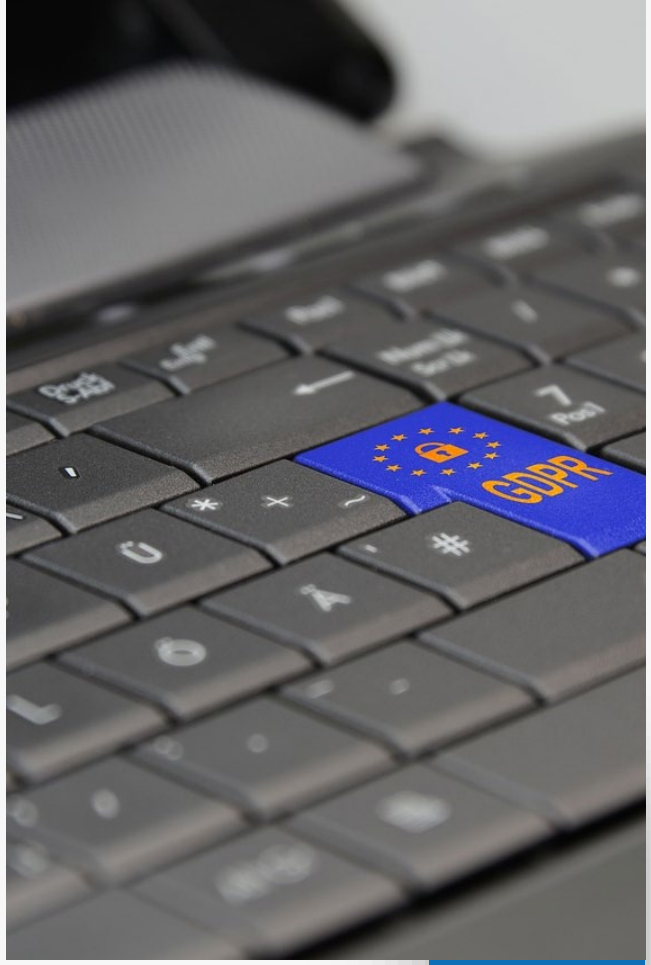
IKF

General Data Protection Regulation (GDPR) in practice

Mikis Moselt, Przemyslaw Kniaziuk| Interact | 02.04.2023

Interact

Co-funded by the European Union
Interreg



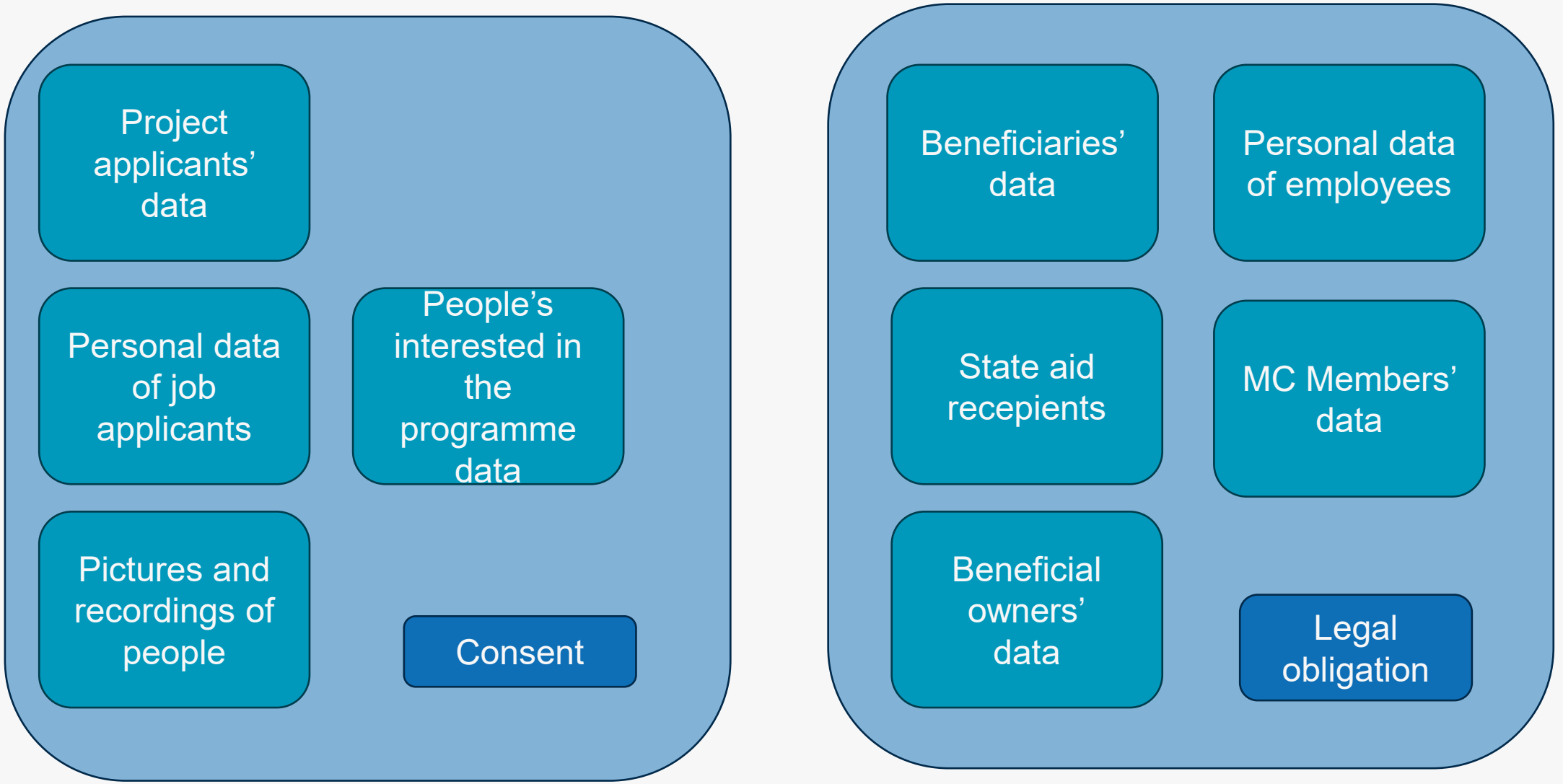
GDPR -
6 (8) years after

Prevention is better than cure

Learn from the mistakes of others. You can't live long enough to make them all yourself.

Anna Eleanor Roosevelt

GDPR in Interreg

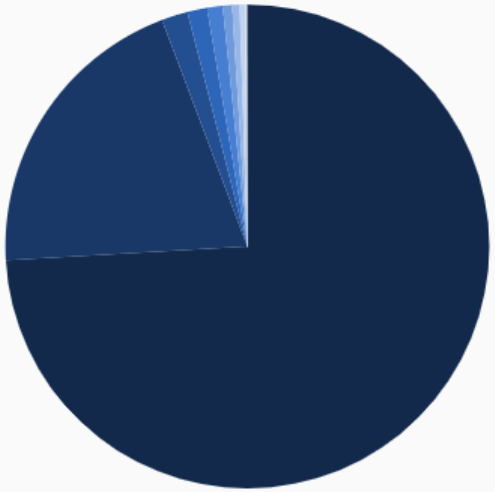


Administrative fines for public authorities?

Fines can be imposed on public authorities	Fines cannot be imposed on public authorities
• Bulgaria (and the highest fine to date was imposed against an authority); • Italy; • Netherlands; • Poland (with significant limitation, up to PLN 100,000 (approx. EUR 21,740) for public institutions and up to PLN 10,000 (approx. EUR 2,174) for cultural institutions); • United Kingdom (strategy for greater use of its wider powers in relation to the public sector (including warnings, reprimands and enforcement notices), and reserve fines only for the most serious cases.	• Austria; • Belgium (except in cases where public bodies would offer services or goods on the free market); • Czech Republic; • France; • Germany; • Hungary; • Norway; • Spain.

Some statistics

1. By total sum of fines:

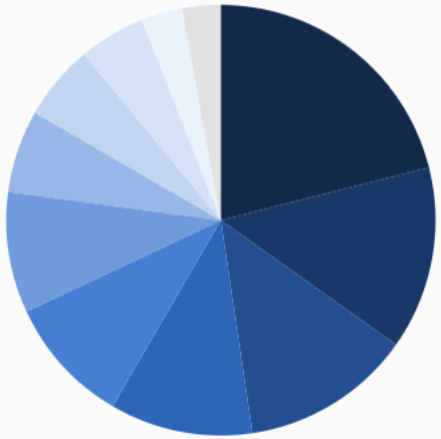


Sector	Sum of Fines
Media, Telecoms and Broadcasting	**€ 3,312,407,366** (at 286 fines)
Industry and Commerce	**€ 902,268,961** (at 438 fines)
Transportation and Energy	**€ 78,365,570** (at 104 fines)
Employment	**€ 59,024,877** (at 129 fines)
Finance, Insurance and Consulting	**€ 46,545,158** (at 200 fines)
Public Sector and Education	**€ 27,461,063** (at 224 fines)
Accomodation and Hospitalty	**€ 22,490,048** (at 65 fines)
Health Care	**€ 16,495,209** (at 189 fines)
Real Estate	**€ 2,601,831** (at 60 fines)
Individuals and Private Associations	**€ 2,048,166** (at 267 fines)
Not assigned	**€ 1,549,508** (at 118 fines)

Source: enforcementtracker.com, provided by CMS Law.Tax

Some statistics

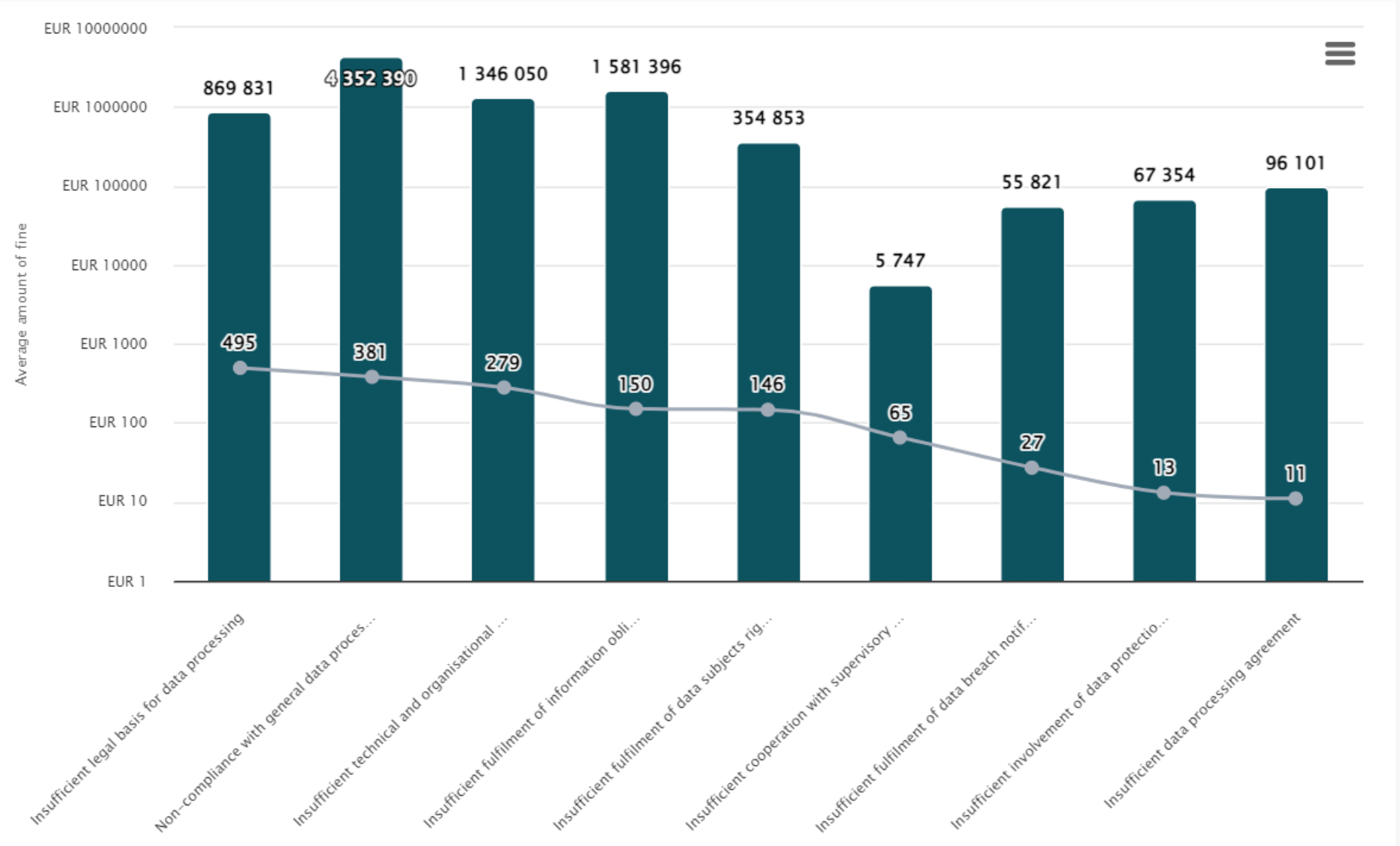
2. By total number of fines:



Sector	Number of Fines
Industry and Commerce	**438** (with total € 902,268,961)
Media, Telecoms and Broadcasting	**286** (with total € 3,312,407,366)
Individuals and Private Associations	**267** (with total € 2,048,166)
Public Sector and Education	**224** (with total € 27,461,063)
Finance, Insurance and Consulting	**200** (with total € 46,545,158)
Health Care	**189** (with total € 16,495,209)
Employment	**129** (with total € 59,024,877)
Not assigned	**118** (with total € 1,549,508)
Transportation and Energy	**104** (with total € 78,365,570)
Accomodation and Hospitalty	**65** (with total € 22,490,048)
Real Estate	**60** (with total € 2,601,831)

Source: enforcementtracker.com, provided by CMS Law.Tax

Some statistics



Source: enforcementtracker.com, provided by CMS Law.Tax

Common types of violation

- Insufficient legal basis for data processing
- Non-compliance with general data processing principles
- Insufficient technical and organisational measures to ensure information security
- Insufficient fulfilment of information obligations
- Insufficient fulfilment of data subjects' rights
- Insufficient cooperation with supervisory authority
- Insufficient fulfilment of data breach notification obligations
- Lack of appointment of data protection officer
- Insufficient data processing agreement

Cases

Interact
Co-funded by the European Union
Interreg

Cases

Bulgaria – no appropriate technical and organisational measures

Bulgarian National Revenue Agency ("NRA"), the main government tax authority was fined approx. EUR 2,550,000 by the CPDP in August 2019, for failing to implement appropriate technical and organisational measures. This resulted in unauthorised access to and dissemination of 6,074,140 individuals' personal data. A number of the affected data subjects brought claims against the state of Bulgaria for damages resulting from the data leakage.

Cases

Italy

The Italian DPA (Garante) has imposed a fine of EUR 7,000 on the oncology health care facility I.S.P.R.O.. An individual had mistakenly received medical records from another patient via e-mail.

Cases

Netherlands (1) – various

Dutch Tax Administration ("Belastingdienst") was fined on 12 April 2022 in the amount of EUR 3.7 million. The fine was imposed because the Tax Administration illegally processed personal data over a period of many years in its ‘fraud identification facility’ ("Fraude Signalering Voorziening", "FSV"). The FSV was a blacklist which the Tax Administration used to register indications of fraud, often with major repercussions for people who had been wrongly included on the list.

Cases

Netherlands (2)

- The Tax Administration had no statutory basis for processing personal data in the FSV: EUR 1 million.
- The purpose of the FSV was not specifically described in advance: EUR 750,000.
- The FSV contained incorrect and obsolete information: EUR 750,000.
- The respective data was retained for far too long: EUR 250,000.
- The FSV was not adequately protected: EUR 500,000.
- The Tax Administration waited for more than a year to ask its internal privacy supervisor for advice on assessing the risks of using the FSV: EUR 450,000.

Cases

Portugal

The Portuguese DPA has imposed a fine of EUR 170,000 on Setúbal municipality. The DPA found data protection violations regarding the collection of personal data from Ukrainian refugees. The municipality had asked refugees to fill out a form at the time of their arrival and provide various details on personal data, such as name, date of birth, marital status, etc. The DPA noted, that the municipality had not sufficiently informed the data subjects about the data processing. In addition, the DPA found that the municipality had failed to implement sufficient technical and organizational to protect personal data, as well as to define a retention period for the data. The municipality had also failed to appoint a data protection officer.

Cases

United Kingdom (1)

On 22 May 2020, the Interim Advocate's Office (IAO) sent a newsletter by email to 251 subscribers on its mailing list using the 'To' field. The email addresses of the recipients were visible to all who received the email.

The Commissioner considers that the IAO has failed to ensure appropriate security, resulting in the inappropriate disclosure of email addresses relating to 209 individuals. Of those 209 email addresses, 110 email addresses contained the individuals' full name and the remainder of the email addresses contained a mixture of formulations of names, such as initials or first and last name only. It is noted that the individuals may not be identifiable from the email addresses alone, however the email addresses could be used to identify individuals in combination with other information. The Commissioner considers that the IAO should have had a more secure process in place for the sending of group emails than inputting email addresses into the 'To' field and then copying them into the 'bcc' (blind carbon copy) field.

Cases

United Kingdom (2)

There was no technical solution in place for the sending of group emails, such as mail merge. There was no documented process in place for the sending of the newsletter by group email and no training was provided to staff on the process.

In the course of investigation it was noted that the IAO took immediate steps to inform all of those affected and to update them on the investigation into the breach. The IAO also issued an apology to all of those affected and put emotional support arrangements in place to help those affected.

Cases

France

In 2022, the fine of EUR 600,000 in the hospitality and accommodation sector was imposed by the French DPA (CNIL) on ACCOR SA (ETid-1361). According to the CNIL, the ACCOR hotel group had used data collected through some of its websites, e.g. when customers made a booking, for advertising newsletters without proper consent, as the checkbox used was pre-ticked. In addition, affected persons could not properly unsubscribe from this newsletter for weeks due to persistent technical problems.

Cases

Ireland

The (un-)availability of data has also become subject to fines.
With EUR 460,000, the second highest fine in the health care sector in the reporting period has been imposed by the Irish DPA a data controller which suffered a ransomware attack. In the course of the attack, records of about 70,000 people were accessed, altered and/or destroyed.
About 2,500 records were affected permanently.

Lessons learned

1. Pay attention to what information you **really** need to collect for your purpose (art.5, sub C – Data minimisation)
2. Keep in mind the **purposes** indicated in your general disclaimer statement and make sure that your current collection of data is part of it (art.5, sub.B – Purpose limitation)
3. Pay attention to the **retention period** of the collected data. Disclaimers should always indicate the purpose of the collection, but also the duration of the collection. The duration has to be justified and should not be undetermined (art.5, sub E – Storage limitation)
4. Pay a lot of **attention** in sharing the personal data you store with third part organizations (processors). E.g. sharing personal data with sub-contractors or contractors. Scope and extension of sharing has always to be listed in your contract. Process of data always be authorized by controller (art.28 - Processor)
5. Always **check** your legal basis for the processing of personal data collected (art.6 – Lawfulness of processing)
6. Always **make clear** how the people can manage their personal data and react according to regulation to any request (art.12-23 – Chapter 3 – Rights of the data subject
7. Very important: always **remember to involve your DPO** in any decision and if you face any doubt about how to collect, store and process personal data.