*OFFICE OF THE COMMISSIONER*
*FOR PERSONAL DATA PROTECTION*

Our ref. 11.17.001.008.042

17 February 2021

Data Protection Officer
GRS Professional Recruitment Services Ltd
Limassol, Cyprus

**Subject: Investigation of complaints concerning a data breach occurred on 11.02.2020**

Dear Sir,

Following our exchange of communications concerning the above subject, we hereby inform you on the decision of the Commissioner.

We recall that three complaints were lodged in Malta in February 2020, against the controller GRS Recruitment LTD, and the incident involves two emails sent to 201 recipients on 11/02/2020, providing information about IT job vacancies and in which the email addresses were shown to all recipient (emails were sent with cc instead of bcc). The recipients of the messages were candidates who registered with the controller. The complainants expressed concerns about the possible consequences of the unlawful disclosure of their personal data to third parties.

It is noted that the data breach was notified to the Commissioner by the controller on 12/02/2020 and it was further communicated to the data subjects, in line with articles 33 and 34 GDPR. In the data breach notification submitted on 12/02/2020, you affirmed that the cause of the breach was due to an internal human error and not to a malicious user. Concerning the measures taken before the breach, you stated that the company adheres to the principles of privacy by default, that all employees undertook training on how contacting data subjects, how personal data should be respected and handled, including on how to send job notifications to data subjects. Concerning the actions taken after the incident, you proposed as a corrective measure to impose to employees obtaining the approval of a Director and the DPO of the company before any external email can be sent to more than three data subjects, whilst the employee who made the error, will be subject to a disciplinary hearing and will undertake further training.

In the course of the investigation process of the complaints received, you explained that the procedure of the identification and handling of personal data breaches was effective, since it enabled the controller to notify the breach to the Commissioner within the timeframe foreseen in the GDPR. Moreover, you affirmed that, to date, none of the data subjects instituted legal proceedings against the controller claiming compensation of any damage which the data subject may have suffered as a result of the data breach.

After assessment of all information available in relation to this case, the Commissioner considers that by disclosing the email addresses of candidates to all the recipients, the controller infringed the obligations referred to in Article 32 of the GDPR. The Commissioner further considers that appropriate technical and organisational measures should be taken to ensure the protection of the rights and freedoms of natural persons with regard to the processing of their personal data.

You previously proposed a number of corrective measures to mitigate the risks, however the Commissioner requires additional technical measures to be implemented by the controller to prevent such an incident to occur in the future and namely –

- An alert message to be clearly displayed every time an email is sent to recipients outside the organisations;
- Whenever a mass email is to be sent, an information message shall pop-up on the sender's screen in a manner that cannot be missed and, ideally, preventing the user from proceeding with the sending of the communication unless a positive action is taken, such as, prompting the user to close the message box;
- Disable the cc field or limit the number of email addresses that the field can contain;
- Set up a delay rule in the delivery of any email message.

In light of the above, and in accordance with the powers conferred to the Commissioner by Article 58(2)(d) of the GDPR, the Commissioner orders the controller:

a) to implement the technical measures described above,

b) to inform the Commissioner on the actions taken to comply with this Decision at the latest within one month from the date of this letter

Best regards,

Commissioner
for personal data protection