Law Enforcement Directive

FRP questionnaire

NOTE: This short brief is an internal document that was produced by FRA to support the Commission's work. It is not to be distributed further and is not an official output of the Agency.

Overview of responses

A total of 804 organisations from the FRA's Fundamental Rights Platform (FRP) received a short questionnaire on the law enforcement directive. Two reminders were sent, and an additional week was provided after the deadline of 22 October 2021 for participants to respond.

- FRA received 88 responses. However, out of those, 55 responses were incomplete.
- Out of the remaining 33 responses, nine responded either 'no' or 'don't know' to both introductory questions:

1. *'Is the protection of individuals' fundamental rights in the context of law enforcement one of the areas of work for your organisation?', and*
2. *'Are data protection and the right to privacy among the areas of work for your organisation?'*

These nine respondents did not go further in the questionnaire.

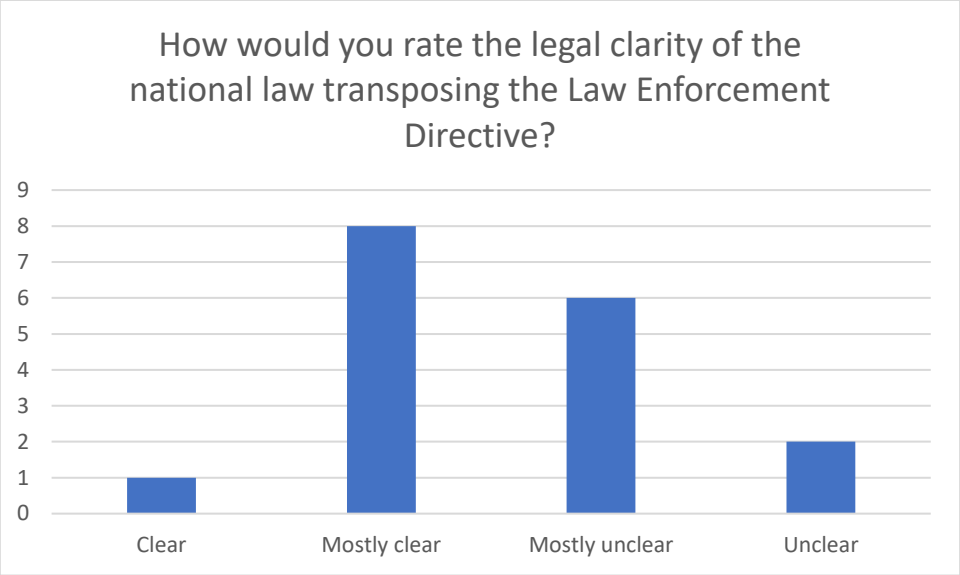
- Finally, seven respondents indicated either 'not at all familiar' or 'don't know' to the question:

'How familiar are you with the Law Enforcement Directive in the context of your work?'
These seven respondents did not provide further replies to the questionnaire.

Consequently, FRA received 17 full replies. This analysis is based on these 17 replies.

Given the very low number of complete responses - the findings should be treated with caution and cannot be taken to represent the situation in the EU. However, the results do identify some points of interest.

1. Clarity of the law



N=17

Out of the five respondents that indicated that they were ***very familiar*** with the Law Enforcement Directive in the context of their work, two indicated that the national law transposing the document was 'mostly clear' or 'clear', while three indicated that the national law was either 'unclear' or 'mostly unclear'.

When requested to provide clarifications:

- one of the respondents mentioned the incomplete transposition of the Directive into national law, referring to the opinion of the national DPA and a complaint to the European Commission for failing to properly implement the provisions of the LED.
- a second respondent indicated that although the LED was transposed almost "word by word" into national law, the legal basis for processing personal data was very limited, describing personal data in very broad categories, and allowing for very long data retention.

Out of the eight respondents that indicated that they were ***somewhat familiar*** with the Law Enforcement Directive in the context of their work, six indicated that the national law transposing the document was 'mostly clear', while two indicated that the national law was 'mostly unclear'.

When requested to provide clarifications:

- Both respondents referred to the terminology, stating that some wording was "biased or not clear", or "Unapproachable for the man in the street".

Out of the four respondents that indicated that they were ***not at all familiar*** with the Law Enforcement Directive in the context of their work, one indicated that the national law transposing the document was 'mostly clear', while three indicated that the national law was either 'unclear' or 'mostly unclear'.

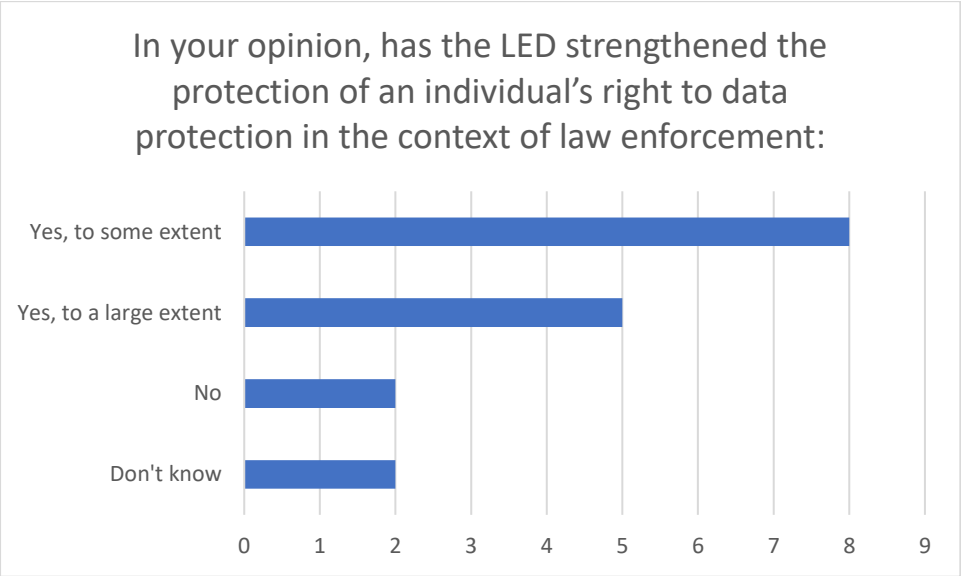
When requested to provide clarifications:

- One refers to an absence of communication: "the law is not sufficiently publicised and we do not receive support"
- One refers to the slowness and absence of publication of the transposition process, and

- One refers to the absence of clarity with regards to the institution in charge of enforcing the law - “it is still unclear to me and my organisation how and by who this law is being enforced. Those supposed to protect individuals’ data are the ones who breach it the most.”

One respondent found the *national law* to be clear, eight to be mostly clear, six to be mostly unclear.

2. Strengthening of data protection in the context of law enforcement



N=17

Out of the four respondents that indicated either that they believe the LED did ***not strengthen*** data protection in the context of law enforcement, or that they ‘don’t know’,

- two referred to the national enforcement capability, stating that either the sanctioning regime was “non-existent”, or that the authorities in charge of the enforcement of the LED were “breaching them and abusing powers”, and
- one referred to the absence of any real change introduced in comparison to the previous regime, notably because a provision from the previous regime was maintained, that would result in the exemption of personal data from data subject rights (in specific areas) under the LED.

Out of the eight respondents that indicated they believe the LED strengthened data protection in the context of law enforcement ***to some extent***:

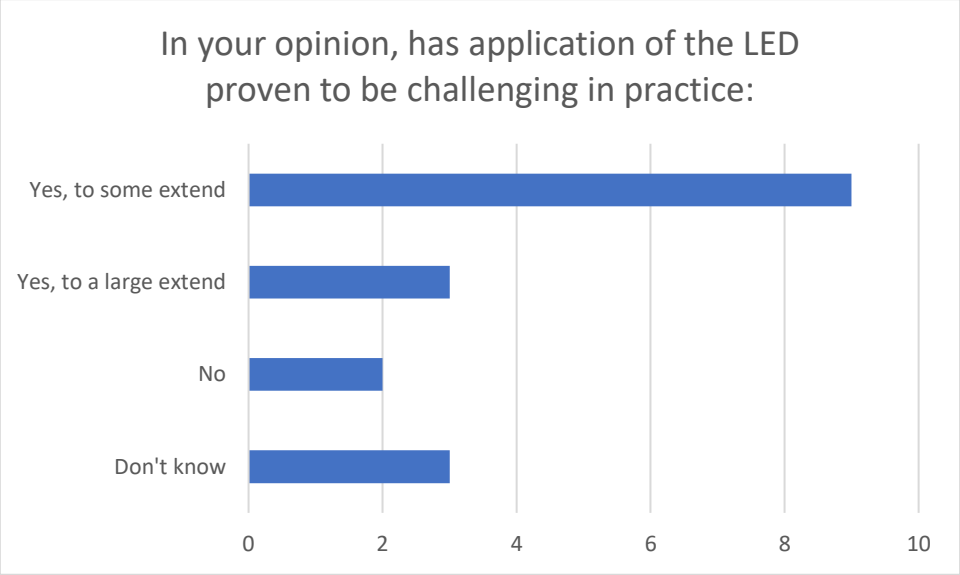
- One referred to the complexity of the national law
- Two to the fact that the enforcement was rather theoretical, one because of the absence of general public awareness, and the other one because of the insufficiency of control mechanisms

- Two refereed to the narrow scope of the Directive: “there are still many areas in which governments can invade privacy under the guise of ensuring public order”, and “the decree does not apply to data processing carried out in the course of activities concerning national security and carried out by EU bodies or agencies”.

Out of the five respondents that indicated that they believe the LED strengthened data protection in the context of law enforcement ***to a large extent***:

- One clarified that society is more attentive to this matter because they have witnessed a “change in the behaviour of the main public institutions and other private entities.”
- Two referred to the broad protection of the LED, with one clarifying though, that while the LED does provide for important novel safeguards (and notably the DPIAs, DPO, Prior Consultation with DPAs, logging, records of processing activities), it has remained a “paper tiger”.

3. Challenges in the practical application of the law



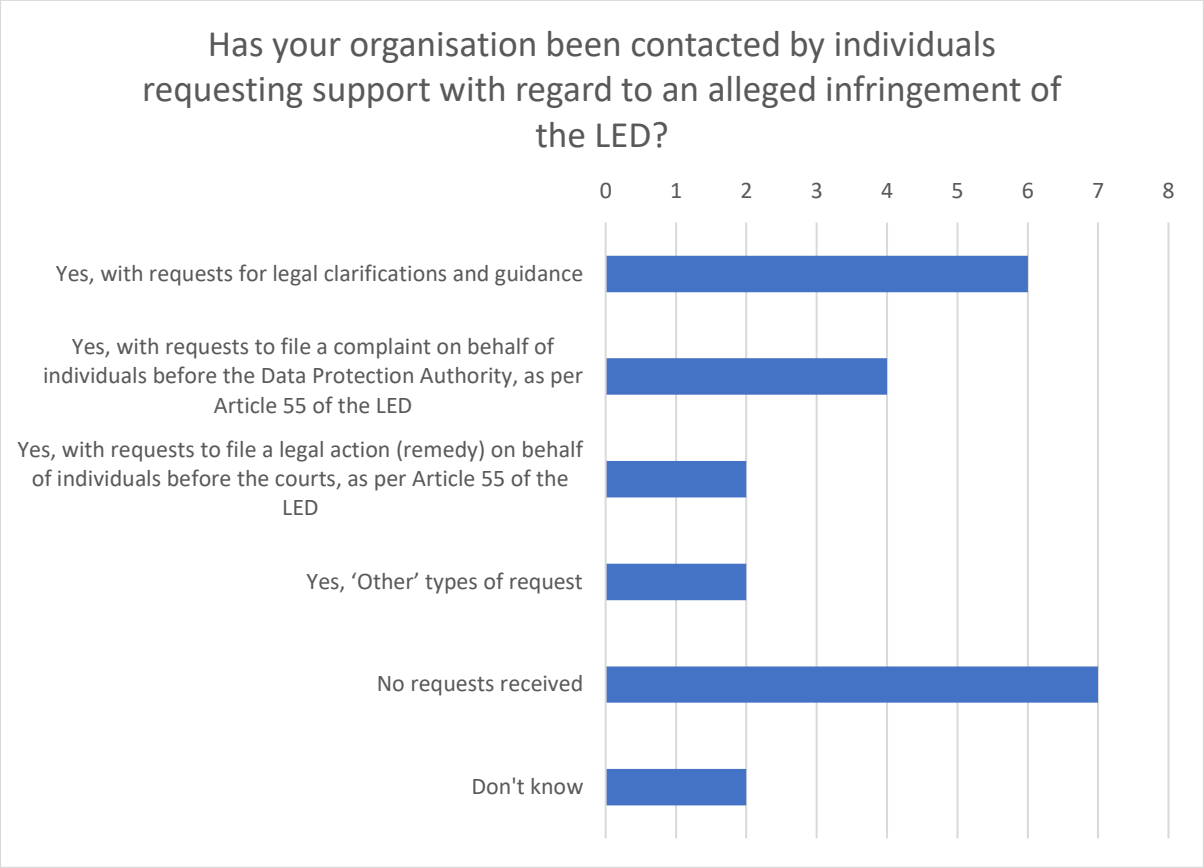
N=17

Out of the twelve respondents that indicated that the application of the LED proved to be challenging to some extent or to a large extent, the following challenges were indicated:

- The exponential growth of the data exchange among the online services' users or within various fields (such as business or social protection). Notably for children, that “remain the most vulnerable category of data users and providers”. (1 reply)
- The complexity of the law, and notably the fragmentation of the categories to which the directive applies can create challenges for what concerns the real aim of the directive. (2 replies)
- The difficulty to address public institutions: some respondents referred to “abusive interpretation” or to “the difficulty to prove a government breach” (2 replies)

- The lack of effective and harmonised tools for implementation: “it would be important that adequate EU funds are allocated for the functioning of DPAs around the EU, so that the European Commission ensure that there is no two speed Europe, of the rich north DPAs and the poor south DPAs.” (2 replies)
- The public is not properly informed, and therefore cannot exercise their rights – such as data access requests. (3 replies)
- Law enforcement officers need appropriate training on the LED (1 reply)

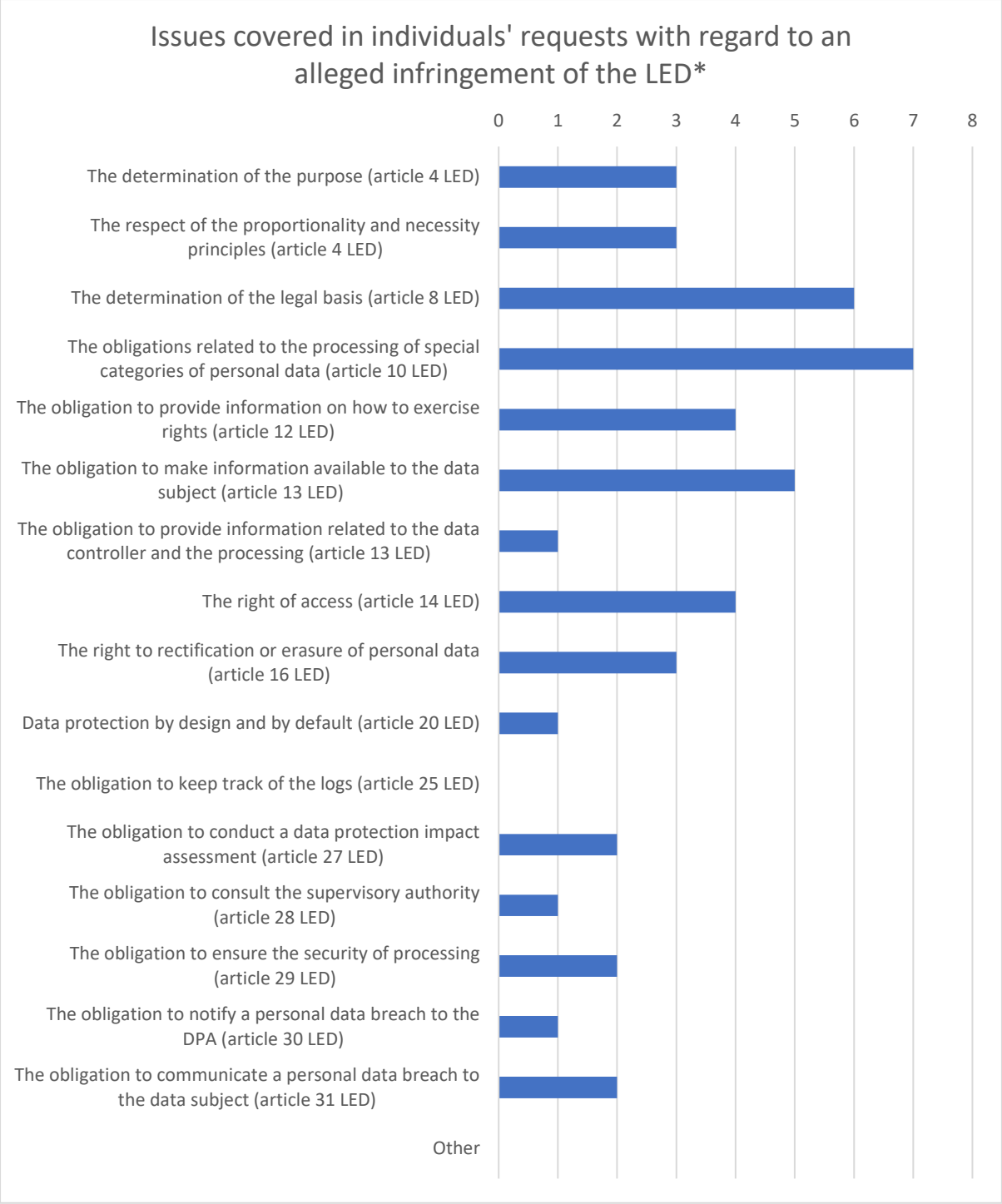
4. Individuals’ requests



N=17
**Multiple choice question.*

Respondents clarified that the two other types of requests – under the category ‘Other’ – were:

- misuse of children's data by different institutions (such as school, social services), and
- private information leaked by services providers and in particular the police, Human Resources, recruitment agencies, health services, asylum and refugees’ cases, immigration matters.



N=17
**Multiple choice question.*

Of those organisations that clarified the number of individuals' requests with regard to an alleged infringement of the LED they received, the following information was provided:

- For legal clarifications and guidance:
  - one organisation specified "many times"
  - one organisation between 20 and 30 times, and
  - three organisations between one and three times.

- For requests to file a complaint on behalf of individuals before the Data Protection Authority:
    - three organisations specified one time, with one clarifying that the request related to "the deletion of biometric data (fingerprints and facial images) retained in a central police database for national passport holders",
    - one organisation did not specify how many requests were received, but indicated that while some requests were introduced, people tend to abandon the request because of the complexity.

- For requests to file a legal action (remedy) on behalf of individuals before the courts:
    - One organisation indicated one case, and
    - One organisation clarified that they have "none because applicants lack often resources to take legal actions due to financial barriers".

- Three organisations mentioned other types of requests (between 1 and 15), but only one clarified the type: mediation (15)

N=17
**Multiple choice question.*

Three organisations clarified the other types of actions – under the category 'Other':

- Mediate the communication with other institutions.
- Ask for clarifications
- Assistance to others with filing complaints