



Mission: GDPR

Experience of Lithuania

Raimondas Andrijauskas

Director

State Data Protection Inspectorate

26 November 2019



Before GDPR

After GDPR



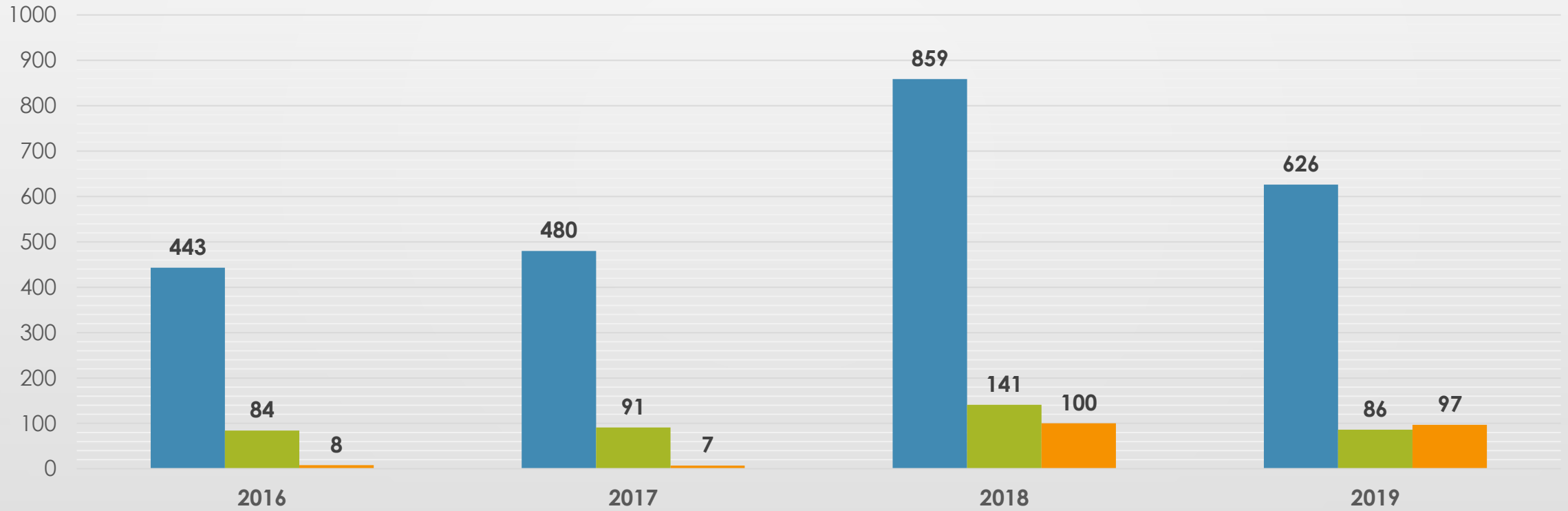
25th May 2018

Statistics



Supervision activities

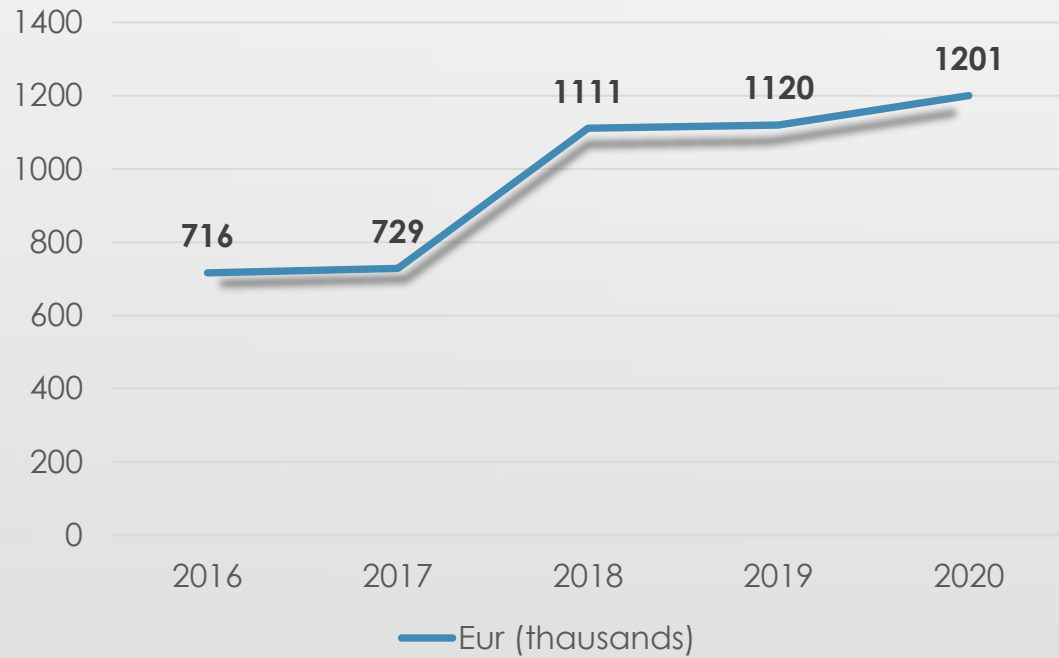
■ Complaints ■ Investigations OI ■ Notifications



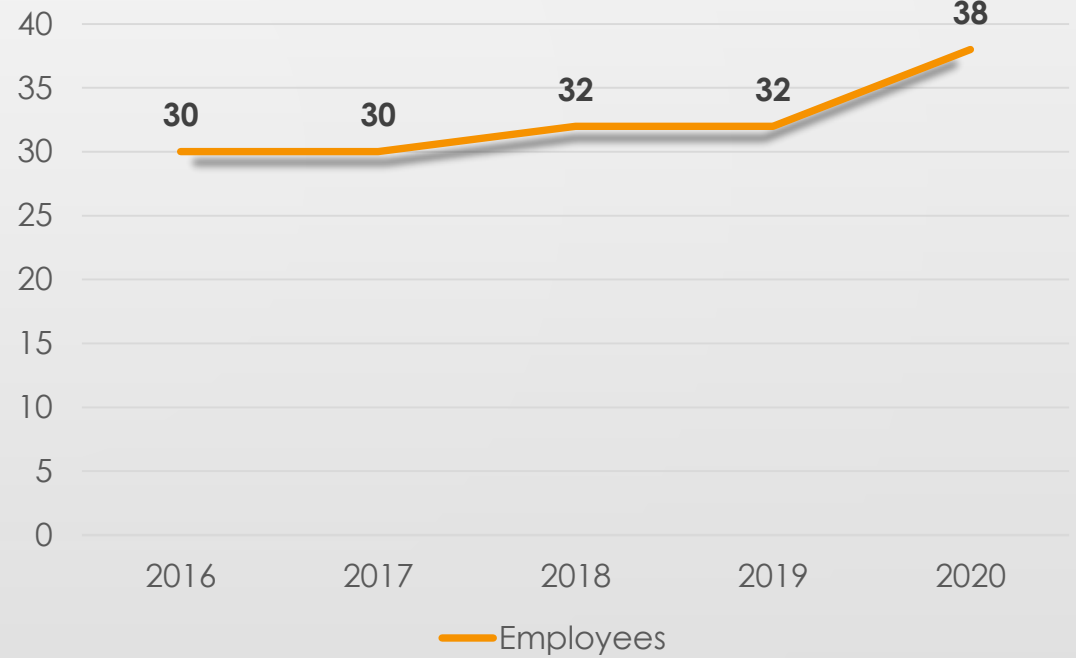
Resources



Budget



Employees



Awareness Raising



2017



☐ Consultations **5696**

☐ Public Information means **136**

☐ Presentations at events **37**

☐ Meetings **69**

☐ Attendance **1963**

2018



☐ Consultations **6298**

☐ Public information means **233**

☐ Presentations at events **77**

☐ Meetings **97**

☐ Attendance **4720**

2019



☐ Consultations **3648**

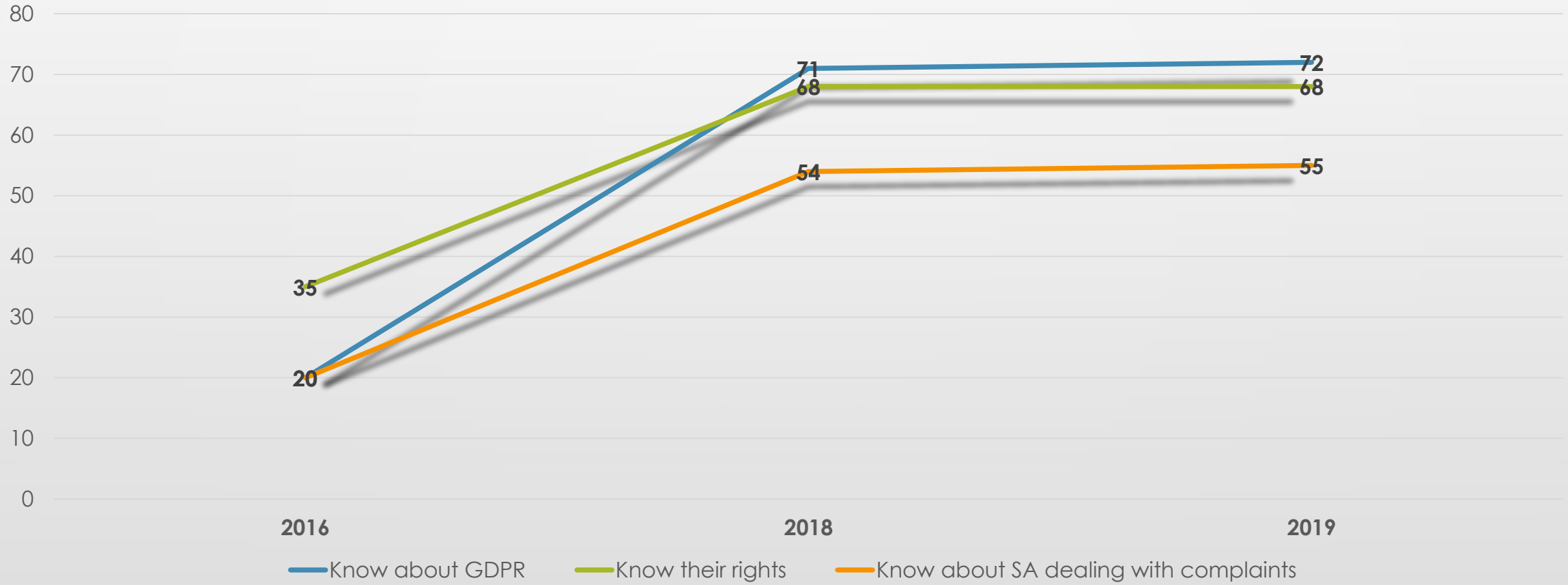
☐ Public information means **158**

☐ Presentations at events **21**

☐ Meetings **70**

☐ Attendance **1500**

Public Surveys Results



Complaint Handling



- **General Data Protection Regulation (GDPR)** came into force on **2018-05-25**
- Amendment to **Law on Legal Protection of Personal Data (LLPPD)** adopted on 2018-06-30, came into force on **2018-07-16**.
- Main elements of complaints handling procedure (terms, subjects rights, content of complaint and etc.) are set in **Chapter 5 Section 3 of LLPPD**
 - LLPPD also provides possibility for SDPI to approve detailed procedures for complaint handling
- SDPI Director Order No 1T-92(1.12.E) of 2019-07-17 „On Approval of Rules for Conducting Investigations and Verifications“

What is complaint?



- GDPR talks about complaint handling, but there is no definition of the complaint
- **Complaint** (Law on Public Administration) - a written application by a person to a public administration entity stating that his or other person's rights or legitimate interests have been violated, and asking that they be defended
- LLPPD states that the complaint could be applied by **data subject about his rights or legitimate interests violations**

What is complaint?



Complaint

- Written application by a data subject to the SDPI stating that his rights or legitimate interests have been violated, and asking that they be defended

*Notice, request,
anonymous
complaint*

- Any other information related to data protection issues which could be used to decide whether to start an investigation on SDPI initiative

Data breach
notification

- Mandatory data controllers (data processors) written notice to SA about personal data breach

Complaint Handling Process

Filing a complaint

Content:

Consignee (SA)

Date

Complainant (his representative) name, surname, contact details (power of attorney)

The person complained of

Description of complained acts (inaction), time, circumstances

Request for SA

Signature

Acceptance / refusal of complaint

Acceptance (3 w. days):

Written response

Acceptance date and registration No

Contacts of the person investigating the complaint

Information about complainant rights

Refusal (5 w. days):

Content requirements are not met (if without this information complaint couldn't be solved)

SA has no competence

Case was already solved within SA (national or other EU SA)

Complaint is pending in national or EU court

pre-trial investigation is under way

More than 2 years elapsed between complained actions and filling of the complaint

Investigation

Documentary check (obligation to provide SA with related documents and information)

On-site visiting (if needed)

Legal and technical (if needed) analysis

Information notice for the complainant about complaint handling progress (**after 3 months** of complaint handling)

Decision (4/6 month)

Complaint or part of it is reasonable

If reasonable, could be set any of the corrective measures mentioned in Art 58 (2) of the GDPR (except administrative fine)

If it is decided to impose a fine, the fine imposition procedure (notice to the data controller) is started

Complaint or part of it is unreasonable

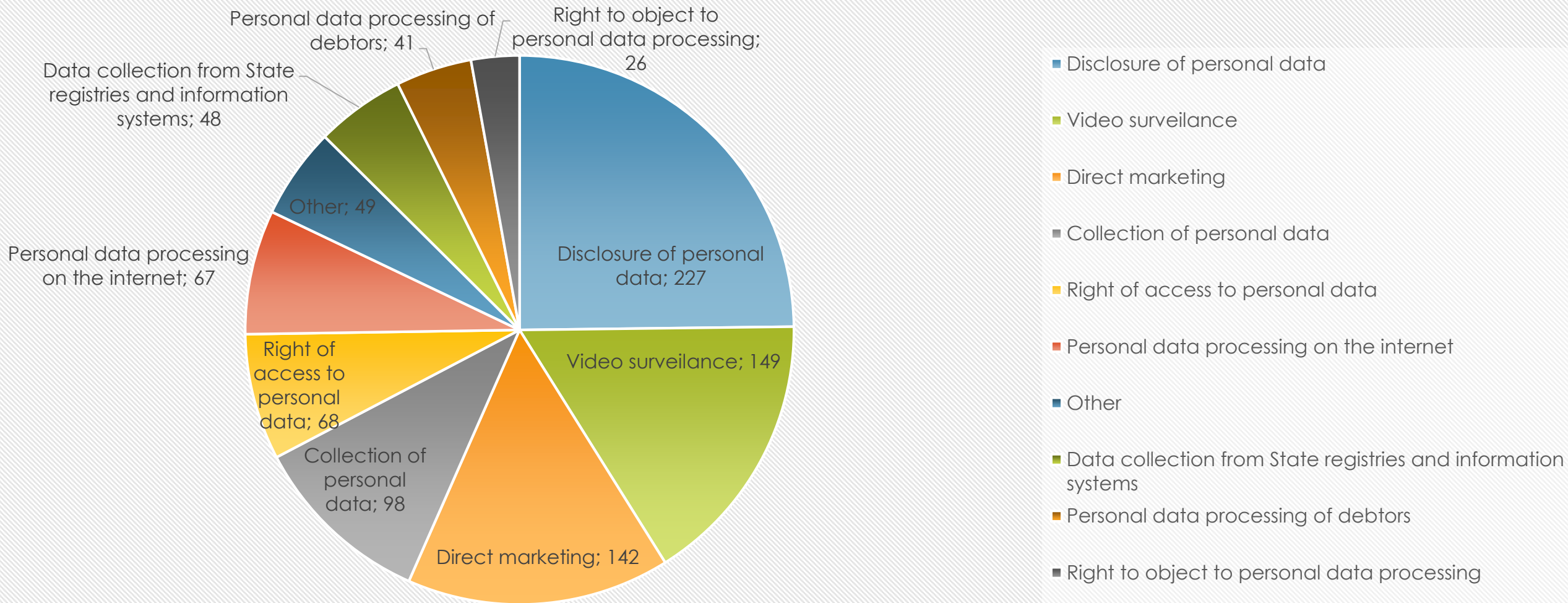
Termination of the complaint (exceptional cases)

Complainants request to terminate complaint handling

Complainant doesn't provide SA with necessary documents or information

Death of complainant and etc.

What is being complained about



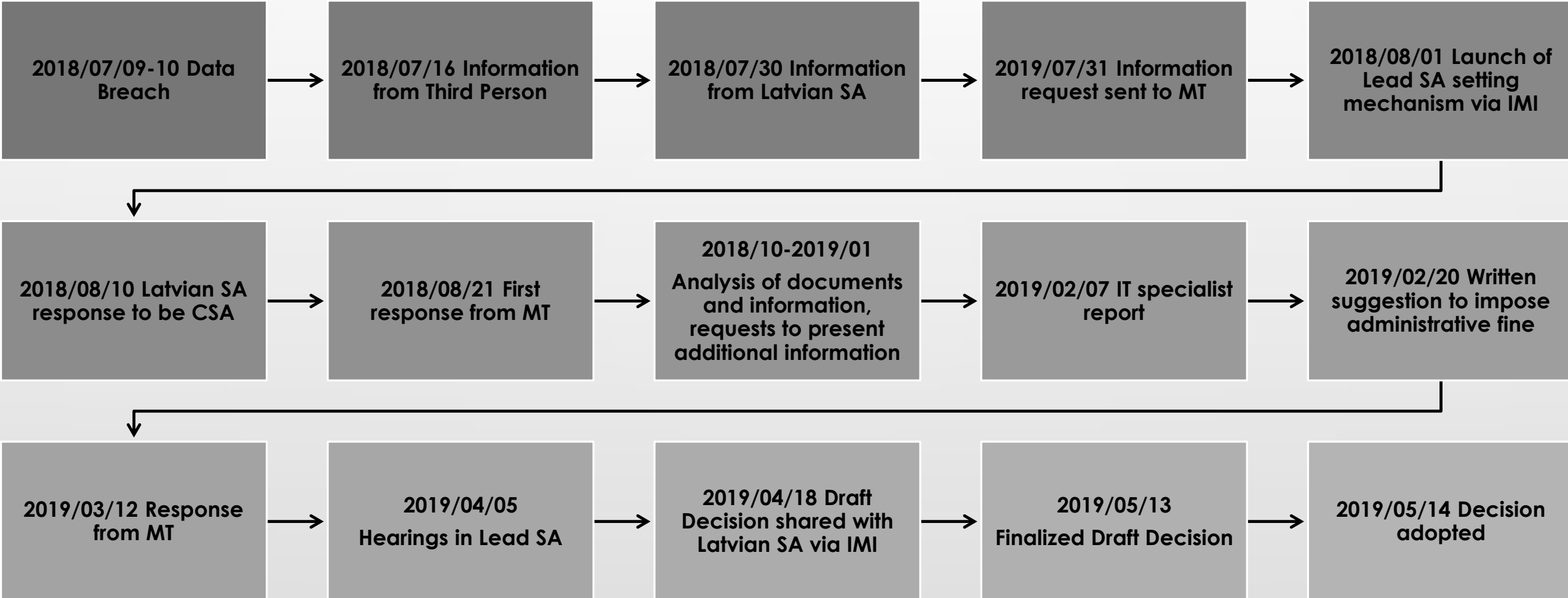
One-Stop-Shop Experience



Brief summary:

- **2018/07/16** Information from Third person about possible Data Breach (occurred 9-10th of July) in MisterTango (similar information was received from **Latvian SA 2018/07/30**)
- MisterTango is financial services providing company that has right to provide **Payment initiation service (PIS)** (Payment initiation service provider (**PISP**))
- Investigation duration (from receiving information to making a decision) – **10 months**
- **Lead SA – Lithuanian SA, Concerned SA – Latvian SA**
- Lithuanian SA's personnel involvement – **4 persons** (3 legal specialists (incl. Director) and 1 IT specialist)
- Administrative fine of the GDPR infringements – **61 500 Euro** (2,5 percent from total income).
 - Main Issues:
 - Lack of fairness and transparency (no information for data subjects about the processing of screenshots of their bank accounts for PIS purposes)
 - Not all processed personal data was necessary in relation to the PIS purposes (data minimisation principle)
 - Storage of personal data (Screenshots) for longer term than they themselves set (storage limitation principle)
 - Have not notified SA about Data Breach
 - Inappropriate technical and **organisational** measures (logs were not presented, 1 person responsible for all the IT matters)
- First case within OSS mechanism with the ending of administrative fine (still of the highest amount)
- Decision was appealed to the Administrative Court

One-Stop-Shop Experience (Timeline)



Lessons



- **Practical:**

- Issues with new developed IMI system (launch of related procedures, translations, responds, etc.)

- **From legal point of view:**

- The fine imposition procedure does not have clear provisions in case where OSS mechanism is triggered:
 - Time limits for conducting investigations and decision making
 - No provisions for suspension of time limits