ICO sets out revised approach to public sector enforcement

Share

Date
30 June 2022

Type
News

The Information Commissioner's Office (ICO) has today set out a revised approach to working more effectively with public authorities.

This approach, which is outlined in an open letter from the UK Information Commissioner John Edwards to public authorities, will see use of the Commissioner's discretion to reduce the impact of fines on the public sector, coupled with better engagement including publicising lessons learned and sharing good practice. It will be trialled over the next two years.

In practice, this will mean an increased use of the ICO's wider powers, including warnings, reprimands and enforcement notices, with fines only issued in the most serious cases.

When a fine is considered, the decision notice will give an indication on the amount of the fine the case would have attracted. This will provide information to the wider economy about the levels of penalty others can expect from similar conduct.

Additionally, the ICO will be working more closely with the public sector to encourage compliance with data protection law and prevent harms before they happen.

In support of this approach, the ICO has received a commitment from the UK Government, specifically from the Cabinet Office and the Department for Digital, Culture, Media and Sport, to create a cross-Whitehall senior leadership group to encourage compliance with high data protection standards. The ICO will also engage with the Devolved Administrations and the wider public sector to determine the most effective way to deliver these improvements in these areas.

This revised approach is just one of the initiatives that will be set out in the coming weeks as part of ICO25 – the ICO's new three-year strategic vision – to empower organisations to innovate while using people's data responsibly.

gender identity patients. The 2019 breach happened because the trust failed to use the 'Bcc' field and, within 30 minutes of the mailing, a screenshot of the email was shared on social media including the email addresses of some of the people affected.

Another recent ICO enforcement action includes a reprimand issued to NHS Blood and Transplant Service, after they inadvertently released untested development code into a live system for matching transplant list patients with donated organs in August 2019. This error led to five adult patients on the non-urgent transplant list not being offered transplant livers at the earliest possible opportunity. The organisation remedied the error within a week, and none of the patients involved experienced any harm as a result.

John Edwards, UK Information Commissioner, said:

> "I want to ensure my office remains a pragmatic, proportionate and effective regulator focused on making a difference to people's lives. That means taking a more proactive and targeted approach with public authorities to ensure they are looking after people's information while supporting their communities.
>
> "In the case of Tavistock and Portman NHS Foundation Trust, the breach revealed much more than people's email addresses. Knowing about someone's relationship with a gender identity clinic could be hugely dangerous and damaging to the patients' well-being and personal safety. The trust also failed to learn from previous incidents.
>
> "The NHS Blood and Transplant Service already had good data protection policies and systems in place, but a single human error that went undetected contributed to an incident that could have caused potential harm to people on the non-urgent transplant list.
>
> "My office worked with both organisations to improve their data protection standards and practices. We used different enforcement tools but, crucially, both resulted in changes that better protect the public."

Details of the Tavistock and Portman NHS Foundation Trust incident

In early September 2019, the trust intended to run a competition inviting patients of the adult Gender Identity Clinic to provide artwork to decorate a refurbished clinic building. They sent two identical emails promoting the competition (one to 912 recipients, and the second to 869 recipients) before realising they had not Bcc'd the addresses.

email addresses.

The trust immediately realised the error and tried, unsuccessfully, to recall the emails. They wrote to all the recipients to apologise and informed the ICO later that day.

The ICO investigation found:

- Two similar, smaller incidents had affected a different department of the same trust in 2017. While that department had strengthened their processes as a result, the learning and changes were not implemented across the whole trust.
- The trust was overly reliant on people following policy to prevent bulk emails using 'to' in Outlook. There were no technical or organisational safeguards in place to prevent or mitigate against this very predictable human error. The trust has since procured specialist bulk email software and set "a maximum 'To' recipient" rule on the email server.

The ICO acknowledges that the trust took prompt action to remedy the breach, including prompt notification of the matter and ongoing engagement with the ICO.

With the revised approach, the fine issued to the trust was reduced from £784,800 to £78,400.

Details of the NHS Blood and Transplant Service incident

In August 2019, developers working on the code were finalising changes for matching kidney and pancreas donations to patients. At the same time another developer was working on a future release for liver transplants. Some of the "liver" code was committed to the master version before the "kidney" code was locked down for testing and publishing.

The error was not spotted during user acceptance testing as the developers only considered the impact of the "kidney" code changes, rather than thoroughly testing the entire system.

The full code - including the untested "liver" code - was published on 11 September 2019. The untested code meant five patients awaiting livers were not matched with potentially available organs. The error was spotted and fixed a week later, on 18 September, and there is no evidence of any long-term harm from the incident to the individuals who were directly affected. Of the five people affected, three later received liver donations, and two were too ill at the time of the error to have undergone a transplant. On becoming aware of the error, NHS Blood and Transplant immediately suspended the system and launched an investigation.

NHS Blood and Transplant has engaged fully with the ICO investigation and taken full responsibility for what happened. The organisation has not only learned from our findings

If the revised approach had not been in place, then NHS Blood and Transplant would have received a fine of £749,856. The Information Commissioner has exercised his discretion to reduce the proposed fine to a public reprimand.

Notes to Editors

1. The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
2. The ICO has specific responsibilities set out in the Data Protection Act 2018 (DPA 2018), the UK General Data Protection Regulation (GDPR), the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.
3. The ICO has a number of powers with which to encourage and enforce adherence to the relevant legislation. These include issuing reprimands; ordering organisations to process data differently or stop processing; ordering audits of structures or policies; banning them from holding data and imposing a civil monetary penalty of up to 4% of global turnover.
4. To report a concern to the ICO telephone our helpline 0303 123 1113 or go to ico.org.uk/concerns.