Overview of the GDPR fines issued by the European Data Protection Authorities in the retail industry.

Organization
H&M
Fashion retailer

Data Protection Authority
Hamburg Commissioner for Data Protection and Freedom of Information (“HmbBfDI”) – Germany

Fine
€ 35,300,000

Violation
Insufficient legal basis for data processing

Description
The HmbBfDI has sanctioned an illicit processing of employees’ personal data, after a number of workers of the German subsidiary of the well-known fashion retailer were subject to an extensive collection of details about their private lives. The Authority determined that the team leaders had carried out so-called “Welcome Back Talks” with the employees after their absences. In many cases, details, including holiday experiences, symptoms of illness and diagnoses were recorded. In addition, some supervisors acquired a broad knowledge of their employees’ private lives through corridor conversations, encompassing family issues and religious beliefs. Such information was recorded, digitally stored and made available to other managers throughout the organization. The recordings were sometimes retained for long periods. In addition to a thorough evaluation of individual work performance, the collected data was used, inter alia, to obtain a detailed profile of employees for measures and decisions regarding their employment.

This data processing was discovered when a wrong configuration of the IT system of the company made the contents of these files accessible to employees across the internal network. After the breach, the supervisory authority ordered the contents of the network drive to be “frozen” and demanded access to this data. The company, in complying with the order, submitted a data record of around 60 gigabytes. HmbBfDI’s determination was that “the combination of collecting details about their private lives and the recording of their activities led to a particularly intensive encroachment on employees’ civil rights”.

Source
https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren
2

**Organization**
Carrefour France
*Supermarket*

**Data Protection Authority**
Commission Nationale de l’Informatique et des Libertés ("CNIL") - France

**Fine**
€ 2,250,000

**Violation**
Non-compliance with general data processing principles

**Source**
https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042563756

---

**Organization**
Morele.net Sp.zoo
*E-commerce*

**Data Protection Authority**
Personal Data Protection Office (UODO) - Poland

**Fine**
€ 660,000

**Violation**
Insufficient technical and organisational measures to ensure information security

**Source**

---

**Description**
The CNIL has fined Carrefour France for several violations of the GDPR and Article 82 of the French Data Protection Act governing the use of cookies.

CNIL determined that Carrefour France had, among other things, retained personal data of more than 28 million inactive customers, collected in the context of a loyalty programme, for an excessive period of time and had failed to address the requests of a customer to delete their data as well as customer objections to direct marketing communications.

In addition, CNIL outlined that Carrefour France had not complied with its obligation to facilitate the exercise of data subject rights, asking for too much information to assess the identity of the data subjects and failing to respond to requests within the time limits set out in Article 12 of the GDPR.

Moreover, CNIL added that Carrefour France had breached its duty of information, under Article 13 of the GDPR, since the information provided to users was insufficient, not easily accessible nor easily understandable.

Finally, CNIL held that Carrefour France had breached Article 82 of the French Data Protection Act by placing cookies on users' devices, without first having obtained users’ consent.

---

**Description**
The decision of the Polish Data Protection Authority concerned a data breach of 2.2 million customers.

The breach occurred due to the lack of appropriate technical (insufficient safeguards) and organisational measures (on the monitoring of potential risks related to atypical online behaviour) implemented by the company. In particular, the OUDO stated that there was a lack of appropriate response procedures to deal with the emergence of unusual network traffic.

The breach was deemed by the supervisory authority as significant and of a serious nature, because it concerned a large number of people and for the type of the data violated. Indeed, the data concerned included name and surname, phone number, email, delivery address, and in the case of about 35,000 people, their payment instalment information (including Personal ID number), education, source of income and net income, household maintenance costs, and marital status.

In its decision, the supervisory authority also pointed out that, as a result of the infringement, there was a high risk of adverse effects on individuals whose personal data fell into the wrong hands, such as identity theft.
4

**Organization**
Doorstep Dispensaree Ltd.
*Pharmacy*

**Data Protection Authority**
Information Commissioner’s Office (“ICO”) – UK

**Fine**
€ 320,000

**Violation**
Insufficient technical and organisational measures to ensure information security

**Source**

---

**Description**
The ICO has fined the pharmacy for failing to ensure the security of special category data.

Doorstep Dispensaree Ltd, a supplies medicines to customers and care homes, had left about 500,000 documents in unlocked containers at the back of its premises. The documents included names, addresses, dates of birth, NHS numbers, medical information and prescriptions belonging to an unknown number of people.

Some of the documents had not been appropriately protected against the elements and were therefore water damaged.

---

5

**Organization**
AVON COSMETICS SAU
*Manufacture and online sale of skin care, make-up, perfume and hair products.*

**Data Protection Authority**
Agencia Española de Protección de Datos (“AEPD”) – Spain

**Fine**
€ 60,000

**Violation**
Insufficient legal basis for data processing

**Source**

---

**Description**
The AEPD has fined the company for unlawfully processing data.

The case originated upon a claim from a consumer that had alleged Avon Cosmetics unlawfully processed his data without appropriately verifying his identity. As a consequence, a third party had made use of this information to fraudulently receive products from the company without paying the amounts due. Further, the complainant’s data were entered into a bad debt register in error, preventing him from operating with his bank.

The supervisory authority stressed the fact that the data controller had not put in place the necessary due diligence to verify the identity of the person.
**Organization**
Coop Finnmark SA
Retailer

**Data Protection Authority**
Norwegian Supervisory Authority (Datatilsynet) – Norway

**Fine**
€ 40,000

**Violation**
Insufficient legal basis for data processing

**Source**
https://www.datatilsynet.no/contentassets/5cd2e76bd5d2481f9578ffe721b7e24d/vedtak-om-overtredelsesgebyr-til-coop-finnmark-sa.pdf

---

**Organization**
IDdesign A / S
Furniture retailer

**Data Protection Authority**
Danish Data Protection Agency (Datatilsynet) – Denmark

**Fine**
€ 13,450

**Violation**
Non-compliance with general data processing principles

**Source**

---

**Description**
The case concerned the unlawful distribution of a camera recording from a shop.

The manager of the shop in question had made a recording of surveillance footage with their phone and had distributed the recording.

The supervisory authority has stated that Coop Finnmark had lacked a legal basis for the shop manager’s distribution of the surveillance footage.

The supervisory authority has given weight to the fact that the camera footage showed children, and that the distribution potentially entailed a major risk to their privacy.

---

**Description**
Datatilsynet has fined the data controller for failure to delete data of about 385,000 customers.

In the fall of 2018, the supervisory authority audited the company. The main objective was to investigate whether retention periods regarding the deletion of personal data complied with the GDPR principles. Before the visit, the company had given an overview of its customer data management system, including applicable retention periods. It also explained that it had upgraded its system in some of its shops, but not in all.

During the audit carried out by Datatilsynet, IDdesign had revealed that the data included in the old system – comprising the names, addresses, telephone numbers, e-mail addresses and purchase history of its customers – had never been deleted.

The use of an old system to indefinitely store the individuals’ personal data violated Article 5 (1)(e) of the GDPR (storage limitation), which states that the data controllers have to process personal data in such a way that data subjects cannot be identified for longer than is necessary for the purposes for which the personal data are processed.
**Organization**
Recambios Villallegre S.L.  
*Car parts retailer*

**Data Protection Authority**
Agencia Española de Protección de Datos (“AEPD”) – Spain

**Fine**
€ 12,000

**Violation**
Insufficient legal basis for data processing

**Source**

---

**Description**
The company was sanctioned for publishing images of a person on social networks without a legal basis and for the lack of information regarding the installed video surveillance system.

In particular, the investigation took place because of a claim from a citizen in which he/she reported to the AEPD a harassment campaign that the company had carried out through Facebook and WhatsApp against a person who, according to the company, had stolen money from the office cash register. This activity was considered by the AEPD as unlawful processing of the individual's data in breach of Article 6(1) of the GDPR.

In addition, the company had used images collected with security cameras, without having an informative sign on the premises that mentioned the use of these cameras, in breach of art. 13 of the GDPR.

---

**Organization**
Unknown  
*Merchant*

**Data Protection Authority**
Autorité de protection des données (“APD”) - Belgium

**Fine**
€ 10,000

**Violation**
Non-compliance with general data processing principles

**Source**

---

**Description**
The APD has fined a merchant for failing to comply with the principles of processing of personal data and to the requirements of a valid consent under Article 7 of the GDPR.

In particular, the supervisory authority outlined that it had received a complaint from an individual who had refused to show his electronic identity card to the merchant for the creation of a customer loyalty card.

The activity that the merchant had carried out breached the GDPR principle of data minimization, considering that the merchant, in order to create the loyalty card, required access to personally identifiable information indicated in the identity card, including the photo and barcode which is linked to the individual's social identification number.

Finally, the merchant also had breached the provisions set out in Article 7 of the GDPR, since the consent requested to data subjects was not freely given. Indeed, the customer did not have an alternative choice.
### Organization
Unknown  
Merchant providing services in an online store

### Data Protection Authority
Data State Inspectorate (DSI) - Latvia

### Fine
€ 7,000

### Violation
Insufficient fulfilment of data subjects’ rights

### Source

---

### Organization
S.C. Marsorom S.R.L.  
Online care tyres retailer

### Data Protection Authority
National Supervisory Authority for Personal Data Processing (“ANSPDCP”) – Romania

### Fine
€ 3,000

### Violation
Insufficient technical and organisational measures to ensure information security

### Source

---

### Description
DSI has fined a merchant for non-compliance with the data subject’s rights and non-cooperation with the supervisory authority.

In particular, the data subject had repeatedly approached the merchant with a request to delete all personal data which the merchant had obtained within the framework of the order placed by the submitter with the merchant. Following the data subject’s requests to delete his/her personal data, the merchant repeatedly sent commercial communications in the form of text messages to the applicant’s mobile phone number.

In addition, the merchant did not cooperate with the DSI and did not provide the necessary information in the time requested. The merchant also did not comply with the order issued by the DSI in accordance with Article 58 (2) (c) and (g) of the GDPR and Article 23 of the Personal Data Processing Law.

---

### Description
The investigation took place following a notification claiming that some personal data of the data controller’s customers could be viewed on the controller’s website.

The supervisory authority has held that the data controller failed to take appropriate measures, pursuant to Articles 25 and 32 of the GDPR, as it did not adopt sufficient security measures to prevent the unauthorised access and disclosure of personal data of customers who placed orders on this site.

In addition, the data controller was recommended to establish a shorter storage period of personal data related to customer accounts in order to comply with the principle of storage limitation enshrined in Article 5(1)(e) of the GDPR.
Description
The violation alleged against the company concerned the failure to comply with the corrective measures ordered by the supervisory authority. In particular, in response to several complaints to the ANSPDCP about receiving SMS marketing messages without the data subjects’ consent, the supervisory authority launched an investigation and found several violations of the GDPR.

In addition, upon finding GDPR violations, the supervisory authority ordered the company to implement corrective measures and, specifically, to respond to the authority on findings of GDPR violations within five days. However, the company had failed to respond as ordered by the ANSPDCP, therefore breaching Article 83(5)(e) of the GDPR.

Description
The supervisory authority has sanctioned the data controller Estee Lauder Romania SRL, because the company had violated the provisions of Articles 6, 7 and 9 of the GDPR. In particular, in its decision, the supervisory authority has stated that the data controller had conducted illegal processing by disclosing and collecting personal data (name, surname, telephone number, date of birth and health information) without consent or other legal basis.
Organization
Dante International S.A.  
Owner of the online retailer eMAG

Data Protection Authority
National Supervisory Authority for Personal Data Processing (“ANSPDCP”) – Romania

Fine
€ 3,000

Violation
Insufficient legal basis for data processing

Source

Description
The supervisory authority has fined the owner of the e-commerce website eMag due to the violation of the provisions set out in Article 6 of the GDPR, in relation to the provisions of Article 21 (3) of the GDPR.

In particular, the company sent a commercial e-mail to a customer though the latter had previously unsubscribed from commercial communications.

Organization
Comercio Online Levante, S.L.  
Manufacture and online sale of skin care, make-up, perfume and hair products

Data Protection Authority
Agencia Española de Protección de Datos (“AEPD”) – Spain

Fine
€ 3,000

Violation
Insufficient technical and organisational measures to ensure information security

Source

Description
The case concerned a data breach which occurred to the data controller.

The complaint concerned the fact that when users tried to access their user account on perfumespremium.es, the personal data of a different user was displayed.

AEPD has stated that in allowing the access of the data of a third party, the data controller violated Article 32 of the GDPR.

Thus, the supervisory authority has concluded that the company by failing to comply with the required technical measures of data protection, had breached, inter alia, the principle of confidentiality, as set out in Article 5 (1)(f) of the GDPR.
Organisation
Mymovies Europa 2000, S.L.
Household appliances retailer.

Data Protection Authority
Agencia Española de Protección de Datos (“AEPD”) – Spain

Fine
€ 1,400

Violation
Insufficient fulfilment of information obligations

Source

Description
The infringement concerned a lack of information pursuant to Article 13 of the GDPR.
In particular, the company had not published a privacy statement on its website. The company had used an online form that allowed the collection of certain categories of personal data on its website but had not provided any information under Article 13 GDPR.

Organisation
eShop for Sports (M.L. PRO.FIT SOLUTIONS LTD)
Fitness retailer

Data Protection Authority
Commissioner for Personal Data Protection – Cyprus

Fine
€ 1,000

Violation
Insufficient legal basis for data processing

Source

Description
The data controller sent SMS marketing messages without the data subject’s consent. In addition, no appropriate measures were taken, such as the possibility for telephone users to block marketing messages from the data controller by opting out of receiving SMS marketing messages.
Organization
CERRAJERO ONLINE S.L.
Hardware store.

Data Protection Authority
Agencia Española de Protección de Datos ("AEPD")
– Spain

Fine
€ 900

Violation
Insufficient fulfilment of information obligations

Source

**Description**
The AEPD has sanctioned the data controller for the breach of Article 13 of the GDPR.
The company had collected personal data of data subjects without providing accurate information about the data collection in its privacy policy, as required by Article 13 of the GDPR. The privacy policy contained only information on repealed legislation.

Organization
Chenming Ye (Bazar Real)

Data Protection Authority
Agencia Española de Protección de Datos ("AEPD")
– Spain

Fine
€ 540

Violation
Insufficient fulfilment of information obligations

Source

**Description**
The AEPD held that the data controller had installed a CCTV camera on its property without informing the clients about the video recording.
In addition, the supervisory authority has ordered the data controller to shift the surveillance camera’s position so that it will no longer record public roads and to put up a warning sign that CCTV is in use.

This paper is not intended to be a fully comprehensive report and the information provided herein does not constitute legal advice. All contents are provided for general informational purposes only. The information is based on the decisions issued by the mentioned European supervisory authorities and made available through their websites, whose links are included in this document.

Please note that it is possible that some of the decisions reported herein may have been reformed or overturned.