Overview of some striking sanctions imposed by Data Protection Authorities in recent times

EY Law - June 2020

EY Law

Some striking sanctions imposed by Data Protection Authorities of neighboring countries*

*Non-exhaustive list

EY Law

I. Some striking sanctions imposed by Data Protection Authorities of neighboring countries

Country & date	Sanctions	Controller/ Processor	Summary
17/12/2019 	204.600.000,00 EUR (not final)	Airline company	Insufficient technical and organizational measures to ensure information security: ➢ cyber incident involving user traffic to the airline's website being diverted to a fraudulent site; ➢ personal data of +/- 500.000 customers were compromised; ➢ the ICO's investigation has found that a variety of information was compromised by poor security arrangements at the company.
09/07/2019 	110.390.200,00 EUR (not final)	Hotel chain	Insufficient technical and organizational measures to ensure information security: ➢ the proposed fine relates to a cyber incident which was notified to the ICO by the hotel chain; ➢ a variety of personal data contained in approximately 339 million guest records globally were exposed by the cyber incident; ➢ the hotel chain did not carry out sufficient due diligence when it purchased another hotel group (whose systems had been compromised years earlier) and should have done more to secure its own IT systems.

I. Some striking sanctions imposed by Data Protection Authorities of neighboring countries

Country & date	Sanctions	Controller/ Processor	Summary
21/01/2019 	50.000.000,00 EUR	Search engine company	Insufficient legal basis for data processing: ➢ complaints concerned the creation of an account of the search engine company during the configuration of a mobile phone using the Android operating system; ➢ lack of transparency; ➢ insufficient information; ➢ lack of legal basis; and ➢ the obtained consents had not been given "specific" and not "unambiguous".
21/11/2019 	500.000,00 EUR	Company specialized in thermal insulation of private homes	Insufficient fulfilment of data subjects rights: ➢ the company was fined for cold calls after several complainants obtained cold calls, despite having declared directly to the caller and by post that they did not want this; ➢ the company had stored excessive information about customers and their health; and ➢ the company had not informed customers about the processing of their personal data or the recording of telephone conversations.

I. Some striking sanctions imposed by Data Protection Authorities of neighboring countries

Country & date	Sanctions	Controller/ Processor	Summary
30/10/2019 	14.500.000,00 EUR	Real estate company	Non-compliance with general data processing principles (i.e. storage limitation): ➢ use of an archiving system for the storage of personal data of tenants that did not provide for the possibility of removing data that was no longer required; ➢ involved data on the personal and financial circumstances of tenants, i.e. salary statements and health insurance data as well as bank statements.
12/04/2019 	80.000,00 EUR	Medium-sized company in the financial sector	Insufficient technical and organizational measures to ensure information security: ➢ the company had failed to take the necessary care to preserve the integrity and confidentiality of information when disposing of documents containing personal data of two customers; ➢ without prior anonymization, the papers were disposed of in the general waste paper recycling system, where the documents were found by a neighbor.

EY Law

I. Some striking sanctions imposed by Data Protection Authorities of neighboring countries

Country & date	Sanctions	Controller/ Processor	Summary
15/01/2020 	27.800.000,00 EUR	Telecom operator	Insufficient legal basis for data processing: ➢ lack of consent for marketing activities (telemarketing and cold calling), addressing of data subjects who asked not to be contacted with marketing offers; ➢ invalid consents collected in apps; ➢ lack of appropriate security measures to protect personal data; ➢ lack of clear data retention periods.
11/12/2019 	8.500.000,00 EUR	Energy provider	Insufficient legal basis for data processing: ➢ unlawful processing in connection with telemarketing and telesales activities: promotional calls were made without the consent of the person contacted or despite that person's refusal to receive promotional calls and without triggering the special procedures for checking the public opt-out register; ➢ personal data were processed longer than the permitted data retention periods; and ➢ personal data on potential customers were collected from entities who had not obtained consent for the disclosure of such data.

I. Some striking sanctions imposed by Data Protection Authorities of neighboring countries

Country & date	Sanctions	Controller/ Processor	Summary
03/03/2020 	525.000,00 EUR	Not-for-profit tennis association	Insufficient legal basis for data processing: ➢ the organization sold personal data such as name, gender and address to third parties (i.e. sponsors) for direct marketing purposes without obtaining the consent of the data subjects; ➢ the data protection authority rejected the existence of a legitimate interest for the sale of the personal data and therefore decided that there was no legal basis for the transfer of the personal data to the sponsors.
18/06/2019 	460.000,00 EUR	Hospital	Insufficient technical and organizational measures to ensure information security: ➢ failing to implement the necessary security measures to protect the personal health data of its patients, in particular in terms of authentication and traceability as defined in Article 32 of the GDPR.

Some striking sanctions imposed by the Belgian Data Protection Authority

*non exhaustive list

EY Law

II. Some striking sanctions imposed by the Belgian Data Protection Authority

Date	Sanctions	Controller/ Processor	Summary
14/05/2020 	50.000,00 EUR	Social media platform	Insufficient legal basis for data processing: ➢ unlawful collection and usage of personal data without a valid legal basis in the context of an "invite a friend" functionality; ➢ the platform relied on the *user's* consent for the processing of the personal data of *non-users* in the context of this functionality; ➢ only the data subject whose personal data are being processed can validly give his/her consent.
14/05/2020 	50.000,00 EUR	Insurance company	Insufficient legal basis for data processing: ➢ the privacy policy stated that personal data were processed on the basis of legitimate interest for various purposes. Since for most purposes no legitimate interest had been demonstrated, consent for these processing operations had to be obtained. Violation of the obligation of transparency: ➢ the privacy policy did not meet the requirements of the GDPR (e.g. no distinction between ordinary and health data, no indication of the specific legitimate interest, no mention of the right to object to processing activities for direct marketing).

II. Some striking sanctions imposed by the Belgian Data Protection Authority

Date	Sanctions	Controller/ Processor	Summary
28/04/2020 	50.000,00 EUR	Telecom company	The data protection officer ("DPO") was not in a position to work independently: ➢ the company's DPO was not sufficiently involved in the processing of personal data breaches; ➢ the company did not have a system in place to prevent a conflict of interest of the DPO (e.g. the DPO had several other positions within the company).
17/09/2019 	10.000,00 EUR	Liquor store	Non-compliance with general data processing principles: ➢ misuse of an electronic identity card (eID) to create a loyalty card: ▪ violation of data minimization principle: the merchant did not require all the data on the eID card, including the photo and barcode which is linked to the data subject's identification number, to create the loyalty card; ▪ insufficient legal basis for data processing: consent has not been freely given, because customers were not offered an alternative to obtain a loyalty card but to provide their eID; ➢ in the meantime, the decision of the Belgian DPA has been annulled by the Market Court.

II. Some striking sanctions imposed by the Belgian Data Protection Authority

Date	Sanctions	Controller/ Processor	Summary
17/12/2019 	2.000,00 EUR	Non-profit association for specialized nursing care	Insufficient fulfilment of data subjects rights: ➢ failure to comply with the data subject's requests to get access to her personal data and to have her personal data deleted.
29/05/2020 	1.000,00 EUR	Non-profit association	Unlawful sending of direct marketing promotional material: ➢ the association kept sending promotional material to a former donor (up to 7 years after his donation), while this person had repeatedly requested the association to no longer send him such promotional material and to delete his personal data; ➢ the association could not invoke its legitimate interest for sending the promotional materials, because it has not fulfilled its obligation to provide additional safeguards on behalf of the data subject (i.e. the provision and facilitation of the right to object, and the immediate follow-up to such an objection made by the data subject).

II. Some striking sanctions imposed by the Belgian Data Protection Authority

Date	Sanctions	Controller/ Processor	Summary
22/04/2020 	- **Obligation to establish a register of all processing activities** - including its camera image processing activities - within 3 months of notification of the decision; - **Obligation to inform the DPA** of the follow-up given to the obligation to establish the register (above) within the same time limit.	Retail store	Violations of both the Camera Law and the GDPR: ➢ the Controller did not report the use of a surveillance camera. The use of such cameras must be reported to the police services, at the latest the day before the camera is put into use; ➢ lack of recording of the images from the surveillance camera in the register of processing activities; ➢ absence of an image processing register; ➢ both registers can be combined in one register.
09/07/2019 	- **Reprimand** - **Publication of decision,** including identification details of both parties	Federal Public Service Health	Insufficient fulfilment of data subjects rights: ➢ the defendant did not meet the complainant's request to allow him access to his personal data in order to ascertain the reason for the decision to deprive him of the post of deputy member; ➢ in the meantime, the decision of the Belgian DPA has been annulled by the Market Court.

II. Some striking sanctions imposed by the Belgian Data Protection Authority

Date	Sanctions	Controller/ Processor	Summary
15/04/2020 	- !! **Obligation to freeze the processing of personal data** until the necessary safeguards are put in place !! - Obligation to ensure that the information provided by the Controller regarding its processing activities is compliant with the GDPR. - Warning to closely monitor in the future (i) the designation and positioning of the DPO and (ii) the performance of the tasks by the DPO.	Municipal institution	Multiple violations of the GDPR: ➢ unlawful processing of personal data; ➢ failure to demonstrate sufficiently the lawfulness of the processing with regard to public security; ➢ lack of transparent information and communication towards data subjects; ➢ insufficient information for data subjects in the privacy policy on the use of platforms with third party (joint) data controllers; ➢ insufficient information to data subjects on the processing of personal data; ➢ failure to demonstrate that the DPO complies with the qualitative requirements imposed by the GDPR; ➢ failure to demonstrate that the position of the DPO is sufficiently independent and allows reporting to the highest management body.

II. Some striking sanctions imposed by the Belgian Data Protection Authority

Date	Sanctions	Controller/ Processor	Summary
21/02/2020 	- Company A: **reprimand** - Company B: claim declared unfounded	Two former employers, in the context of a dismissal of an employee	The claimant argues that the two companies violated the GDPR by (i) collecting information about him from his new employer and then passing it on to his trade union, and (ii) communicating this information without his knowledge, in particular information about legal proceedings in which he is personally involved. ➢ the fact that an employer shares information about one of its employees by telephone does not constitute "data processing" within the meaning of the GDPR. ➢ the processing of personal data may be based on the "legitimate interest" of a company when the company has to defend itself against the allegations of a former employee in the context of a dismissal procedure. ➢ according to the Authority, the company acted disproportionately since the grounds for dismissal do not in themselves relate to and precede the information provided by the new employer.

For all advice and assistance:
contact the Digital Law Team

Jan Decorte
Associate Partner EY Law
Digital Law team

+32 (0)475 63 06 06
jan.decorte@be.ey.com

EY Law