# ADMINISTRATIVE FINES AND SANCTIONS UNDER REGULATION (EU) 2018/1725 – EDPS

## Recital 81 + Article 66

Factors to consider in deciding whether to impose a fine pursuant to Art. 58(2)(i) and in establishing the amount of the fine:

Fines as sanctions of last resort:
– where the EUI fails to comply with an order by the EDPS to:
- **comply with** the data subject's **requests to exercise rights** pursuant to the EDPR;
- **bring** processing operations **into compliance** with the EDPR;
- **communicate a personal data breach** to the data subject;
- **temporarily or definitively limit or discontinue** a processing activity;
- **rectify, erase, restrict** the processing of personal data and **notify** such actions to recipients to whom the personal data at stake have been disclosed;
- **suspend data flows** to a recipient in a Member State, a third country or an international organisation

– and depending on the circumstances of each individual case

Review by Court of Justice – Art. 64(3)

Two different classes of fines – Art. 66(2) and (3)

Mitigating and aggravating circumstances – Art. 66(2)

Maximum amount of the fine in case of infringements in the context of a continuous processing – Art. 66(4)

## Recital 81

In order to strengthen the supervisory role of the European Data Protection Supervisor and the effective enforcement of this Regulation, the European Data Protection Supervisor should, as a **sanction of last resort**, have the power to impose **administrative fines**.
The fines should aim at sanctioning the Union institution or body — rather than individuals — for non-compliance with Regulation (EU) 2018/1725, to **deter future violations** of Regulation (EU) 2018/1725 and to **foster a culture of personal data protection** within the Union institutions and bodies. ...

**Progressive approach** by EDPS → issue:
- **warnings** that the intended processing operations are likely to infringe Regulation (EU) 2018/1725 (Article 58(2)(a)) ;
- **reprimands** where the processing has infringed Regulation (EU) 2018/1725 (Article 58(2)(b)) - for minor infringements (e.g. only one person affected by the infringement; no significant harm for the data subject; no previous or structural issues encountered by the EUI in this regard)
- **orders** (Article 58(2)(d) to (h) and (j))

**before** starting the proceeding on **administrative fines** in case of non-compliance with an order of the EDPS

## Article 66(1)

**whether to impose** the fine and the **amount** of the fine:

a) **nature, gravity and duration of the infringement** + **nature, scope or purpose of the processing** + **number of data subjects affected** + **level of damage suffered** by them;

b) **action taken by the EUI to mitigate the damage** suffered by data subjects;

c) **degree of responsibility** of the EUI + **technical and organisational measures implemented** by them pursuant to Articles 27 and 33;

d) **similar previous infringements** by the EUI;

e) **degree of cooperation with the EDPS** to remedy the infringement and mitigate the possible adverse effects of the infringement;

f) **categories of personal data affected** by the infringement;

g) **manner in which the infringement became known to the EDPS**, in particular whether, and if so to what extent, the EUI notified the infringement;

h) **compliance with any of the measures** referred to **in Article 58 previously ordered** (+ warnings, reprimands, referral of the matter) against the EUI concerned **with regard to the same subject-matter**.

+ **when imposing** the fine on an EUI: **proportionality of amount** of the fine.

## Article 69 of EDPR = Art. 49 of Reg. 45/2001

Where an **official or other servant** of the Union
fails to comply with the obligations laid down in *Regulation (EU) 2018/1725*,
whether **intentionally or through negligence** on **his or her part**,
the official or other servant concerned shall be liable to
**disciplinary or other action**, in accordance with the rules and procedures laid down **in the Staff Regulations**.

*Example: data breach committed by the official unlawfully accessing the email account of a colleague via his or her computer and further disclosure of the content of the emails to his or her friends*

Communication from vice-President Kinnock to the **Commission**, SEC(2004)730, at page 4, Section 2.3.1. of the **Guidelines for applying Article 22 of the Staff Regulation**:
"**the misconduct must be personal**". "The personal dimension of the misconduct must be established for each official and other servant on **a case-by-case basis** in the light of **his/her individual action and failures to act which resulted in a damage**."; "serious personal misconduct on the part of a subordinate does not ipso facto entail serious personal misconduct on the part of his/her superior or vice versa."

EDPS to take into account the outcome of the disciplinary proceeding against the staff member to better ascertain unlawful processing by staff member:
- due to personal misconduct, acting in his or her individual capacity → individual responsibility excluding the responsibility of the EUI → sanctions in SR by EUI
- as implementing action of an EUI's policy → responsibility of the EUI → admin fine by EDPS
- due to structural issues in an EUI that should have been addressed by the EUI for the performance of its tasks → responsibility of the EUI → admin fine by EDPS

## Regulation (EU) 2018/1725 (EDPR)

| ***Category 1 Infringements*** maximum fine of 25 000 EUR per infringement and of 250 000 EUR per year | ***Category 2 Infringements*** maximum fine of 50 000 EUR per infringement and of 500 000 EUR per year |
|---|---|
| **Infringements for which fining is explicitly set out in Art. 66(2) of the EDPR** | **Infringements for which fining is explicitly set out in Art. 66(3) of the EDPR** |
| **Art. 8** - Conditions applicable to a child's consent in relation to information society services | **Art. 4** - Principles relating to processing of personal data |
| **Art. 12** - Processing which does not require identification | **Art. 5 -** Lawfulness of processing |
| **Art. 27** - Data protection by design and by default | **Art. 7 -** Conditions for consent |
| **Art. 28** - Joint controllers | **Art. 10** - Processing of special categories of personal data |
| **Art. 29** - Processor | **Art. 14 -** Transparent information, communication and modalities for the exercise of the rights of the data subject |
| **Art. 30** - Processing under the authority of the controller or processor | **Art. 15 -** Information to be provided where personal data are collected from the data subject |
| **Art. 31** - Records of processing activities | **Art. 16 -** Information to be provided where personal data have not been obtained from the data subject |
| **Art. 32** - Cooperation with the European Data Protection Supervisor | **Art. 17 -** Right of access by the data subject |
| **Art. 33** - Security of processing | **Art. 18 -** Right to rectification |
| **Art. 34** - Notification of a personal data breach to the European Data Protection Supervisor | **Art. 19 -** Right to erasure ('right to be forgotten') |
| **Art. 35** - Communication of a personal data breach to the data subject | **Art. 20 -** Right to restriction of processing |
| **Art. 39** - Data protection impact assessment | **Art. 21 -** Notification obligation regarding rectification or erasure of personal data or restriction of processing |
| **Art. 40** - Prior consultation | **Art. 22 -** Right to data portability |
| **Art. 43** - Designation of the data protection officer | **Art. 23 -** Right to object |
| **Art. 44** - Position of the data protection officer | **Art. 24 -** Automated individual decision-making, including profiling |
| **Art. 45** - Tasks of the data protection officer | **Art. 46 -** General principle for transfers |
| | **Art. 47 -** Transfers on the basis of an adequacy decision |
| | **Art. 48 -** Transfers subject to appropriate safeguards |
| | **Art. 49 -** Transfers or disclosures not authorised by Union law |
| | **Art. 50 -** Derogations for specific situations |
| **Infringements for which fining is not explicitly set out in Art. 66(2) or (3), but could be sanctioned in line with Art. 66(1) as failure to comply with order under Art. 58(2)(e) of the EDPR** | **Infringements for which fining is not explicitly set out in Art. 66(2) or (3), but could be sanctioned in line with Art. 66(1) as failure to comply with order under Art. 58(2)(e) of the EDPR** |
| **Rec (49) EUDPR in connection with Art. 42 GDPR** - Certification of EUI | **Art. 6 -** Processing for another compatible purpose |
| **Art. 26 -** Responsibility of the controller | **Rec (21) in connection with Art. 5 -** Transmission of personal data within the same Union institution or body and the recipient is not part of the controller, or to other Union institutions or bodies |
| **Art. 37** - Protection of information transmitted to, stored in, related to, processed by and collected from users' terminal equipment | **Art. 9 -** Transmissions of personal data to recipients established in the Union other than Union institutions and bodies |
| **Art. 38** - Directories of users | **Art. 11 -** Processing of personal data relating to criminal convictions and offences |
| | **Art. 13 -** Safeguards relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes |
| | **Art. 25 -** Restrictions |
| | **Art. 36** - Confidentiality of electronic communications |