

UOOU-0341/21

The Office inspected the processor of personal data, namely the supplier of the online vaccination reservation system. The subject of the inspection was primarily a breach of security, consisting of an error in the functionality of the website system of the inspected person, which allowed the display of the insured person's number (and thus also the social security number) and its subsequent transfer to the USA through the tool for obtaining statistical data Google Analytics.

The Office conducted an extensive investigation in order to verify the authenticity of the instructions given by the controller to the processor (controlled person), based on which the processing of personal data took place, including the instructions that related to the security breach that occurred, so that it could reliably determine responsibility for its occurrence.

Above all, the Office stated that the controlled person, as another processor, is jointly responsible for the violation of the provisions of Article 32 paragraph 1 letter b) GDPR, because, as an expert, she did not alert the administrator to the inappropriateness of the instruction to create a system in which the URL address contained the policyholder's number (birth number) and processed this with the simultaneous use of the Google Analytics service, thereby leaking URL addresses including policyholder numbers in the scope approx. 80 thousand data subjects. In the defined period, the processing of personal data by the controlled person was not carried out in accordance with the GDPR when this processing was governed by a contract without the latter fulfilling the attributes of Article 28 paragraph 3 of the GDPR. Furthermore, it also violated Article 37, paragraph 1 of the GDPR, as it did not appoint a personal data protection officer for processing.

The inspection was fundamentally hampered by the approach of the administrator, who for almost the entire duration of the inspection refused (despite repeated calls from the Office) to confirm the processor's claim that the instructions to set up the system in such a way that the security breach occurred were issued by him. He confirmed these only after the inspected person filed objections to the inspection findings. This approach had a negative impact on the length of the inspection, as the confirmation of the instruction was of key importance for determining responsibility (or share in it) for the security breach.

Administrative proceedings were initiated in the matter.

In this context, the Office primarily emphasizes that it is entitled to control also the processor of personal data (i.e. not only the administrator who is primarily responsible for the processing of personal data), while it is also the processor who may be jointly responsible (and in some cases also separately responsible) for breach of GDPR.

ContextLocation: Document folders > Site map > Main menu > Supervisory and decision-making activities > Completed inspections > Inspections for the year 2022 > Inspection activity in the field of personal data protection – 2nd semester > Healthcare > Supplier of the online vaccination reservation systemView current documents | document archive | documents including the archive