EUROPEAN DATA PROTECTION SUPERVISOR

# Orientations from the EDPS. Reactions of EU institutions as employers to the COVID-19 crisis


15 July 2020

**Executive Summary**

The European institutions, bodies and agencies have had to react to the COVID-19 crisis not only in their policy roles, but also in their roles as employers. Changes in operations, such as moving the vast majority of staff to remote working have raised numerous questions on which EUIs consulted the EDPS.

This document compiles the advice given on questions such as teleworking tools, staff management, health data aspects and replying to data subject access requests.

This document builds on the experience of the past months and addresses the issues that were raised to us or encountered by us and is still relevant because telework will most likely be a big part of the 'new normal' for EUIs work.

## TABLE OF CONTENTS

# Table of Contents

# 1 Introduction

The COVID-19 outbreak forced many EUIs to switch their operation almost exclusively to telework for most of their staff. EUIs have also made other adaptations to their operations and are planning measures to protect staff and visitors upon return to the office. However, the emergency of this situation does not mean that data protection rules applicable to EUIs can be set aside. **Data protection rules currently in force within the EUIs are flexible enough to allow for various measures in order to allow business continuity of EUIs operations and the EDPS is fully aware that some adaptations resulting from an emergency situation may require some time**. At the same time, there should be no doubt that the essential data protection requirements set out in Article 8 of the EU Charter of Fundamental Rights and in Regulation (EU) 2018/1725 (the Regulation), such as the principles of accountability, data protection by design and by default, security and transparency continue to apply. As public institutions, EUIs have to lead by example here, to protect the trust their staff, stakeholders, and the public at large place in them.

Although EUIs are already in the process of planning a possible gradual return to the office, telework is likely to remain a big part of the new normal for near future. This document builds on the experience of the past months and addresses the issues that were raised to us or encountered by us.

This document is addressed to controllers and Data Protection Officers (DPOs) in the EUIs. Controllers should consult their EUI's DPO early in the process of developing organisational responses to this crisis. DPOs guide and advise controllers, but in the end, controllers are accountable for compliance with the Regulation, so 'you' in statements such as 'you should do X' refers to the controller in this document.

# 2 Teleworking tools

The need for teleworking tools to keep up activities has grown dramatically in an extremely short timeframe, e.g. for conference calls, remote collaboration, audio- or videoconferencing or webinars. Some EUIs already had the necessary tools in place, while others are looking for solutions. If you already have signed contractual agreements with external providers for new products and services, in view of the urgency of the situation, you should start assessing these terms and conditions in order to check compliance with the Regulation or identify the steps to take to mitigate the risks of non-compliance.

Given the size of the market and the number of tools available, the EDPS cannot provide a full "buyers' guide" to such tools. If you provide the tools for various EUIs or join a group of EUIs to choose a service or software, you will need to check these issues for the benefit of all other EUIs concerned. Specific terms and conditions based on the Regulation may not be needed as long as similar elements complying with Regulation 2016/679 (GDPR) can already fulfil your needs (and as long as they do not contradict any additional/different requirements set out in the Regulation).

We can, however, provide some tips on the most common issues and pitfalls to look for and to help you choose data protection friendly tools:

## 2.1 Decision-making processes

Operational needs on exceptional circumstances should not lead EUIs to ignore data protection and security requirements when searching for adequate teleworking tools. Take into account that often there will not be a tool that serves all needs. So, EUIs are advised to state the use cases defining their requirements (including data protection safeguards) and look for those tools that best fit them.

Although the current situation may require quick decisions, you should **follow your EUI's established IT governance processes as far as possible** while, at the same time, proactively identify and address any data protection issue that may arise from the envisaged implementation of such tools (data protection by design). You need to involve your **DPO** in this process. Make sure that there is an overview of the tools used, a prior assessment on their security, confidentiality and privacy features and that your IT department can provide guidance, so your EUI can make an informed decision, preferably at the highest management level.

Otherwise, there may be a **risk that parts of your organisation start using freely available tools that may not be in line with your EUI's IT strategy**, may expose personal data or other confidential information to third parties or external attackers and expose your EUI to unnecessary reputational and other risks. Not addressing these issues now may create lock-in effects down the road, introduce critical data protection issues and additional security risks.

For guidance on these processes, please see the EDPS Guidelines on IT governance and IT management and the EDPS Preliminary Opinion on privacy by design.

## 2.2 Corporate and private devices

Aside from addressing IT security issues, great care should be taken in relation to data protection when private devices are used for teleworking. It is advised that when staff use private devices for teleworking (laptops, tablets etc.) your IT department should be consulted for potential security issues or specific configuration settings that have to be applied on them. Where personal data will be processed on personal devices, your institution should **provide the users with clear policies and instructions** on how to handle these personal data (e.g. as an IT Guidance on telework for the staff). Conversely, providing corporate equipment will give your EUI more control over the IT environment used by staff and reduce temptations for the so-called "shadow IT".

**Besides, be mindful of the principle of data minimisation and avoid unnecessary sharing of personal data when managing requests for corporate devices in your EUI**.

For more information on mobile device management, whether corporate devices or bring-your-own-device, please see the EDPS guidelines on mobile devices.

## 2.3 Controller/processor roles

Make sure that any software/service used does not reveal personal data on your staff and their communication partners to the vendor/software producer.

When relying on **external providers** for new products or services, EUIs should always aim at **privileging the most privacy friendly tools and ensuring that they have appropriate control over how external providers will handle the data entrusted to them**. Even if the contract relies on terms and conditions common to all customers (e.g. most online services), given EUIs' role as public service institutions, it is necessary to check the roles and the controls in place. Usually, a controller-processor relationship with your EUI being the controller offers

the highest amount of control for your EUI. To avoid any issue about who is responsible for the data processing activity, make sure that the controller and processor's roles and responsibilities are clearly identified. **Make also sure that your controller-processor agreements cover all the mandatory elements under Article 29(3) of the Regulation**, e.g. to have all the necessary information regarding the sub-processors which are part of the processing agreement.

For more information, please see Article 29 of the Regulation and the EDPS guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725.

## 2.4 Data processing in the EU/EEA and data transfers

If you have to rely on an external provider, then first check if one established in the EU/EEA satisfies your requirements and make sure that your controller-processor agreement complies with the requirements set out in section 2.3 (see above).

**Also when using such providers established in the EU/EEA, be sure to check if their services entail any transfers of personal data outside the EU/EEA**, including for purposes like backups, troubleshooting/customer support etc. Should that be the case, make sure that your provider has appropriate safeguards that meet the requirements set out under Chapter V of the Regulation in place, such as approved binding corporate rules.

If your external provider is not established in the EU/EEA and does not fall within the scope of an adequacy decision by the European Commission, then you need to obtain **appropriate safeguard**s under Article 48 of the Regulation.

For further information see the EDPS Information Note on international data transfers after Brexit, which contains an overview of the different transfer instruments available to EUIs beyond that specific context.

## 2.5 Functionalities for monitoring by employer or provider

Remote collaboration and videoconferencing tools often allow for additional monitoring of staff compared to "offline" collaboration. By default, there should be **no monitoring by employer or provider**.

Concerning **monitoring by the provider, check the description of their services to make sure that there is no monitoring in place and obtain additional contractual safeguards where required**.

Concerning **monitoring by the employer, configure tools in a way that avoids such data collection and be transparent about this to staff**. If some form of monitoring by the employer is required, you have to identify if these intrusive measures are proportionate to the aim to be achieved. You may want to consult our guidelines on proportionality on such issues and by applying the data protection by design and default obligations in order to achieve your aim while respecting your staff's right to privacy. In addition, bear in mind that staff is working from home, sometimes with their private device. Their home space and personal digital privacy should not be encroached upon. While the video-surveillance guidelines mainly deal with video-surveillance, sections on employee monitoring (page 20), areas under heightened expectation of privacy (page 21) and covert surveillance (page 23) may provide general guidance on staff monitoring while teleworking.

As a final practical point: videoconferencing tools usually allow for the recording of meetings. You should **follow the same approach for recording as you do for in-person meetings**: this will usually require obtaining **consent** from the people who will be recorded.

## 2.6 Data retention

Whether provided in-house or by external providers, make sure that any new tools are configured with **appropriate retention periods** in compliance with the purpose of the data processing activity. For **external providers, obtain a clear and binding commitment that your EUI's information is either returned to you or deleted at the end of the contract** (see also above on controller/processor - this is a mandatory requirement to impose on your processors, under Article 29(3)(g) of the Regulation).

## 2.7 Data security

Adopting new or increasing the use of existing teleworking tools may raise additional data security issues.

Your IT Department, in collaboration with your Local Information Security Officer (LISO) has to take the necessary measures to safeguard the confidentiality, integrity and availability of personal data processing performed by different electronic communication means: instant messaging platforms, online collaboration tools, webmail, videoconferencing tools etc. **Security requires the collaboration between IT departments, the LISO, the DPO and all users.**

As the response to the COVID-19 situation led to additional teleworking and a growing demand for external connection workload on the business network, this might lead to **possible deviation from standard processes** and potential inaccessibility of automated tools during telework, thus there is a **higher chance of data breaches due to human error**. The reporting obligations of personal data breaches remain. The EDPS guidelines on personal data breach notifications provide practical advice in this regard.

Identify and document alternative processes to be followed, make sure all your staff have a clear communication channel to the LISO and **raise staff awareness on common data breach sources such as increasing spoofing, phishing and social engineering attacks using COVID-19 related messages.** There have also been several reports of online conferencing tools being targeted, where hackers have gained unauthorised access to conversations and have sent phishing emails to steal credentials.

For new tools, general data security requirements under Article 33 of the Regulation and other obligations linked to information security continue to apply. For instance, best practice technologies based on cryptography should be employed on a risk-based approach in order to ensure end-to-end encryption (as opposed to point to point), the authenticity of the sender and the integrity of the information.

New contracts and Service Level Agreements with external service providers that provide IT services should be reviewed in order to ensure that they implement sufficient security measures.

This would also be an opportunity to review whether existing tools fulfil all these requirements set out above as well as update your current policies such as securities policy.

The EDPS Guidelines on the use of cloud computing services by the European institutions and bodies are still relevant here. You may also refer to the EDPS Guidelines on mobile apps. While they provide guidance to EUIs developing their own apps, the questions raised are also relevant to ask to providers of apps that your EUI may want to start using.

# 3 Health data issues

## 3.1 Role of medical services

In general, access to and processing of health data is limited to qualified healthcare professionals.

Your medical service is well placed to provide guidance on preventive measures internally. Staff (suspected of being) infected with COVID-19 have to cooperate with their care provider, competent national (public health) authorities and their EUI's medical service where appropriate**.**

Following the evolution of the clinical case is primarily the task of the treating physician. Nonetheless, like in any sickness leave, your EUI's medical service will be involved where required and necessary.

However, EUIs should be watchful of their staff's medical privacy and the additional requirements set out in Article 10 of the Regulation in relation to the processing of health data. Notwithstanding, considering the high contagious rate of COVID-19 and the duty of care of EUIs towards its staff, EUIs medical services may adopt additional follow-up measures towards suspect or confirmed cases.

If another EUI provides medical services to you under a SLA or similar, the same applies. It may make sense to have a reminder to the medical service providing these services to your EUI.

As already stated by the EDPS, this crisis might require temporary measures and thus any additional retention of data related to this crisis should also be temporary. It is good practice to address this issue early on and decide on triggering the deletion of this data after a defined public health milestone in the crisis is reached.

## 3.2 Exposure notification and contact tracing

Contact tracing is one of the tools at the disposal of public health authorities to control infectious diseases.

As already explained in earlier guidance[1], **should competent public health authorities contact EUIs as part of their national contact tracing activities, EUI can disclose relevant information** (e.g. people who have been in the same meeting, who share offices etc.) while preserving the medical confidentiality of such information as explained in section 3.1. What happens with data disclosed to the competent national public health authorities? They have to process them in line with the applicable legislation.

In some EU Member States, COVID-19 is a notifiable communicable disease, so the general practitioner who has made the diagnosis will report a positive case to public health authorities (including the person's name, and the public health authority will get in touch with them for contact tracing). Informing colleagues of the identity of a confirmed case: when doing 'old school' contact tracing, public health authorities are very careful not to disclose that information.

This means GDPR and the legal acts assigning these tasks to competent national authorities apply to their further processing. The competent authorities are separate controllers from the

[1] Message to all EUI DPOs of 12 March 2020

EUIs here. Retention periods, data subject rights etc. follow the procedures adopted by the competent authorities. The relevant national DPA supervises their compliance with the GDPR.

### 3.3 Social and private aspects

EUIs should not divulge the identity of confirmed cases to the staff at large. That said, in case a staff member voluntarily mentions their own health condition to colleagues, data protection rules **do not block social initiatives organised among colleagues to e.g. send flowers or a card**.

## 4 Data subject rights

Furthermore, the coronavirus crisis **does not suspend data subject's rights and they are entitled to exercise their rights,** unless specific, duly adopted and documented restrictions under Article 25 of the Regulation apply.

Make sure that you have remote access to the information systems for access requests. Should you still face a situation where your EUI will not be in a position to timely reply to requests, you should document the underlying reasons and decision-making, as well as communicate to data subjects, prior to the expiry of the statutory deadline, that there will be a delay in responding to their requests, the reason thereof and the expected duration of the delay.

## 5 EDPS assisting EUIs

During this crisis, it is still essential to comply with the requirements set out in the Regulation. For instance, please make sure to regularly update your register of processing operations and comply with any need for a DPIA. Under the principle of accountability, there should be an evidence trail to document the decisions taken in relation to data protection issues.

The EDPS is aware that it is currently a testing time for all EUIs. As previously stated and as the present document illustrates, the Regulation applies and is flexible enough to be adapted to this current environment.

When the crisis recedes (or in reaction to complaints received), the EDPS may review the actions taken by your institution during this crisis in relation to data protection.

We remain available to assist you and to provide informal or formal specific guidance on any matter related to this crisis.