EUROPEAN LAW BLOG
NEWS AND COMMENTS ON EU LAW

ELB Blogpost 11/2024, 12 February 2024
Tags: C-683/21 *Nacionalinis visomenes sveikatos centras prie Sveikatos apsaugos ministerijos*
Topics: Artificial Intelligence, Data Protection and Digital Governance

When EU Data Protection Meets AI Tools – The CJEU determines responsibility: An analysis of C-683/21 *Nacionalinis visomenes sveikatos centras prie Sveikatos apsaugos ministerijos*

By Professor Elspeth Guild, Queen Mary University of London

Nowhere in this judgment of 5 December 2023 does the term 'artificial intelligence' (AI) appear, yet for the first time the Court of Justice of the EU's Grand Chamber (CJEU) deals with the issue of legal responsibility and liability for the use of personal data by AI tools. It is a ground-breaking judgment which merits serious consideration, in particular as it allocates responsibility for AI operations and liability for data protection breaches, in accordance with the EU General Data Protection Regulation's rules regarding the identification and duties of data controllers. The reference, from a court in Lithuania made in October 2022, only attracted the attention of the Dutch authorities who intervened before the Court and the Council. No other Member State participated in the case.

While the EU legislator has recently completed negotiation of an AI Act which will regulate the use of AI tools through the lens of risk assessments based on consumer protection and fundamental rights, the CJEU has begun to address who is responsible when things go wrong as regards the use of personal data. The EU legal tool which the Court used in this case is the GDPR – the allocation of legal responsibility regarding the duties of data controllers and critically, who counts as a data controller with responsibilities.

The subject matter of the case is data protection relating to the development and use of an app for the purposes of containing the Covid-19 pandemic. The Lithuanian Ministry of Health commissioned a mobile app from a company to register and monitor personal data of persons who had been exposed to the Covid-19 virus for the purposes of epidemiological follow up (para 12). The private company which obtained the contract

agreed in the contract that both itself and the Ministry were data controllers as regards the app (para 16). Employees of the Ministry and the company exchanged numerous emails regarding aspects of the creation of the app and copied in the relevant director at the ministry (para 13-15). The app was made available to the public via Google Play Store and Apple App Store from 4 April 2020 whereby more than 3,000 people used the app and provided extensive personal data. On 26 May, it ceased to be operational, and on 4 June, the Ministry notified the company that it was terminating the contract on the ground of lack of funding (paras 17 – 19). But in the period of its operation, users of the app had received and replied to questions involving the processing of personal data, including sensitive data regarding health status and conditions of isolation.

On 18 May 2020, the Lithuania State Data Protection Inspectorate began an investigation into the collection and use of personal data by and for use of the app. An added quirk regarding the facts of the case was that another Lithuanian company which manages an IT system on monitoring and controlling transmissible diseases had received copies of personal data collected by the app. Further, for purposes of testing the app, fictitious data were used except that the actual telephone numbers of the company's employees were also used (no doubt a requirement of the way the app was built) (para 25).

In its judgment, the Court of Justice found that the Ministry of Health body had actually participated in the determination of the purposes and means of the processing of personal data for the development of the app (para 33). This conclusion was not affected by the fact that the body had been referred to as a controller in a confidentiality policy. Nor was it affected by the facts that: (1) the Ministry body did not itself process any personal data; (2) it had no contract with the company developing the app; (3) it did not acquire the mobile application at issue; nor (4) did it authorise dissemination of the app through online shops (para 35). The Court held that provided that the Ministry body satisfies the condition laid down by Article 4(7) GDPR on the designation of a controller, it is responsible and liable not only for any processing of personal data which it itself carries out, but also for any such processing carried out on its behalf (para 36). The only way the Ministry body would not be a controller for GDPR purposes, would be if, prior to that application being made available, it expressly objected to such making available (para 37).

The importance of this section of the judgment is that the body which gives instructions regarding how an AI tool (the app) should be developed can only escape GDPR duties as a data controller where it has objected to the making available of the app. This casts wide the net of responsibility and, in particular, places data controller duties on the entity commissioning an app (AI tool), not just on those who are carrying out the instructions by developing the app or the app itself (as some of the more arcane propositions about responsibility have suggested). In the words of the Court:

> "an entity which has entrusted an undertaking with the development of a mobile IT application and which has, in that context, participated in the determination of the purposes and means of the processing of personal data carried out through that application may be regarded as a controller, within the meaning of that provision, even if that entity has not itself performed any processing operations in respect of such data, has not expressly agreed to the performance of specific operations for such processing or to that mobile application being made available to the public, and has not acquired the abovementioned mobile application, unless, prior to that application being made available to the public, that entity expressly objected to such making available and to the resulting processing of personal data." (para 38)

The Ministry body was not solely responsible, however, for the development of the app and the use of personal data. Indeed, it appears that it did not actually have access to the personal data involved. The CJEU nonetheless held that it was a joint controller for GDPR purposes and had joint responsibility for the personal data processing. But the Court accepted that joint controllers may not necessarily have equal responsibility as they may be involved at different stages of the processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case (para 42). Relevant to the question of allocation of responsibility may be whether there was a common decision taken by two or more entities or whether it results from converging decisions of those entities. Where the situation engages the latter – which is to say, converging decisions – entities will have responsibility where each of the decisions complements the other in such a way as to result in a tangible impact on the determination of the purposes and means of processing (para 43). In any event, responsibility does not require a formal agreement between the controllers as regards the purposes and means of processing (para 44).

The use of data for purposes of training AI tools is a necessary part of developing an AI tool. Depending on the objective of the AI tool, personal data may be necessary for this purpose. In academic circles, the adequacy of anonymising personal data for these training purposes has received substantial attention particularly as regards avoiding responsibility for processing. The CJEU addresses this debate first stating that question whether personal data are used for the purposes of IT testing or for another purpose has no bearing on whether the operation in question is classified as 'processing' within the meaning of the GDPR. However, this only applies to data relating to a natural person who can be identified, directly or indirectly (paras 51 and 53). Whether the personal data is used in its original form or as copies makes no difference, the key is the possible identification of the person. But, according to the Court, personal data which have undergone pseudonymisation and which could be attributed to a natural person by the use of

additional information constitutes information on an identifiable natural person, to which the principles of data protection apply (para 58). Accordingly, the Court held that, unless personal data have been rendered anonymous in such a manner that the subject of those data is not or is no longer identifiable, or unless it involves fictitious data which do not relate to an existing natural person, its use including for testing purposes constitutes 'processing' (para 59).

In response to the final questions from the national court, the CJEU examines the issue of liability of controllers for administrative fines. The Lithuanian Government and the Council argued that the GDPR allows a margin of discretion to state authorities to impose administrative fines for breaches without establishing that an infringement was committed intentionally or negligently (para 62). The Court rejects this interpretation outright primarily on the basis of the nature of a regulation as directly applicable and only in specific situations requiring national measures of application (paras 63 and 64). According to the Court, the substantive conditions for the imposition of fines under the GDPR must be applied. This means that only infringements which are committed wrongfully (limited to intentionally or negligently committed ones) by the controller, may result in an administrative fine being imposed on that controller (para 73). But the Court held that a controller may be penalised for conduct falling within the scope of the GDPR where that controller could not have been unaware of the infringing nature of its conduct, whether or not it was aware that it was infringing the provisions of the GDPR (para 81). The standard for determining when a body 'could not be unaware' is decisive here. The Court helpful stated that where the controller is a legal person, it is not necessary for there to have been action by, or even knowledge on the part of, the management body of that legal person to meet the standard (para 82). The fact that the controller did not carry out the processing but it was carried out by a processor on behalf of that controller (para 84). But the controller is neither responsible nor liable where a processor has processed personal data in a manner incompatible with the framework of, or detailed arrangements for, the processing as determined by the controller, or in such a manner that it cannot reasonably be considered that that controller consented to such processing (para 85).

The CJEU's analysis of the development and use of an AI tool from the perspective of the GDPR is most welcome. There has been infrequent judicial attention to this aspect of the burgeoning debate about AI tools and their use (see Ufert). While academic discussion has raised questions about GDPR-proofing AI, clear judicial interpretation is only beginning to emerge. This judgment constitutes an important step in this development and provides key clarification for entities commissioning and developing AI tools with and for use on personal data regarding the safeguards which they need to ensure are in place to comply with GDPR. Where the processing of personal data in the development and use of AI tools takes place in the context of prevention, investigation, detection or prosecution of criminal

offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security instead of the GDPR being the applicable law, the Law Enforcement Directive (LED) applies with different standards of protection for personal data. It will be important to watch the development of CJEU's case law in this area when it is faced with questions relating to the interpretation of the LED and development and use of AI tools.