

GDPR

Update on developments

Online, 13 December 2024

Przemyslaw Kniaziuk, Mikis Moselt | Interact

Interact



Co-funded by
the European Union
Interreg

Network meeting objectives

- To update
- To network & exchange
- To discuss common solutions for current issues
- Answer questions (also from the registration form)
- The meeting will be NOT recorded



Agenda

01

Legal update

02

**IT tools and
GDPR
compliance**

03

**Non-
compliance
fines**

04

**Artificial
Intelligence
and data
protection**

GDPR developments

- Increase of transparency – beneficiaries, MC members, beneficial owners, salary slips when real costs applied, State aid recipients, declarations on the absence of conflict of interest, whistleblowers data
- Often contested by data subjects – transparency vs. privacy
- Data transfers to non-EU third countries with/without adequacy decisions
- AI use means personal data processing

Adequacy decisions review 2024

The EC has so far recognized these countries and territories as providing adequate protection:

Andorra, Argentina, Canada (commercial organisations), **Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom, the United States** (only commercial organisations certified under the EU-US Data Privacy Framework) and **Uruguay**.

GDPR fines

- Data protection authorities have imposed over 6 680 fines amounting to around EUR 4.2 billion
- All authorities imposed administrative fines, except Denmark, which does not provide for administrative fines
- The highest number of fines were imposed in Germany (2 106) and Spain (1 596)
- The authority in Ireland has imposed the highest total amount of fines (EUR 2.8 billion) followed by Luxembourg (EUR 746 million), Italy (EUR 197 million) and France (EUR 131 million)

The New York Times

Google Is Fined \$57 Million Under Europe's Data Privacy Law

Share full article



By Adam Satariano

Jan. 21, 2019

LONDON — After European policymakers adopted a [sweeping data privacy law](#) last year, the big question was how regulators would use their newfound authority against the most powerful technology companies.

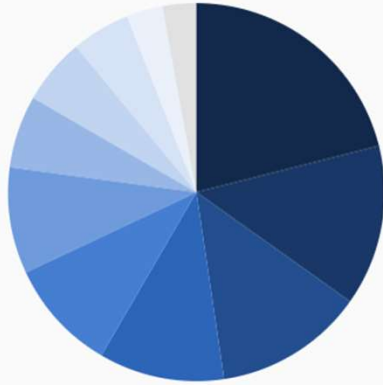
In the first major example, the French data protection authority announced Monday that [it had fined Google 50 million euros](#), or about \$57 million, for not properly disclosing to users how data is collected across its services — including its search engine, Google Maps and YouTube — to present personalized advertisements.

Administrative fines for public authorities?

Fines can be imposed on public authorities	Fines cannot be imposed on public authorities
<ul style="list-style-type: none">• 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.• Iceland	<ul style="list-style-type: none">• Austria;• Belgium (except in cases where public bodies would offer services or goods on the free market);• Czech Republic;• Denmark• France;• Germany;• Hungary;• Norway;• Spain.

Some statistics

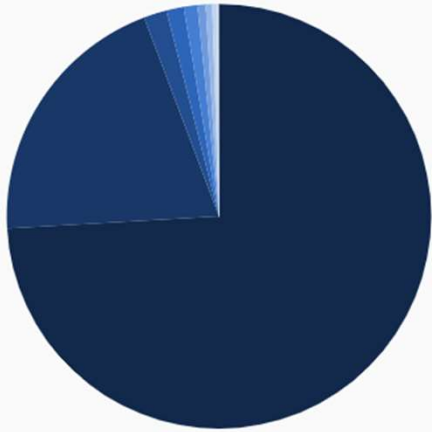
2. By total number of fines:



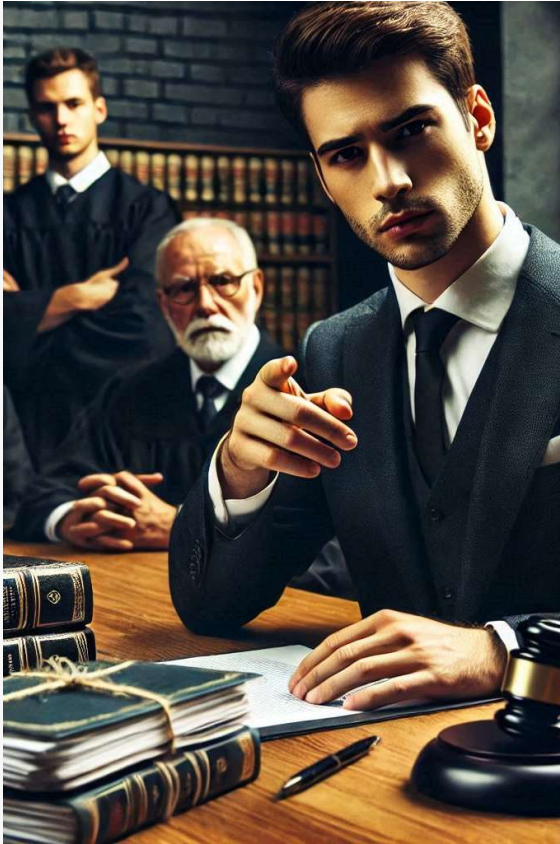
Sector	Number of Fines
Industry and Commerce	438 (with total € 902,268,961)
Media, Telecoms and Broadcasting	286 (with total € 3,312,407,366)
Individuals and Private Associations	267 (with total € 2,048,166)
Public Sector and Education	224 (with total € 27,461,063)
Finance, Insurance and Consulting	200 (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)
Accommodation and Hospitality	65 (with total € 22,490,048)
Real Estate	60 (with total € 2,601,831)

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)
Accommodation and Hospitality	€ 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)



Legal obligation Art. 6.1(c) GDPR



MC members data

Art. 39(1) CPR

- Some German Managing Authorities (MAs) take the view that not the names of the natural persons are to be published.
 - ✓ propose to publish the names of these (member) authorities/bodies but not their respective representatives
 - ✓ sufficient to keep a list of representatives at the MA to be able to provide the member bodies' representatives if needed
- GDPR requires the “economical use” of personal data (Article 5(1)(c) GDPR)
- nominated MC members claim many cases of data misuse in the past
- especially personal data published on the internet by public authorities have been repeatedly misused by the so-called [‘Reichsbürger’](#)



MC members data

Art. 39(1) CPR

- the obligation to publish the list of members of the MC requires the publication of the names of the representatives, i.e. of the persons representing the authorities, intermediate bodies and partners.
- the requirement to publish the list of the members of the monitoring committee on the “programme” website has the ultimate aim of ensuring transparency and avoiding conflicts of interest
- whenever a member changes, (e.g. a different person representing the same organisation) the list has to be updated and published (again).
- during the nomination process, the managing authority has to provide potential candidates for membership with information referred to in Articles 13 and 14 of the GDPR and inform them in advance that their names will be made public, so they are fully aware of this legal obligation, when accepting the membership.

CoI declarations

Payment slips

Conflict of interest declarations

- Financial actors including national authorities at any level shall not take any action which may bring their own interests into conflict with those of the Union
- Where there is a risk of a conflict of interests involving a member of staff of a national authority, the person in question shall refer the matter to his or her hierarchical superior

Article 61 of recast Financial Regulation

Payment slips and employment document

- If staff costs declared as real cost, legal obligation to collect them
- Monitoring systems able hide sensitive data (privileges)
- If not, staff costs can be claimed on the basis of SCOs

Article 39.3(a) of Interreg Regulation

Sensitive data in Jems

Dashboard / Applications / INT9800284 - 12345-2step / Project privileges

Application form INT9800284 - 12345-2step

Project privileges

⚠ Users working at the same time in the same page may lead to unexpected loss of data (users overwrite other users content). Please make sure a project is properly reviewed before submission.

Application Form users / Project managers

* jems username
admin@jems.eu

view edit manage

+

PP1 1

No control institution assigned

* jems username

view edit **Sensitive data**

+

interreg Confunded by the European Union

Dashboard / Applications / IA-0100045 - Internature / PP2 Trey Research / Partner report R.2

Partner report R.2

PP2 Trey Research

Status **Certified** Open controller work

Report Identification Work plan progress Public procurements List of expenditures Contributions

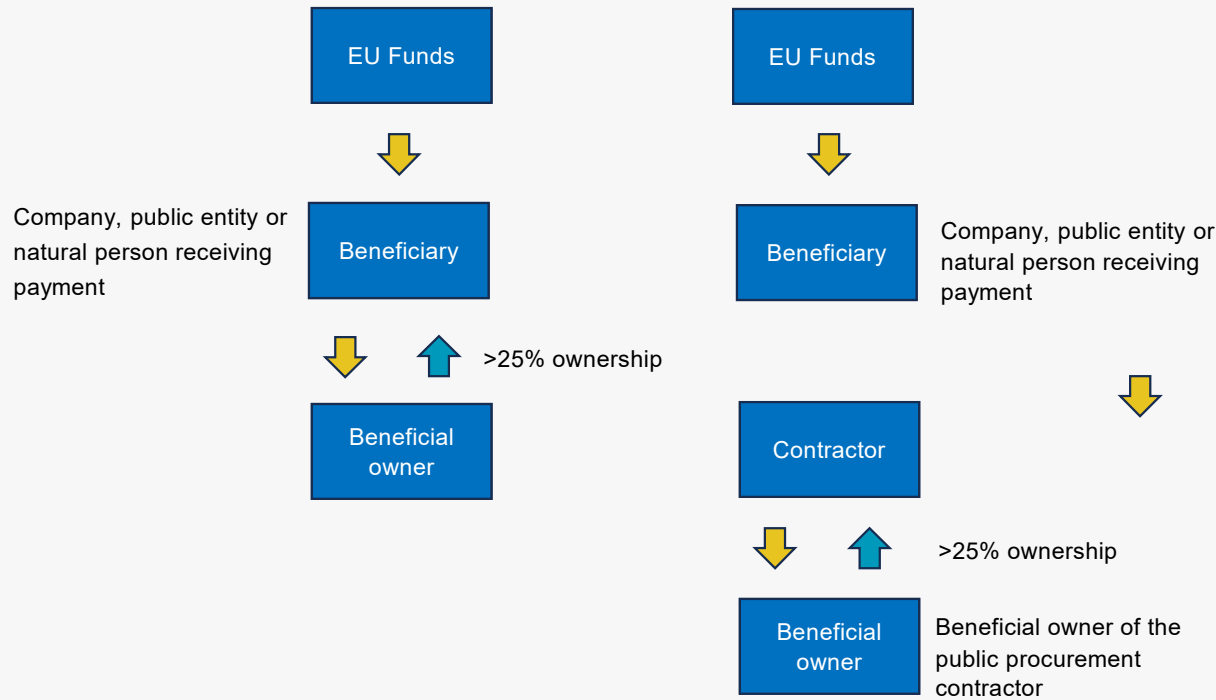
Report annexes

ⓘ Sensitive data is hidden to non-privileged users

Partner report R.2	File name	Location	Upload date	User	File size	Actions
Work plan progress	Invoice 9.pdf	Expenditure	06/10/2024 5:36 PM	admin@jems.eu	250.6 kB	Download
List of expenditures	Invoice 8.pdf	Expenditure	06/10/2024 5:38 PM	admin@jems.eu	144.9 kB	Download
Public procurements	Invoice 10.pdf	Expenditure	06/10/2024 5:38 PM	admin@jems.eu	553.3 kB	Download
Contributions	Invoice 7.pdf	Expenditure	06/10/2024 5:37 PM	admin@jems.eu	125.3 kB	Download
	Invoice 7.pdf	Expenditure	06/10/2024 5:37 PM	admin@jems.eu	125.3 kB	Download

Items per page: 25 1-5 of 5

Beneficial owners – who are they?



Beneficial owners data

Annex XVII - Data to be recorded and stored electronically on each operation

Info on all beneficial owners of the beneficiary (field 3)

- first name(s) and last names(s),
- dates(s) of birth
- VAT registration number(s) or tax identification number(s)

The same info on beneficial owners of the public procurement contractor(s) (field 23)

- For PPs above the EU PP Directive thresholds
- If SCOs applied, beneficial owners' data stored for SCO direct costs only
- Additionally, if there are subcontractors with a budget above EUR 50.000, basic info on them -> only for the lead service provided, who signs the service contract.

Beneficial owners data

Member States shall:

- ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership
- ensure that breaches of this Article are subject to effective, proportionate and dissuasive measures or sanctions
- require that the beneficial owners provide those entities with all the information necessary for the corporate or other legal entity to comply with the requirements in the first subparagraph
- ensure that the information held in the central register is adequate, accurate and current, and shall put in place mechanisms to this effect

Article 30 of 4 and 5AMLD – transposed by all MS

Risk scoring systems (Arachne)

Provision of data will be obligatory under the next MFF:

on the recipient, legal person

- recipient's full legal name, VAT identification number or another unique identifier established at country level
- the address
- the beneficial owner(s) of the recipient, where the recipient is not a natural person: the first name(s), last name(s), date of birth, and VAT identification number(s) or tax identification number(s) where available or another unique identifier at country level

on the recipient, natural person

- the first and last name; the date of birth;
- the region on NUTS 2 level when the recipient is a natural person and is domiciled in the Union or the country when the recipient is a natural person and is not domiciled in the Union;

Publications of exclusion

- financial penalty should be reinforced by the possibility to publish the information related to the exclusion in a manner that satisfies the data-protection requirements
- When natural persons are concerned, personal data should only be published in exceptional circumstances justified by the seriousness of the conduct or its impact on the financial interests of the Union.
- Early Detection and Exclusion System (EDES)

Article 142, recast Financial Regulation



Interact Collaboration Platform x EDES database - European Com x +

commission.europa.eu/strategy-and-policy/eu-budget/how-it-works/annual-lifecycle/implementation/anti-fraud-measures/ed... ☆

★ Art. 62(1) - 63 Log in with EU-Login

Name Country Code

Name/Address	Country	Administrative Measures	Period	Grounds	Comments
HAMASHA AHMED*MUSTAPHA HASAN AHMAD BEAR AL SABE A ST JABEL AL HUSSEIN PLAZA CENTER 2ND FLOOR FLAT 2 BL 15 11732 AMMAN	JO	EXCLUSION	03/12/2027	Exclusion Art. 136(1)(d) FR - fraud and criminal activities	Based on a classification of law pursuant to Article 136(1)(d)(i) of the Financial Regulation.
DELOITTE CONSULTING SL PLAZA PABLO RUIZ PICASSO 1 TORRE PICASSO 28020 MADRID	ES	EXCLUSION	19/01/2025	Exclusion Art. 136(1)(c) FR - grave professional misconduct	Based on preliminary classification in law pursuant to Article 136(2) of the Financial Regulation - No final judgment or final administrative decision
PROZONE DOO ZA RAZVOJ I IMPLEMENTACIJU INFORMACIONIH TEHNOLOGIJA*PROZONE LLC FOR DEVELOPMENT AND IMPLEMENTATION OF INFORMATION TECHNOLOGY PUSKINOVA 26 21000 NOVI SAD	RS	EXCLUSION	25/12/2025	Exclusion Art. 136(1)(c) FR - grave professional misconduct	Based on a preliminary classification in law pursuant to Article 106(1)(c)(iv) and (v) of Reg. No 966/2012. (Similar provisions are now found in Art. 136(1)(c)(iv) and (v) of Regulation 2018/1046.)

10 25 50 100

Whistleblowers' data

Member States shall ensure that the identity of the reporting person is not disclosed to anyone beyond the authorised staff members competent to receive or follow up on reports, without the explicit consent of that person. This shall also apply to any other information from which the identity of the reporting person may be directly or indirectly deduced.

State aid recipients

General Block Exemption Regulation

- Obligatory publication in the Transparency Award Module lowered from EUR 500 000 to EUR 100 000 in 2023
- Usually legal person data, sometimes natural persons data;

De minimis

- As of 1 December 2026 use of national / central union register will be obligatory -> publication of de minimis granted
- Usually legal person data, sometimes natural persons data;













Software and GDPR

Microsoft 365

Data location ×

As part of our transparency principles, we publish the location where Microsoft stores your customer data, see [Where your Microsoft 365 customer data is stored](#).









Service	Geography
 Copilot for Microsoft 365	European Union
 Exchange Online	European Union
 Exchange Online Protection	European Union
 Microsoft Teams	European Union
 OneDrive	European Union
 SharePoint	European Union
 Viva Connections	European Union
 Viva Topics	European Union

- DSK German Authority declares Microsoft 365 non compliant with GDPR in 2022 (Opinion) triggering lower authorities actions against the use of it especially concerning the use by organisations dealing with minors data (schools);
- EDPS (European Data Protection Supervisor) releases a BINDING report against the use of Microsoft 365 by the European Commission in March 2024.
- EU Commission has not prevented the unsafe transfer of data to countries outside the European Union ("**third countries**");
- the exact data collected when using Microsoft 365 had not been determined. The data processing agreement ("**DPA**") between the European Commission and Microsoft therefore did not sufficiently specify what type of personal data was collected and which specific recipients received it.

Microsoft 365

Data location ×

As part of our transparency principles, we publish the location where Microsoft stores your customer data, see [Where your Microsoft 365 customer data is stored](#).

Service	Geography
 Copilot for Microsoft 365	European Union
 Exchange Online	European Union
 Exchange Online Protection	European Union
 Microsoft Teams	European Union
 OneDrive	European Union
 SharePoint	European Union
 Viva Connections	European Union
 Viva Topics	European Union

Actors are well advised to accompany the use of Microsoft 365 with data protection risk minimisation measures. The most effective risk minimisation measures include, for example:

- Implementation and documentation of a data protection impact assessment in accordance with Art. 35 GDPR
- Implementation of transparent data subject information in accordance with Art. 13 GDPR
- Entry in the register of processing activities pursuant to Art. 30 GDPR
- Selection of data protection-friendly settings by the respective Microsoft 365 system administrators

Apple iOS 18.1 onward



- Issues with DMA (Digital Market Act) in regards of letting third parts accessing the OS;
- Issues with GDPR in regards of collection of data and data transfer outside EU (specifically USA)

So far Apple has preferred postpone release of Apple Intelligence in fear of violating EU Regulations.

Currently waiting for sentencing on similar cases with an expected release in April/May 2025.

LinkedIn sentence



Administrative penalties, which are worth around 310 million Euros have been issued by Ireland's [Data Protection Commission](#) (DPC) under GDPR.

The regulator found a raft of breaches, including breaches to the lawfulness, fairness and transparency of its data processing in this area.

The GDPR requires that uses of people's information have a proper legal basis. In this case, the justifications LinkedIn had relied upon to run its tracking ads business were found to be invalid. It also did not properly inform users about its uses of their information.

LinkedIn had sought to claim (variously) "consent"-, "legitimate interests"-, and "contractual necessity"-based legal bases for processing people's information to track and profile its users for behavioral advertising. LinkedIn also failed to comply with the GDPR principles of transparency and fairness.



Cases



Cases

Poland – no appropriate technical and organisational measures

An employee of the catering company Res-Gastro M. Gawęł Sp. k. from Kolbuszowa in the Podkarpackie region, lost a flash drive with personal data.

There were unencrypted files containing personal data of another employee, namely name and surname, address, citizenship, gender, date of birth, personal identification number (PESEL number), passport series and number, telephone number, e-mail address, photos and data on the amount of earnings. The flash drive also contained encrypted files with financial data.

The President of the Personal Data Protection Office imposed a fine of 54 600 € on Res-Gastro.



Cases

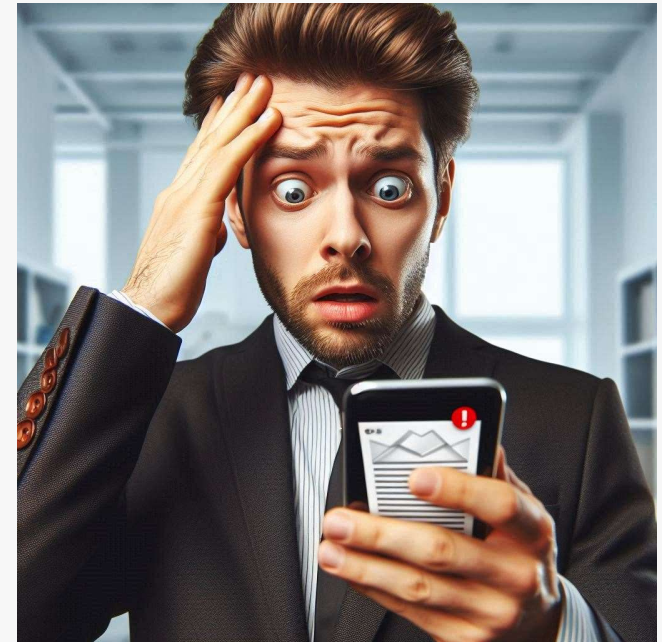
Italy

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.

Poland

The Polish Supervisory Authority (SA) was informed that unauthorised recipient had received a document confirming the award of compensation in an email attachment. The e-mail from the insurance company contained personal data such as first name, last name, mailing address, brand, model and registration number of the car, as well as the policy number, damage number and the amount of the claim awarded. The unauthorised recipient informed the insurance company of the receipt of an e-mail with an attachment containing someone else's personal data, but did not receive any response.

The President of the Polish SA has imposed the administrative fine in the amount of € 24.000 on the insurance company. The reason for imposing the administrative fine was a failure to notify the personal data breach to the supervisory authority.



Cases

Iceland

The Icelandic SA decided to investigate the use of cloud services in elementary schools. The investigation was limited to the use of Google Workspace for Education, Google's educational system, in the five largest municipalities in Iceland.

The Icelandic SA's investigation revealed that students' personal data were not only processed on the instructions of the municipality, but also for Google's own purposes. The municipality failed to demonstrate how further processing by Google was compatible with the purpose for which students' personal data were initially collected i.e., in order to provide education in accordance with the national compulsory school act.

The Icelandic SA ordered the municipality to bring the processing operations in Google's educational system into compliance with the Regulation. Furthermore, the Icelandic SA imposed a fine of app. EUR 18.580 on the municipality.



Cases

Ireland

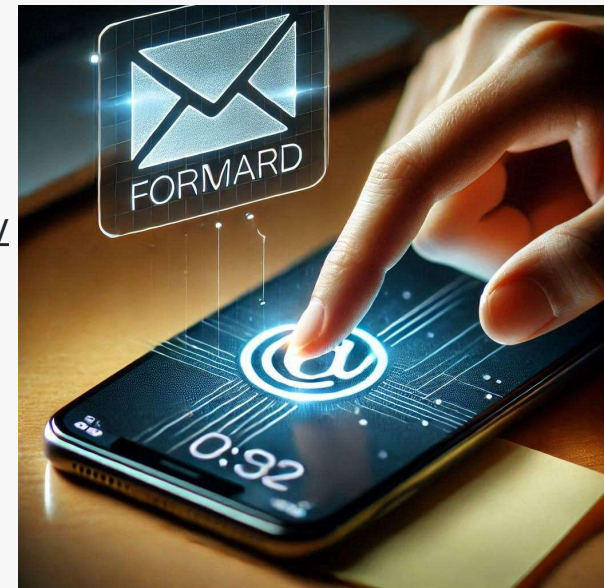
The (un-)availability of data has also become subject to fines. With EUR 460,000, the second highest fine in the health care sector in the reporting period has been imposed by the Irish DPA a data controller which suffered a ransomware attack. In the course of the attack, records of about 70,000 people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



Cases

Norway

The Norwegian DPA has imposed a fine of EUR 9,700 on a company. The DPA had received a complaint from a former employee of the company. Background of the complaint is the fact that after the employee's termination, both professional and private e-mails from the employee's mailbox were automatically forwarded to an e-mail address administrated by the managing director. During its investigation, the DPA found that the controller had automatically forwarded the e-mails without a valid legal basis. Also, the controller did not inform the former employee about the processing of the data by forwarding the e-mails, contrary to its obligation under Art. 13 GDPR. Finally, the DPA found that the controller did not properly comply with a request of objection to the processing submitted by the former employee.





AI and personal data protection



AI and data protection

- Personal data is a major source of information for AI used for training models
- But explicit consent needed for the processing of personal data
- For AI, this means individuals must be informed and consent to their data being used in AI models, all other rights need to be respected
- If someone asks you for access to their personal data, or to delete their personal data you hold on them within the AI system – can you do it?
- Some AI models have inherent risks relating to the way in which they respond to inputs or “prompts”, such as memorisation, which can cause passages of (personal) training data to be unintentionally regurgitated by the product (reproduction of training data)
- Sometimes, AI products rely on a process of “filtering” to prevent certain types of data (such as personal data, inappropriate data, and copyright data) to be provided to a user in response to a query or prompt.

AI and data protection

- Without a retention schedule and associated processes, your organisation risks non-compliance with the principle of ‘storage limitation’.
- Consider if you publish personal data on your own website
- You may need to ensure that you protect that personal data from being collected and used for AI training or other processing where you have not already agreed that purpose with your staff or users, or if they do not have a reasonable expectation it will be used for AI training.



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.

Contact us @

Przemyslaw.Kniaziuk@interact.eu
Mikis.Moselt@interact.eu



Cooperation **works**

All materials will be available on:

[Interact website](#) / [Library](#)