The Agency for the Protection of Personal Data imposed an administrative fine on the processing manager - the debt collection agency B2 Kapital d.o.o. in the amount of EUR 2,265,000.00 (HRK 17,065,642.50) due to the following violations of the General Data Protection Regulation:

The data controller did not clearly and accurately inform its respondents about the processing of their personal data through the notification on the processing of personal data (privacy policy), and regarding the legal basis for the return of overpaid funds, which is against the provisions of Article 13, paragraph 1 of the General Regulation on Protection data. This resulted in the non-transparent processing of the respondents' personal data (that is, incorrect information regarding the legal basis of processing from Article 6, paragraph 1 of the General Data Protection Regulation) of which there were (at least) 132,652 at the time of the monitoring, and the privacy policy remained unchanged and the violation has not yet been remedied, i.e. it has lasted from May 25, 2018 until today.

2. Contrary to the provisions of Article 28, Paragraph 3 of the General Data Protection Regulation, the data controller did not enter into a contract on the processing of personal data with the processor for the simple bankruptcy monitoring service of consumers, and thus the security of the personal data of 83,896 respondents (OIB) was threatened, since concluding a contract with the processor is one of a kind of security levers that ensures that the rules for the processing of personal data, their course in the business relationship between the manager and the processor are clearly agreed upon, and that the processor ensures that the processor meets the technical and organizational protection measures during processing personal data of a large number of respondents. It was established that the said violation lasted from the acceptance of the offer to provide the service of monitoring simple consumer bankruptcy, that is, from February 14, 2019 to February 26, 2021, when the business cooperation was interrupted.

3. The controller did not take appropriate technical and organizational protection measures when processing personal data, which is contrary to Article 32, Paragraph 1, Points b) and d) and Paragraph 2 of the General Regulation on Data Protection. By not taking appropriate measures, there was a violation of the security of the personal data of all respondents (at least 132,652 at the time of the surveillance), i.e. their basic identification data (at least in the structure: first and last name, date of birth and OIB) and, consequently, all personal data entered in to the storage systems of the debt collection agency, which are of a financial nature and thus quite sensitive. In the process, it was determined that the violation has been ongoing since at least 2019 and has not yet been remedied, all due to the failure to take appropriate protective measures.

Namely, in December 2022, the Agency for the Protection of Personal Data received an anonymous petition in which it was stated that there was unauthorized processing of a large number of personal data of natural persons - debtors by the debt collection agency, and a USB stick containing personal data was attached. data in the structure of first and last name, date of birth and OIB for a total of 77,317 natural persons who had outstanding debts to credit institutions, and which were purchased by the debt collection agency based on the cession agreement.

On the basis of official duties, the Agency initiated a supervisory procedure in December 2022 and conducted a procedure in which the three previously described violations were determined due to negligent treatment by the processing manager (claims collection agency). The controller bears the greatest degree of responsibility for not taking technical protection measures, since it was precisely because of deficiencies in such a security system that unsafe processing of a large number of personal data occurred. The debt collection agency lost complete control over the movement of personal data of their respondents and could not explain the causes of unauthorized exfiltration (extraction) of personal data.

Also, as an aggravating circumstance in the conducted administrative procedure, certain deficiencies in cooperation were determined. Namely, after several letters sent by the Agency for the purpose of requesting additional statements or documentation from the processing manager, he responded to them before the last days of the set deadline and sent letters for the purpose of extending the deadline and clarifying the requested circumstances, although he could have requested the same before. and which to a certain extent influenced the delay of the procedure. Also, upon repeated requests from the Personal Data Protection Agency for certain documentation (list of system records), the processing manager did not provide it.

Also, as an additional aggravating circumstance, the fact that the data controller has not informed the Agency until today that he has taken additional protection measures that would prevent future risks of established violations and that he has not adjusted the privacy policy available on their website to date has been taken into account.

In conclusion, we state that in this particular case, we are talking about a violation of several provisions of the General Data Protection Regulation by one of the leading companies in the field of debt collection, which should not have allowed itself to process the personal data of a large number of respondents in a non-transparent and insecure manner. Also, the data controller would probably never have noticed the exfiltration of personal data of a large number of respondents, at least for 77,317 of them from their system, if the Agency for the Protection of Personal Data had not received an anonymous report and conducted surveillance activities. To this day, the data controller has not clarified all the circumstances of the breach, i.e. the

transfer of a certain amount of personal data outside their storage system, which additionally speaks of inadequate protection measures on the part of the data controller.

We also point out that in this particular case we are talking about possible individual criminal liability, that is, the commission of a criminal offense, which is the responsibility of the Ministry of the Interior, which conducts criminal investigations within its jurisdiction.