

Public notification of cyber-attack on Electoral Commission systems | Electoral Commission Search Public notification of cyber-attack on Electoral Commission systems You are in the section Home about the cyber-attack Information about the cyber-attack First published: 8 August 2023 Last updated: 8 August 2023 Introduction The Electoral Commission has a duty under Articles 33 and 34 of the UK General Data Protection Regulation to notify data subjects if their data has been breached by inappropriate access, loss, or theft from our systems. This notification gives important information about the personal data affected, the potential impact on individuals, and measures we've taken in response to a complex cyber-attack. The incident was identified in October 2022 after suspicious activity was detected on our systems. It became clear that hostile actors had first accessed the systems in August 2021. During the cyber-attack, the perpetrators had access to the Commission's servers which held our email, our control systems, and copies of the electoral registers. They were able to access reference copies of the electoral registers, held by the Commission for research purposes and to enable permissibility checks on political donations. The registers held at the time of the cyber-attack include the name and address of anyone in Great Britain who was registered to vote between 2014 and 2022, the names of those registered as overseas voters during the same period, and the names and addresses of anyone registered in Northern Ireland in 2018. The registers did not include the details of those registered anonymously. The Commission's email system was also accessible during the attack. We understand the concern this attack may cause and apologise to those affected. Since the attack was discovered, we have worked with security specialists to investigate the incident and have taken action to secure our systems and reduce the risk of future attacks. Public notification It is our assessment that the information affected by this breach does not pose a high risk to individuals and this notification is being given due to the high volume of personal data potentially viewed or removed during the cyber-attack. Personal data affected by this incident: Personal data contained in email system of the Commission: Name, first name and surname. Email addresses (personal and/or business). Home address if included in a webform or email. Contact telephone number (personal and/or business). Content of the webform and email that may contain personal data. Any personal images sent to the Commission. Personal data contained in Electoral Register entries: Name, first name and surname Home address in register entries Date on which a person achieves voting age that year. Electoral Register data not held by the Commission: Anonymous registrations Address of overseas electors registered outside of the UK. Electoral register copies The Commission holds copies of the electoral registers to enable its statutory functions. They are used for research purposes and to enable permissibility checks on political donations. The electoral register data held by the Commission has not been amended or changed in anyway as a result of the attack and remains in the form in which we received it. The data contained in the registers is limited, and much of it is already in the public domain. Our online privacy policy is accessible online via the following link <https://www.electoralcommission.org.uk/privacy-policy> Impact on individuals According to the risk assessment used by the Information Commissioner's Office to assess the harm of data breaches, the personal data held on the electoral registers – typically name and address – does not in itself present a high risk to individuals. It is possible however that this data could be combined with other data in the public domain, such as that which individuals choose to share themselves, to infer patterns of behaviour or to identify and profile individuals. The attack has not had an impact on the electoral process, has not affected the

rights or access to the democratic process of any individual, nor has it affected anyone's electoral registration status. The personal data held on the Commission's email servers is also unlikely to present a high risk to individuals unless someone has sent us sensitive or personal information in the body of an email, as an attachment or via a form on our website, such information may include medical conditions, gender, sexuality, or personal financial details. Information related to donations and/or loans to registered political parties and non-party campaigners is held in a system not affected by this incident. No immediate action needs to be taken in response to this notification. However, anyone who has been in contact with the Commission, or who was registered to vote in Great Britain between 2014 and 2022, and in Northern Ireland in 2018, should remain vigilant for unauthorised use or release of their personal data. If you have concerns over personal data which you may have sent to the Commission, please contact our Data Protection Officer, using the details below.

Mitigations We have taken steps to secure our systems against future attacks and improved our protections around personal data. We have strengthened our network login requirements, improved the monitoring and alert system for active threats and reviewed and updated our firewall policies. The Commission has worked with external security experts and the National Cyber Security Centre to investigate and secure its systems. Data subjects retain the right to complain to the UK Supervisory Authority, the Information Commissioner's Office (ICO). Contacting us about the cyber-attack

The Electoral Commission London office address 3 Bunhill Row, London EC1Y 8YZ, email: dataprotection@electoralcommission.org.uk for the purposes of this notification. The Data Protection officer is Andrew Simpson, Head of Digital, Data, Technology and Facilities. Information about the cyber-attack

Read answers to questions you may have about the cyber-attack

Submit our form to find out about your data, or to make a complaint