



Dear Former Colleagues,

We have been informed by one of our third-party vendors that non-sensitive information regarding some former staff and service providers who worked at our company was accessed by an unauthorised third party on 31 May 2023.

The vendor hired a cybersecurity consultancy to investigate and took immediate steps to patch the vulnerability in their software.

We now know that the accessed information includes name, employee ID, line manager ID, work email address, job title, phone number, business area and work location.

At present we are not aware of any unauthorised use of this data, but we encourage you to continue to be vigilant in identifying phishing and social engineering attempts, as part of our ongoing efforts to protect our colleagues and our customers.

For inquiries, please contact kvkkiletisim@hsbc.com.tr.

Regards,

HSBC Portföy Yönetimi A.Ş