EU Court of Justice clarifies concept of â€œinformed consentâ€• for collection of personal data

On 11 November, the Court of Justice of the EU (“CJEU”) rendered its judgment (Case Câ€‘61/19) in a case (Orange România SA v. Autoritatea NaÅ£ionalÄƒ de Supraveghere a PrelucrÄƒrii Datelor cu Caracter Personal) about informed consent. The CJEU followed the Advocate General Maciej Szpunar (“AG”) Opinion. The issue at stake? What exactly does the notion of “free and informed consent” cover when processing personal data and what are the criteria for assessing such consent (e.g. retention of customers' identity documents by a telecommunications operator)? With this new decision, and Planet49, the CJEU shows how strictly it interprets the criteria for obtaining valid consent.

What happened in this case?

Orange Romania, a provider of mobile telecommunication services, had concluded contracts for the provision of such services with its customers on its premises. Copies of the customers’ identity documents (“IDs”) were annexed to these contracts, which stipulated that the customers had been informed and had given their consent to the collection and storage of these copies. The box relating to that clause had been ticked by Orange Romania before the contract was signed.

According to the National Authority for the Supervision of Personal Data Processing (“ANSPDCP”), Orange Romania failed to prove that customers had made an informed choice about collecting and storing copies of their IDs, and ANSPDCP imposed a fine. Orange Romania brought an action before the Regional Court of Bucharest challenging the fine. The latter referred questions to the CJEU on the concept of “consent” to ascertain what conditions must be met for an expression of will to be considered (i) specific and informed and (ii) freely given.

In its Opinion, the AG said that it was legitimate for a company to ask customers to provide some personal data and to prove their identity for the purposes of concluding a contract. However, requiring customers to consent to their IDs being copied and stored appeared unnecessary for performing a contract. The CJEU agreed.

How is consent validly constituted under EU law (including GDPR)?

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the processing of his/her personal data.

The guiding principle is that of a self-determined decision of an individual who is capable of making choices about the use and processing of his/her data. In that regard, consent is not validly given in the case of silence, pre-ticked boxes or inactivity.

What exactly is freely given consent?

The requirement of an “indication” of the data subject’s wishes clearly points to active (rather than passive) behaviour and necessitates that the data subject enjoys a high degree of autonomy when choosing whether to give consent.

In the case at issue, there was no freely given consent. The customers do not appear to have personally ticked the box relating to that clause; the fact that the box was ticked is not in itself a positive indication of those customers’ consent to a copy of their IDs being collected and stored. Without any confirmation that the clause was actually read and digested, merely signing the contracts containing the ticked box does not prove such customers’ consent. The customer may have ignored the clause, making it impossible to establish clearly whether consent has been freely given.

In addition, if a customer did not consent to a copy of his/her ID being collected or stored, Orange Romania required him/her to declare this in writing. According to the CJEU, such an additional requirement is liable to unduly restrict the freedom to choose to object to that collection and storage.

In a previous case in the online world, the CJEU established that consent given in the form of a preselected tick of a checkbox does not indicate active consent on the part of the website user (see our previous Law-Now).

What exactly is informed consent?

There should be no doubt whatsoever as to whether the data subject received sufficient information. The data subject must be informed of all circumstances surrounding the data processing and its consequences.

If the data subject’s consent is part of a written declaration that includes other matters, that declaration must be presented in an intelligible and easily accessible form, using clear and plain language. The contractual terms must not be misleading as to concluding the contract even if the data subject refuses to consent to the processing of his/her data. A customer cannot make an informed choice if he/she is not aware of the consequences.

Who has the burden of proof for showing that consent has been given?

When processing is based on consent, it is for the controller to demonstrate that the data subject (customer) has consented to the processing of his/her data. This provision constitutes a

specification of the principle of accountability. The controller must also prove that all the conditions for effectiveness have been met.

What are the practical steps you should take to comply with this new ruling?

By taking the following proactive steps, you can reduce the risk of a fine for unlawful data processing:

- Be transparent. Data subjects (customers) must know (i) which data is to be processed; (ii) the duration of such processing; (iii) the specific purpose of the data and how it will be processed; (iv) who is processing the data; and (v) whether the data is intended to be transferred to third parties.
- Keep in mind that consent is a clear affirmative action where the indication of the data subject's wishes clearly points to active rather than passive behaviour.
- Note that a positive action should not be required to refuse consent (e.g. completing an additional form setting out that refusal). Consumers should not feel that refusal (e.g. to consent to the copying and storing of their IDs) is not in line with regular procedures.
- Make sure that your contractual terms are not misleading as to concluding the contract even if data subjects refuse to consent to the processing of their data.
- Inform your data subjects about the consequences of refusing to give consent (e.g. is consent to the data processing a condition for concluding the contract?).
- Do not rely on pre-ticked boxes; it is not a valid form of consent under the GDPR in both the analogue and online worlds.
- Choose another possible ground for processing the data if obtaining valid consent is not certain, or where consent is not specifically required.
- Seek remedies from your local supervisory authority if you have any concerns about the legality of processing personal data.

For more information on cybersecurity, please contact your usual CMS advisor. Did you know our tech & data practice is recognised as tier 1 (best-in-class) by Chambers and Legal 500?

Thomas Dubuisson, Associate, Brussels
Tom De Cordier, Partner, Brussels