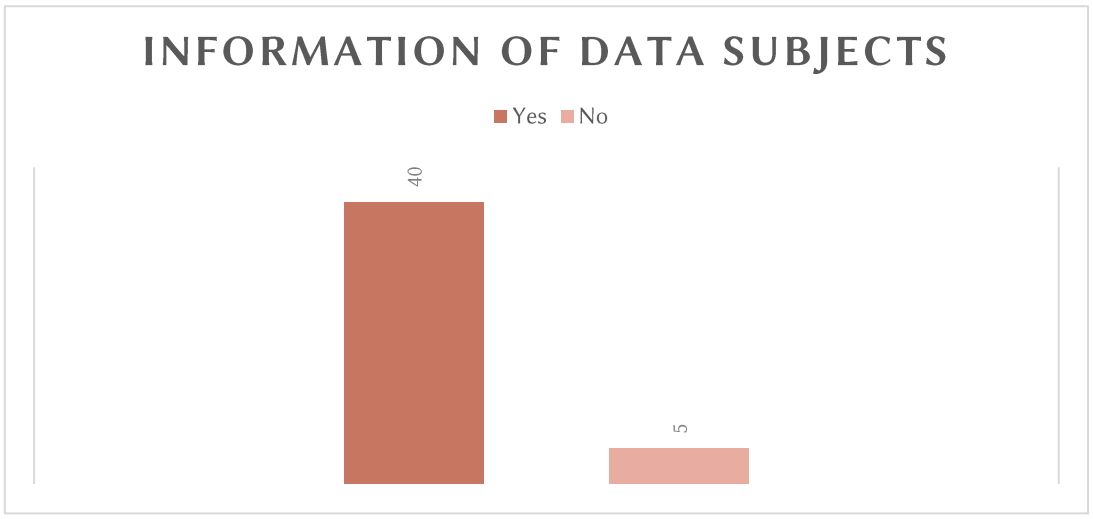
Table 20



Although not specifically addressed in the survey, EUIs sometimes used the free text boxes to indicate exactly which personal data they process. Answers indicated that EUIs generally collected the name and location in the building of the individual (e.g. office number), alongside the date. A few EUIs highlighted that whilst presence in the building was monitored, personal data was not collected; only a total aggregate number of presences (e.g. collected through a clock in/out system) is kept.

Information of data subjects

Table 21

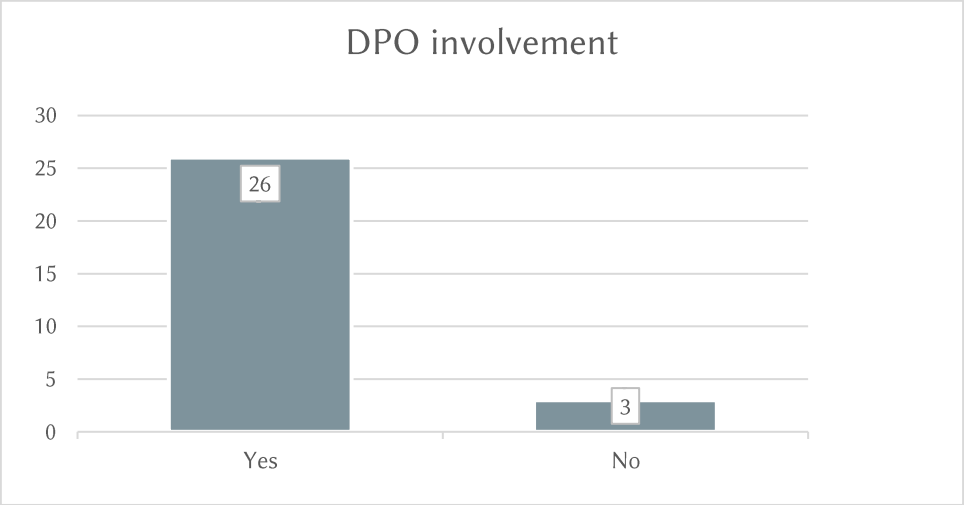


Almost all EUIs informed data subjects about the new processing operation.

DPO involvement

Just over half of the EUIs monitoring presence on their premises involved their DPO. This constituted both written and oral advice.

Table 22



RETENTION AND DURATION OF THE PROCESSING

Most of the EUIs (40 out of 45 replies) were still undertaking processing at the time of the survey. Very few EUIs stated they have discontinued processing whereas several stated that they had not specified a time limit as to the processing operation, neither a periodic review of its necessity.

3.4.2. Legal analysis and recommendations on monitoring staff presence

The EDPS welcomes the fact that EUIs demonstrated clearly defined purposes concerning monitoring staff presence in line with the purpose limitation principle[37]. Additionally, a significant number of EUIs correctly identified Article 5(1)(a) (task in the public interest) as an appropriate lawful ground for processing.

That said, there is room for improvement in the following areas:

GROUND FOR LAWFULNESS

EUIs should distinguish the lawful grounds they rely upon depending on the purpose of processing. This may be appropriate where EUIs are monitoring staff presence for two different purposes - i.e. to check occupancy rate and for contact tracing - which at least nine EUIs appear to be doing.

Our findings under Section 3.1.3 on the inappropriateness of Article 5(1)(b) (legal obligation) and Article 5(1)(e) (vital interest) as lawful grounds, are also applicable for monitoring staff presence.

Additionally, when special categories of data, such as health data, are processed, a lawful ground under Article 10 of the Regulation shall be determined on top of the lawful ground under Article 5 of the Regulation. However, while several EUIs reported the processing of health data, only a few of them cited a lawful ground under Article 10 of the Regulation. The concerned EUIs should review their processes and complement their records in this regard.

[37] Article 4(1)(b) of the Regulation.

CATEGORIES OF PERSONAL DATA PROCESSED

It is not clear why monitoring presence would involve the collection of health data. While we understand that processing of health data is necessary in the context of contact tracing, EUIs should assess the necessity and proportionality of processing health data for the sole purpose of monitoring presence.

Additionally, two EUIs reported to be collecting information from visitors regarding potential infection with COVID-19 activity (e.g. symptoms and contact with infected people), without indicating that they process health data. EUIs should ensure that they properly identify all categories of personal data processed

DPO INVOLVEMENT

Quite a high proportion of EUIs did not involve their DPO either in the design or implementation of this processing operation. We would like to remind EUIs that they should ensure that the DPO is involved early and systematically in all issues relating to data protection within the EUI in accordance with Article 45 of the Regulation[38].

REVIEW OF THE PROCESSING OPERATION

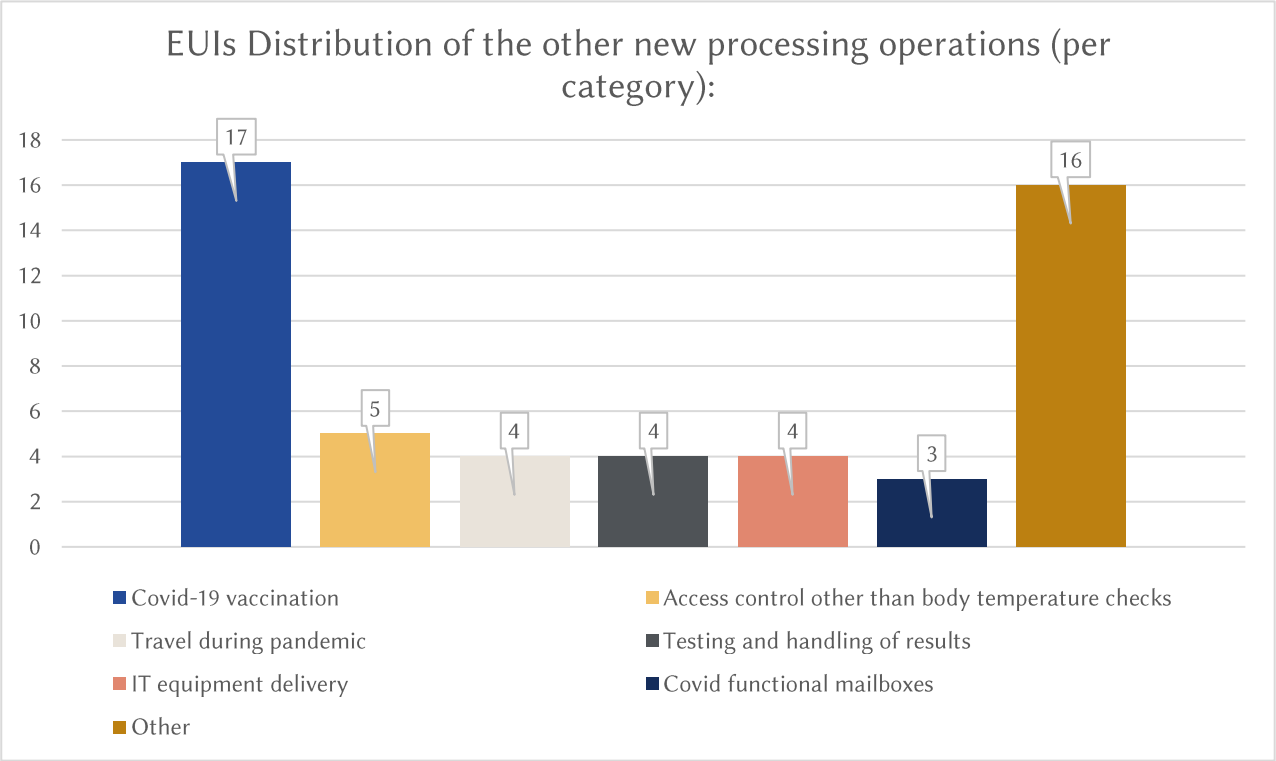
Review periods were not always specific and well-defined. EUIs should regularly reassess the necessity and proportionality of this processing operation in light of the evolution of the epidemic situation and its scientific understanding.

[38] See EDPS position paper on the role of Data Protection Officers of the EU institutions and bodies.

4. OTHER NEW PROCESSING OPERATIONS

Apart from the four processing operations that the EDPS pre-identified in the first part of the survey, EUIs had the possibility to report on any additional processing operations that they introduced in the context of the COVID-19 crisis. The EDPS grouped these additional processing operations per topic, as showed in the graph below.

Table 23



Additional processing operations were also reported that cannot be grouped due to their diverse nature. These concerned: the return to work of vulnerable staff (regarding improved working conditions) (2 occurrences); organisation of training sessions and webinars to help staff perform their tasks during teleworking (2); social activities (2); online assessment of candidates in the context of recruitment procedures (1); administrative tasks conducted remotely (e.g. return of equipment by permanent leavers) (1); business continuity plan (staff contact list (1); opening and scanning of inward professional mail in order to dispatch it electronically; provision of social counselling services provided via Skype or other meeting tools (1); processing of data via open sources for compiling up-to-date information in the fight against disinformation (1); geographical location of staff (1); distribution of masks (1).

From the (sometimes limited) information provided, we have not identified any major issues in relation to these processing activities.

We provide below a detailed analysis of the replies concerning recurrent processing operations, i.e. in relation to COVID-19 vaccination (13 processing operations reported- Section 4.1.) and access control to EUIs premises other than body temperature checks and contact tracing (six processing operations - section 4.2.).

4.1. COVID-19 vaccination campaign

EUIs introduced 17 processing operations related to COVID-19 vaccination, all on an optional basis. Three did not fill out dedicated sections of the survey, and only indicated the purpose of the processing operation without providing additional information.

4.1.1. Main points of interest

Purposes

The main purposes for processing regarded vaccination campaigns and related vaccination surveys, identifying persons who wish to be vaccinated in the EUIs' vaccination centers, establishing priority lists of vulnerable staff, establishing lists to be transferred to national authorities to integrate vaccination of EU staff members and members of their families into national vaccination campaigns, and to comply with national requirements.

Other related purposes included ensuring that staff with their residence outside the place of employment may receive an invitation to be vaccinated in the place of employment, and following up on the vaccination and any side effects experienced. One EUI also established a Vaccine Strategy Task force to coordinate and steer issues related to the EU global response to the COVID-19 pandemic, including a vaccine-sharing mechanism and strategy as well as a vaccination strategy.

Lawfulness and legal basis

Around half of the EUIs relied on Article 5(1)(a) (task in the public interest). In addition, EUIs relied on Articles 5(1)(b) (legal obligation), 5(1)(d) (consent), 5(1)(e) (vital interests of data subjects), 10(2)(a) (explicit consent), 10(2)(b) (employment law), 10(2)(i) (public interest in the area of public health), 10(2)(h) (preventive or occupational medicine), 10(2)(g) (substantial public interest), and 10(2)(c) (vital interests of data subjects).

Individuals targeted and personal data processed

EUIs indicated that they mainly targeted their staff members. Four EUIs also indicated that processing concerns family members of staff, or staff members of other EUIs. Almost all EUIs indicated that they processed health data.

DPO involvement

Almost all EUIs actively involved their DPO in the design and/or the implementation of the processing. The EUI that conducted a DPIA involved the DPO at the DPIA phase.

Retention and duration of the processing

EUIs reported that health-related data processed by their medical services was retained in accordance with the applicable retention periods for medical files. A few mentioned that personal data was kept as long as it is required to distribute the list to the national health authorities, or for one month after transition to the Medical Service in charge. One EUI specified that data of non-staff members was kept "for the duration justified by the situation of the COVID-19 pandemic in case of a need for additional vaccination, but no longer than 30 years".

Concerning review of the processing operation, one EUI reported it would review the process one year after the initial vaccination campaign is completed or by alteration of the procedure. Another EUI reported that a possible revision might take place depending on the developments related to the COVID-19 pandemic and further scientific data available.

4.1.2. Legal analysis and recommendations on vaccination campaign

GROUND FOR LAWFULNESS

Our findings under section 3.1.3 concerning the inappropriate use of Articles 5(1)(b) (legal obligation) and 5(1)(e)/10(2)(c) (vital interest) as lawful grounds are also applicable for COVID-19 vaccination campaigns.

The appropriate ground for lawfulness for processing personal data in the context of COVID-19 vaccination campaigns will depend on the specific processing operation. When staff members identify themselves with their EUI (or the medical service as wishing to be vaccinated and/or as vulnerable and therefore entitled to priority in the vaccination schedule, and where they are then invited and registered for a vaccine, the suitable ground for lawfulness in this context could be consent (Article 5(1)(d) and 10(2)(a) of the Regulation), provided that it complies with all the requirements of the Regulation (including the possibility to withdraw consent at any time) and is not confused with informed consent to medical care[39]. Another possible ground for lawfulness here for staff members could be occupational medicine (Article 10(2)(h) of the Regulation).

Once the vaccine has been administered, the appropriate ground for lawfulness for any follow-up processing activities, for example the transmission of the vaccination status of individuals to national health authorities with a view to issuing COVID-19 Digital Certificates in line with the EU Regulation on the matter[40], should be the accomplishment of a task in the public interest in the area of public health and the obligations of EUIs as employers (Articles 5(1)(a) and 10(2)(b) and (i) of the Regulation). This information is necessary for the Member States to be able to issue certificates[41]. The purpose of this further processing is compatible with the original purpose in line with Article 6 of the Regulation. Moreover, in this context, the transmission to national authorities is compliant with Article 9 of the Regulation.

DPO INVOLVEMENT

The EDPS commends the widespread and active involvement of the DPO in processing related to vaccination campaigns.

---

[39] Where consent is not suitable as ground for lawfulness of the data processing, informed consent could still serve as an appropriate safeguard of the rights of the data subject. See pp. 19-20 of the EDPS Preliminary Opinion of 6 January 2020 on data protection and scientific research.

[40] Member States are responsible for issuing these certificates by virtue of 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, OJ L 211, 16.06.2021, p.1.

[41] In line with Regulation (EU) 2021/953, Member States shall issue the Digital COVID Certificate, which can be either issued automatically or upon request by the data subject in the cases of test and vaccination certificates, while only upon request of the data subject in the case of recovery certificate

4.2. Access control (other than body temperature checks and presence monitoring) for visitors and critical staff

Five EUIs stated that they had introduced six new processing additional processing operations to control access to their premises other than body temperature checks or monitoring presence. Only four of these processing operations were reported on in detail in dedicated sections of the survey.

The survey was closed before the implementation, in July 2021, of the EU Digital COVID certificate, which now serves as an access control tool in several EUIs.

4.2.1. Main points of interest

PURPOSES

The EUIs introduced these access control measures for two broad purposes: to filter access depending on whether a visitor had potentially been exposed to the virus (e.g. by asking for information on contact with infected persons, or on symptoms) and to filter access depending on whether a staff member is 'critical'. Critical staff are those who need to be in the office to perform tasks that they cannot accomplish remotely.

LAWFULNESS AND LEGAL BASIS

The EUIs cited various legal bases, covering Articles 5(1)(a) (task in the public interest); 5(1)(b) (legal obligation); 5(1)(c) (contract), 5(1)(d) (consent); 5(1)(e) (vital interests); 10(2)(a) (consent); 10(2)(b) (employment and social security); 10(2)(c) (vital interests); 10(2)(g) (substantial public interest); 10(2)(h) (occupational medicine.); and 10(2)(i) (public interest in the area of public health).

The EUIs that indicated legal grounds under Article 10 (concerning special categories of personal data), were those that controlled visitors' access via a questionnaire.

RECORDS OF PROCESSING OPERATIONS

All four replies that reported on this processing in detail provided a link to a public record of the processing operation.

INDIVIDUALS TARGETED, SPECIAL CATEGORIES OF DATA, RECIPIENTS

Both staff (in relation to the critical staff certificates) and visitors (in relation to the visitor questionnaires on entry) were targeted.

Both processing operations that targeted staff were mandatory, and did not involve the processing of special category data.

Of the processing operations targeting visitors, one involved health data ("relating to risks concerning COVID-19 condition") and the other did not. Moreover, one was mandatory (with the EUI relying on consent as a lawful ground), and the other was not.

INFORMATION OF DATA SUBJECTS

For all four processing activities reported on in detail, data subjects were informed. The EUIs made their data protection statements available via intranet and webpages, as well as at the entrance/ receptions to the premises.

DPO INVOLVEMENT

For all four processing activities reported on in detail, the DPO was involved and played an active role in the design process.

RETENTION AND DURATION OF THE PROCESSING

For all four processing activities reported on in detail, EUIs specified a time limit. Regarding retention, answers included three months, two weeks, and "ordinary access control retention periods for EU staff and visitors."

Regarding recurrence of review, results varied, and included: review in view of instructions from DG HR and any management decisions; review in view of the evolution of the COVID-19 crisis; review in case of alteration of the process; and review "after the pandemic is over".

4.2.2. Legal analysis and recommendations on access control

GROUND FOR LAWFULNESS

As for other processing reported in the survey, EUIs sometimes appear to adopt a 'scattergun' approach - listing multiple lawful grounds, when not all are applicable. EUIs should rather focus on identifying one concretely applicable lawful ground.

As already mentioned for other processing operations, the reference to a legal obligation (Article 5(1)(b)) by the reporting EUIs is often erroneous, as the Regulation and decisions reported do not specifically mandate the EUI to control access to its premises by collecting personal data. In this vein, our findings under Section 3.1.3 are applicable. This includes with regards to Articles 5(1)(e)/ 10(2)(c) (vital interests), which do not constitute appropriate grounds for lawfulness for processing of personal data in the context of access control.

Further, EUIs referred to consent as a lawful ground (Articles 5(1)(d) and 10(2)(c)). Consent is not appropriate for staff members because in this context, they cannot provide "freely given, specific, informed and unambiguous" as well as "explicit" consent as required by the Regulation[42]. Consent would also not be appropriate for visitors, who are in most cases obliged to come to the EUI premises for work purposes.

INDIVIDUALS, CATEGORIES OF DATA, RECIPIENTS

A few EUIs reported to be collecting information from visitors regarding potential infection with COVID-19 (e.g. symptoms and contact with infected people), but had not indicated that they processed health data. The EDPS invites EUIs to ensure that they properly identify all categories

[42] For the definition of consent, please check Article 3(15) of the Regulation. For special categories of data, the consent must also be specific (Article 10(2)(b) of the Regulation).

of personal data processed when reporting on a given processing operation in line with Article 31 of the Regulation. The EDPS also reminds EUIs to only process personal data for access control that is necessary and proportionate and in line with the data minimisation principle.

DPO INVOLVEMENT AND RECORDS OF PROCESSING OPERATIONS

The EDPS commends the active involvement of the DPO, as well as the public record of processing operations, in all four processing operations that were reported on in detail.

REVIEW OF THE PROCESSING OPERATION

Review periods were not always specific and well-defined. The EDPS advises EUIs to regularly review the necessity and proportionality of processing in light of the evolution of the epidemic situation and its scientific understanding.

EUI'S VERIFICATION OF EU DIGITAL COVID CERTIFICATE

Since the entry into force of the digital COVID-19 certificate in July 2021[43] , several EUIs now require a valid EU Digital COVID Certificate to access their premises, thus only granting access to persons who are vaccinated, who have recovered from COVID-19 or who can show a recent negative COVID-19 test result. The modalities of the verification vary from one EUI to another. The certificate requirement may apply only to external visitors or also staff members; it may be required for the access to the entire EUI's building or only certain areas; and it may involve a mere visual verification of the certificate or a digital verification using an application. Lastly, sometimes Rapid Antigen Tests are possible as an alternative to the EU Digital COVID Certificate.

The EDPS refers to the EDPS Guidance on Return to Work of 9 August 2021.

The visual verification of the EU Digital Certificate (either in digital or paper-based format) would involve an interference with the right to privacy of Article 7 of the Charter but would not constitute a processing of personal data under the Regulation, unlike the digital verification of the Certificate using a dedicated application.As to the role of EUIs in relation to the digital verification of COVID certificates, the EDPS takes the view that EUIs are controllers of the data processed on the app for the purpose of access control. To assess whether EUIs are entitled to require a valid EU Digital COVID Certificate and whether the modalities of this requirement are necessary and proportionate, EUIs must take into account the rules in the area of public health of their host Members State. In particular, they should assess whether national legislation expressly provides for, or obliges, a measure, or whether it is prohibited under the host's national law. As recalled in the EDPS Return to the Workplace, while EUIs enjoy privileges and immunities vis-à-vis their host Member States, those privileges and immunities cover only those areas necessary for the specific functioning of EUIs[44]. The Protocol is usually implemented by specific headquarters or establishment agreements concluded with the authorities of the host Member State. Exceptions from Member State law generally do not include rules on health and safety. Therefore, should EUIs intend to deviate from the national legal regime as regards public health, they should first assess

[43] 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, OJ L 211, 15.6.2021, p 1.

[44] Section 2 and Section 6.1. of the Guidance.

whether a divergence is permitted according to the specific headquarters or establishments agreements concluded with the Member States.

The EDPS also recommends that EUIs take into account the guidance and recommendations from the Member States' national health authorities and the legal interpretations provided by the national data protection authorities.

The EDPS Opinions on the verification of EU Digital COVID Certificate by EUIs are available on its website.

5. USE OF IT TOOLS IN TIMES OF TELEWORK

5.1 New IT tools

36 out of the 54 respondents indicated that they started using one or more new IT tools to ensure business continuity during remote work. 81 IT tools were introduced in total. Given several tools are used by more than one EUI, 38 different tools were introduced.

Considering the diversity of the IT tools, the different purposes for which they were deployed, and the various underlying processing operations connected to the use of the tools, it was difficult to draw meaningful conclusions regarding compliance with the data protection framework.

5.1.1 Main points of interest

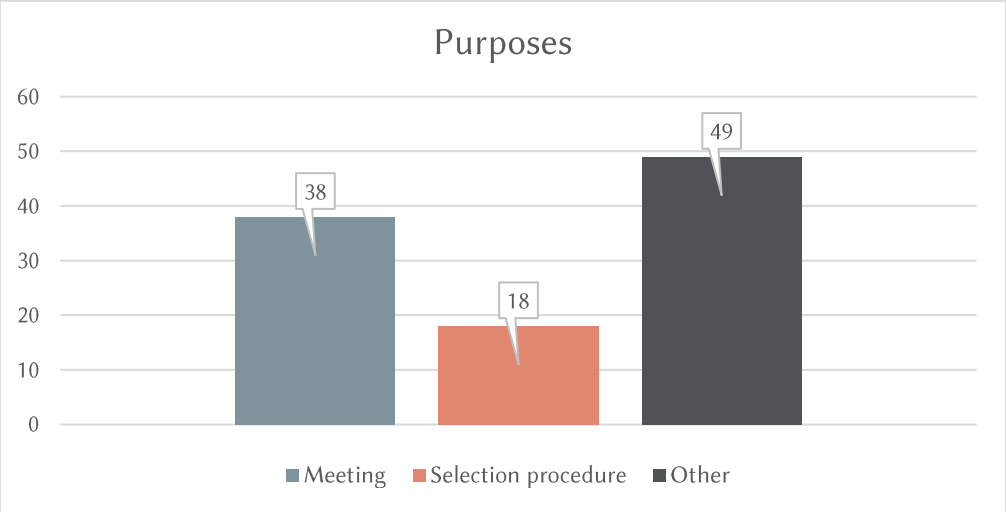
PURPOSES

The majority of the new IT tools were deployed to organise meetings. 18 were deployed for selection and/ or evaluation procedures.

A significant number of EUIs recorded other purposes. These included: data analytics; managerial planning and monitoring; ensuring remote access for IT support; promoting collaboration on shared files; organising conferences, workshops or training sessions; handling electronic signatures; managing records of presence in the context of the Covid-19 pandemic; facilitating online voting procedures; and managing vaccination appointments.

A few EUIs introduced new tools for online recruitment procedures. Two EUIs deployed tools for proctoring tools to be used in the context of recruitment procedures.

Table 24

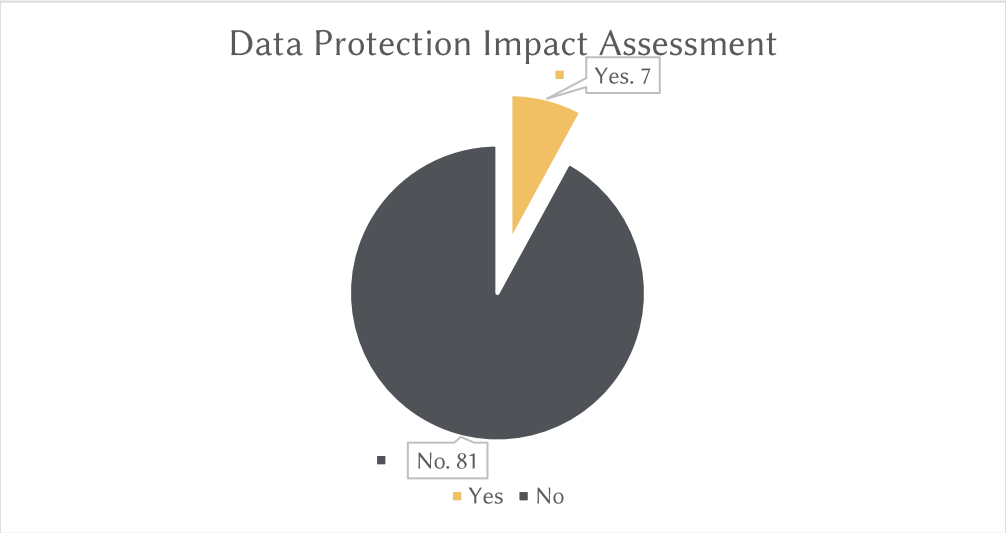


DPIAs

Seven EUIs conducted nine DPIAs regarding new processing operations related to the IT tools. These DPIAs concerned, *inter alia,* videoconferencing tools and an online voting solution.

Extensive changes to the document management system and IT infrastructure, processing of personal data on a large scale, and innovative use of technology such as cloud services, were the main criteria that triggered a DPIA. Some respondents also referred to the sensitive nature of the processing operation, the likelihood of processing sensitive information (such as that which could be included in the content of documents or emails processed in the system) as well as international data transfers.

Table 25



External contractors (processors)

EUIs engaged external contractors for the deployment of 54 IT tools. Several EUIs indicated that the external contractors were service providers (e.g. software providers) that acted as processors.

One EUI indicated that the service providers are both controller and processor. Finally, one EUI pointed out that the external contractor was a sub-processor.

Data protection clauses were included in the contracts in the majority of cases.

5.1.2. Legal analysis and recommendations on new IT tools

General observations

Several EUIs relied on the use of the same IT tools to ensure business continuity during remote work. In the majority of cases, external contractors that provide such services acted as processors, as they process data on behalf of EUIs. We welcome the fact that the majority of EUIs indicated that data protection clauses are included in the respective contracts. Aiming at reinforcing the position of EUIs vis-a-vis such contractors, the EDPS encourages EUIs to develop synergies to jointly negotiate data protection clauses with the respective contractors.

The EDPS is implementing a specific Strategy for EUIs to comply with the 'Schrems II' Ruling and ordered EUIs to report on transfers separately, the survey did not focus on this matter. Nevertheless, the EDPS reminds EUIs that they should pay particular attention to any transfers of personal data outside the EU/EEA that the use of IT tools, in particular those which are cloud-based, may entail. Transfers must be compliant with Chapter V of the Regulation. Useful information is included in the EDPS Strategy for Union institutions, offices, bodies and agencies to comply with the "Schrems II" ruling, as well as on the EDPB recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. The recent EDPS Decision authorising temporarily use of CJEU-Cisco ad hoc clauses for transfers (Cisco Webex) may also serve as an indication on the content of the development of any ad-hoc clauses for transfers in line with Article 48(3)(a) of the Regulation.

DPIAs

The number of DPIAs carried out was low, considering that some of the IT tools concern data processing that prima facie, would meet at least two criteria listed in Annex 1 of the Decision of the EDPS Decision of 16 July 2019 on DPIA lists issued under Articles 39(4) and (5) of the Regulation. Specifically, some of the IT tools likely entail innovative use or applying technological or organisational solutions that can involve novel forms of data collection and usage and/or data processed on a large scale. Additionally, the use of proctoring tools (18 cases) may entail monitoring of data subjects, which may trigger a DPIA depending on how extensive such monitoring is.

Use of external contractors (processors)

EUIs should clarify roles and responsibilities with service providers when using IT services, such as videoconferencing tools. Several EUIs did not indicate sufficient details on the role of the service providers or the inclusion of data protection clauses in the respective contracts. The EDPS advises EUIs to clarify roles and responsibilities with the external contractors. The EDPS Guidelines on the concepts of controller, processor and joint controllership under the Regulation provide useful elements to help EUIs with this assessment and provide guidance on how to ensure that the respective contracts meet the requirements of Article 28 (joint controllership) and 29 (controller-processor relationship) of the Regulation.

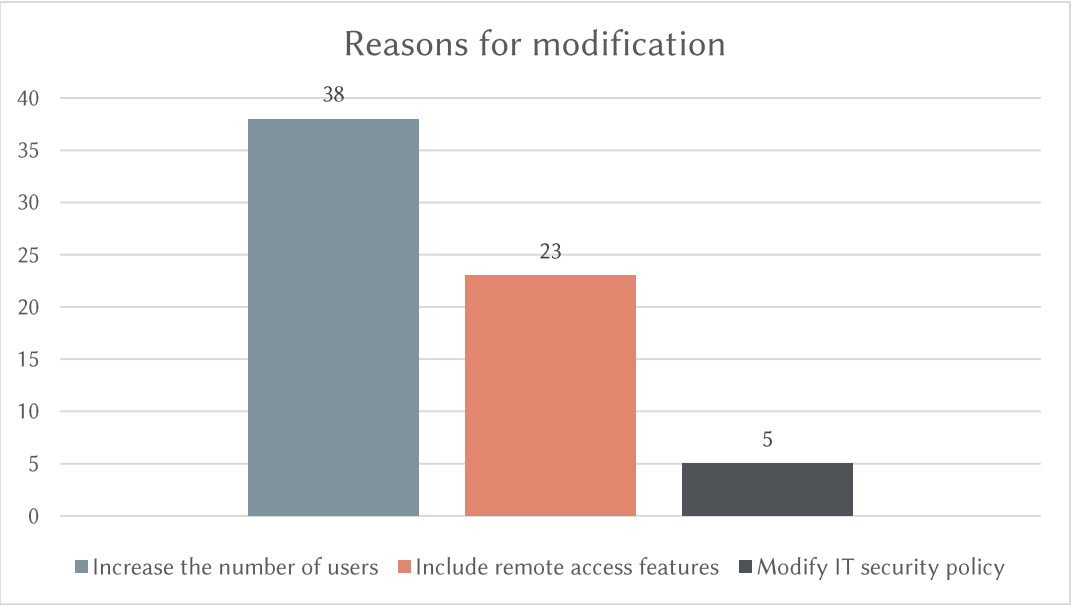
5.2 Modifications to existing tools

27 EUIs reported modifications to existing tools to adapt to remote work. The nature of these modifications was diverse. They included modifications to increase the number of users of a tool (38), to include remote access features (23), to modify the IT security policy (5), to ensure recording of virtual meetings, to gather new categories of personal data, or to introduce increased anonymity and security measures.

Modifications to IT security policies included, for example, the setting of the 'password never expire' option for all user email accounts, to prevent loss of access due to expired passwords, and to reduce the number of visits to the EUI's premises to reset passwords.

In light of the diverse nature of the modifications and the underlying processing operations, the EDPS drew no meaningful conclusions/recommendations to enhance compliance with the data protection framework. In this vein, there were no meaningful results concerning this part of the survey for the purpose of this public report.

Table 26



6. CORE BUSINESS ACTIVITIES

Only one EUI reported that it had implemented two new processing operations aiming to respond to the Covid-19 pandemic as part of its core business. The processing operations implemented concerned public stakeholder meetings related to the Covid-19 crisis as well as the establishment of a system of contacts tasked to report on shortages of medicines caused by major events in the context of the COVID-19 pandemic. From the information made available, we have not identified specific risks as to the processing of COVID-19 related data.

We encourage EUIs that process COVID-19 related data as core business to carefully check their activities in the matter and, if they identify any processing of personal data, to ensure compliance with the Regulation (records, data protection notices, etc.).

7. CONCLUSION

The survey mapped the processing operations introduced by EUIs in the context of the COVID-19 pandemic. In particular, it showed that EUIs have introduced new processing operations on body temperature checks, manual contact tracing, COVID-19 testing and/or handling of results, monitoring staff presence, COVID-19 vaccination campaigns, and other access controls for visitors and critical staff. They also introduced and/ or adapted a range of IT tools, and one EUI introduced processing operations to respond to the pandemic as part of its core business operations.

Overall, the survey results revealed that the EUIs made substantial efforts to ensure new processing operations were compliant with the Regulation, and achieved good practice in a number of areas, as reflected in the respective legal analysis sections. These efforts are particularly commendable given the fact that EUIs had to take action in very short timeframes due to the pandemic's rapid evolution.

Nonetheless, certain data protection aspects deserve closer consideration, and we invite EUIs to check the sections of the report that relate to their current processing activities and, where necessary, to follow the recommendations presented.

Some general conclusions concerning the entirety of the processing operations reported can be drawn. These conclusions are of continued relevance given COVID-19's ongoing impact on EUI's' operations, as well as the longer-lasting legacy it may leave, for example, concerning telework and remote recruitment practices.

First, EUIs should ensure that they define a ground for lawfulness under Article 5 and/or Article 10 of the Regulation that is appropriate for the processing at stake. EUIs should avoid inserting several grounds for lawfulness and should be able to justify the choice of each that they rely upon. EUIs should also keep in mind that a 'legal obligation' must refer to that which is laid down in Union law and is sufficiently specific as to the processing of personal data it requires, that consent must be interpreted restrictively, and that the protection of the 'vital interests' of individuals refer to life-or-death situations. Additionally, EUIs should always be able to point to an applicable legal basis when relying on grounds for lawfulness that refer to Union law (e.g. Article 5(1)(a) or Article 5(1)(b) of the Regulation).

Second, when they envisage a new processing operation, EUIs should carry out a threshold assessment to determine whether a DPIA is needed, in line with the criteria set out in the EDPS Decision on DPIA lists[45].

Third, considering the dynamic evolution of the COVID-19 crisis and of its scientific understanding as well as its now long lasting nature, EUIs should carefully and regularly (re)assess the necessity and proportionality of their existing COVID-related processing activities, as well as any new processing they wish to start. Such an assessment should account for national rules in the host Member State, as well as guidance issued by national health and data protection authorities. This is particularly relevant when EUIs

[45] https://edps.europa.eu/sites/default/files/publication/19-07-16_edps_dpia_list_en.pdf See also the EDPS Accountability on the ground Toolkit, which includes a part on threshold assessment and DPIAs: https://edps.europa.eu/node/4582_en.

Fourth, EUIs should involve their DPOs early and systematically in all issues related to data protection, including in the design (notably regarding the DPIA), implementation, and review of COVID-19 related data processing operations.

Finally, when using the EU Digital COVID Certificate as a requirement for accessing to their premises, EUIs should refer to the EDPS Guidance on Return to Work. They should in particular take into consideration national health and safety rules of the host Member States, as the Protocol on privileges and immunities of EUIs do not cover these rules in general and any divergence should be duly justified in light of the specific situation of each EUI.

We would like to conclude this report by thanking the EUIs for their contributions, and to emphasize the value of the survey's results for the EDPS. In particular, the survey results may feed into updating existing EDPS guidelines, or contribute to the development of new guidelines, depending on the evolution of the COVID-19 pandemic. The survey results will also inform the EDPS' execution of audits and investigations under Article 58 of the Regulation. In this vein, the EDPS has already conducted targeted audits in two EUIs, regarding retention periods for COVID-19 related processing activities which had run out at the time of the on-the spot inspections (October 2021).

We hope that this report will be helpful for EUIs to reassess their existing processing operations generated by the pandemic and to serve as a guide for setting-up new processing operations in relation to COVID-19.

ANNEX 1: TEMPLATE OF THE SURVEY QUESTIONNAIRE

https://edps.europa.eu/system/files/2022-02/2022-covid-survey-report-annex-i_en.pdf

ANNEX 2: LIST OF THE EUIs THAT RESPONDED TO THE SURVEY

Council of the European Union
European Parliament
European Commission
Court of Justice of the European Union
Court of Auditors
European Economic and Social Committee (EESC)
European Investment Bank (EIB) ***together with EIF***
European External Action Service (EEAS)
European Ombudsman
European Data Protection Board (EDPB)
European Data Protection Supervisor (EDPS)
European Central Bank (ECB) ***together with ESRB***
European Anti-Fraud Office (OLAF)
Translation Centre for the Bodies of the European Union (CdT)
Agency for Fundamental Rights (FRA)
Agency for the Cooperation of Energy Regulators (ACER)
European Medicines Agency (EMA)
Community Plant Variety Office (CPVO)
European Training Foundation (ETF)
European Asylum Support Office (EASO)
European Network and Information Security Agency (ENISA)
European Foundation for the Improvement of Living and Working Conditions (Eurofound)
European Food Safety Authority (EFSA)
European Maritime Safety Agency (EMSA)
European Centre for the Development of Vocational Training (CEDEFOP)
European Education and Culture Executive Agency (EACEA)
European Agency for Safety and Health at Work (EU-OSHA)
European Fisheries Control Agency (EFCA)
European Union Satellite Centre (SATCEN)
European Centre for Disease Prevention and Control (ECDC)
European Environment Agency (EEA)
European Investment Fund (EIF) ***together with EIB***

European Border and Coast Guard Agency (Frontex)
European Securities and Markets Authority (ESMA)
European Aviation Safety Agency (EASA)
European Innovation Council and SMEs Executive Agency (EISMEA) [ex EASME]
European Union Intellectual Property Office (EUIPO)
European Climate, Infrastructure and Environment Executive Agency (CINEA) [ex INEA]
European Banking Authority (EBA)
European Chemicals Agency (ECHA)
European Research Council Executive Agency (ERCEA)
European Research Executive Agency (REA)
European Systemic Risk Board (ESRB) *together with ECB*
Fusion for Energy
SESAR Joint Undertaking
Fuel Cells & Hydrogen Joint Undertaking
European Agency for Law Enforcement Training (CEPOL)
European Institute of Innovation and Technology (EIT)
European Defence Agency (EDA)
European Union Institute for Security Studies (EUISS)
eu-LISA
Bio-Based Industries Joint Undertaking
Europol
Shift2Rail Joint Undertaking
Single Resolution Board (SRB)
Eurojust
European Health and Digital Executive Agency (HaDEA) [ex CHAFEA]

NB: The two EUIs that were not yet operational at the time of the survey and did not receive the survey are the European Public Prosecutor Office (EPPO) and the European Labour Agency (ELA)