

The EU's data protection regime includes a number of exceptions to the application of its framework of rights and responsibilities. These provide the basis for the processing of information in light of certain contexts. They are strongly related to the operation of a collaborative information management system as they can provide ways of legitimately processing data in an emergency situation. The specific legal basis on which the processing is based will depend on the actors involved and the purposes of the processing. Within the context of PPDR and DRM we can identify the following legal bases:

Article 6(d) of the GDPR states that personal data can be processed when this is in the vital or essential interests of the data subject. Recital 46 of the GDPR further clarifies that this legal basis could be relied upon specifically within the context of a natural or manmade disaster. Consequently, this provision could serve as the legal basis for the processing of personal information that relates to the victims of a disaster.

The processing of personal data of affected people could also fall within the scope of Article 6 (e). According to this paragraph, the processing of personal data is lawful if the "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed".

On the other hand, first responder agents using the collaborative platform will undoubtedly exchange information that relates to their forces active on the terrain. In this case the first responder agencies will have to base the processing operation of personal information concerning their employees on their legitimate interest as provided by article 6(f) GDPR. If volunteers are working on behalf of a first responder agency, the processing of their data could also be based on consent.

Guiding Questions

How does the GDPR strengthen the need for end user consent in relation to data processing?

What are the exceptions to the requirement of consent and how do they operate?

At what point does an exception lapse and what steps should be taken to deal with the data at this point?

Does the lawfulness of the processing vary according to the specific situation of the person concerned?

Further Information

A first general principle that applies to the processing of personal data is lawfulness. This means that you need to invoke a specific legal basis to legitimise the processing of personal data. Consent is one of them but the GDPR contains a whole range of diverging legal bases. There is also a need to address the extent to which the exceptional situation is on-going. Clear rules laid down in association with the data protection impact assessment process can aid data controllers to put in place strategies to deal with lawful processing in exceptional situations.

Examples

When a first responder agency acts during a crisis, it only needs consent for the processing of the data concerning volunteers. For the victims and the employees of the agency, other processing grounds exist in order to justify the legitimacy of the processing.

Resources

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of “controller” and “processor” [[Link](#)]

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [[Link](#)]

GDPR Overview of the General Data Protection Regulation (2017). Information Commissioner’s Office [[Link](#)]