16 May 2023

Case Reference IC-227469-P3V4

Your request

You asked us for the following:

"*the Information Commission Office Policy, protocols, procedures, compliance with statutory duties, and training of case worker applying to:*

1/ The ICO's Public Sector Equality Duty towards the s7 protected characteristic of Gender Reassignment, Part 11 such as s149 and s150 of Equality Act 2010?

2/ The ICO's Public Sector Equality Duty towards the s7 protected characteristic of Gender Reassignment, s1 of Equality Act 2010? For example how does the ICO address that people who share the s7 protected characteristic are on average the poorest of all protected characteristics, with greatest health and economic damage caused by inaccurate data, and least resources to legally enforce the Data Protection Act 2018.

3/ How the ICO facilitates it being alerted to a s22 Gender Recognition Act 2004 offence of unauthorised protected information? The procedures the ICO takes to investigate s22 offences and the priority the ICO gives to it?

4/ Training given to ICO caseworkers and management of special category data linked to individuals with s7 protected characteristic who make a subject access request, or the procedures used by data controllers which may impact them:
for example (but not limited to): (i) medical assignment of gender/sex at birth, (ii) medical treatment and other alterations associated with gender reassignment, (iii) perceived or declared changes of sexuality, (iv) perceived or declared sex life arising from medical steps in reassignment, (v) perceived or declared genetic data (e.g. XX or XY sex chromosomes), (vi) protected information following application for or granting of a Gender Recognition Certificate (GRC).

5/ Ensuring compliance of political parties GDPR duties towards their members and potential candidates , i.e., Articles, 5, 6, 7, 9, & 14. And compliance with Articles 15-22.

6/ Procedures to ensure data about s7 and other protected information is not being used for unlawful discrimination, victimisation, a

7/ In relation to the above re political parties, the additional Article 9 data safeguards and Article 14 reporting duties for s7 members & candidates data about (i) medical treatments undertaken for gender reassignment (such as surgical procedures, hormone treatment, appearance alteration), (ii) application for/ possession of a GRC?

8/ S170 investigation and prosecution: What is considered grounds for investigation and the priorities given to investigation?
9/ What procedures are in place to minimise risk of Data Controllers not reporting s170 breaches? Including Articles 33 & 34 duties?
10/ What procedures are in place to minimise risk of Data Controllers not informing the data subjects that they are holding or processing their data such as special category data and protected information?
11/ What procedures are in place to minimise risk of Data Controllers not reporting breaches of personal data? Including special category data and protected information. Including Articles 33 & 34 duties?
12/ What procedures are in place for the ICO to be alerted to non-compliance by a data controllers with their Articles 33 & 34 GDPR duties? Such as (but no limited to): (i) enabling whistleblowers to report such breaches or non-compliance with GDPR, (ii) enabling an individual data subject who became aware that their data had been breached to make a complaint on behalf of all those likely to have been affected by the same breach regardless of whether they/others had made an SAR.
13/ Related to the above, what procedures are in place for data subjects to alert the Information Commission Office that they have become aware that their data/ special category data/ protected information has been compromised but they do not know by who? This might arise if a data controller does not comply with their Article 14 and/or Article 34 duty.
14/ What is the policy to investigation, enforcement, and penalties to be applied to data controllers who fail to comply with the Duty to enforce compliance with Articles 33 & 34 for breaches of data affecting s7 people.

15/ In one known example which the ICO handled: over 100 s7 individuals had their special category data breached but were not informed that the breach. When the ICO discovered this, the ICO decided not to enforce the duty on the data controllers to report the breach to the s7 individuals affected, and take action against the data controllers. What is the policy reason why the ICO enforces

GDPR compliance on some data controllers but not others? Is it based upon numbers affected? Is it based upon protected characteristics? Is it based upon which special category data is breached? If non GDPR-compliance is considered more serious if it affects some protected characteristics but not others what is the reasoning for this?

16/ A s173 offence occurs when a person listed in s173(4) alters, defaces, blocks, erases, destroys or conceals information with the intention of preventing disclosure of all or part of the information in the response to the SAR. However, how would a data subject know that their data had been altered, blocked, in the response to their SAR? What policy and procedures do the ICO have in place to detect this misleading?
In the example of the 100 s7 individuals affected above, the concealment of data from data subject requests was only realised after a whistleblower reported it to the ICO. However, the ICO said it could not take action against the data controller & alleged offenders unless the data subject who had made the SAR complained to the ICO themselves not the whistleblower. Perversely the ICO then warned the whistleblower that they would be committing a s170 offence if they informed the data subject of the concealment instead of the data controller even though it was the data controller & data protection officer who were concealing it. This appears to thwart investigation and prosecution of any s173, s144, s148 offences if the data controller is complicit or covering up.
Given this, what procedures are in place to detect s173, s144, and s148 offences? Who can report the alleged offence if the data subject is unaware?
Further complications and hurdles with s173 are: 1/ The charge has to be laid within six months by the ICO, 2/ The Data Protection Act 2018, abolished whistleblowers s170(2) defence of 'believing' they are acting to detect a s173 offence. How is the ICO addressing s173 becoming a dead-letter offence, including not only policy, procedure, and caseworker training, but also plans for the ICO to use s139, 140, or 141 to highlight the problem?

17/ Articles 15 & 16, 17-22 are in place to ensure a data subject can correct inaccurate data and object to unlawful data acquisition, processing, and retention. Given the problems I have raised above (non-compliance with Articles 14, and 34, and s173 being undetectable by the data subject), what policies, processes, and procedures are the ICO using to ensure data subjects can enforce their GDPR rights under Article 15-22?"

Where your questions satisfy the criteria of a valid information request, we have considered your request under the Freedom of Information Act 2000 (FOIA).

Our response

1-3. To the extent that the ICO holds information within scope of each of these questions, it is contained in the following documents:

- Our online guidance on What is special category data? | ICO
- Our online guidance on What about fairness, bias and discrimination? | ICO (Use of Artificial Intelligence)
- ICO25 – Our regulatory approach This references our responsibilities under the Equality Act 2010

4. We can confirm that we do hold some information within scope of this part of your request.

Please see the attached word version of an interactive tool used to establish whether personal data constitutes a protected characteristic/special category data. Please note: this document is in a developmental stage and may not represent the final product.

In terms of internal procedures/policies, our Public Advice and Data Protection Complaints Service uses the attached policy and principles document.

The names of individual members of staff have been redacted under section 40 of the FOIA as we do not think it fair and proportionate to disclose them. We have also redacted an internal email under section 31. As this is a qualified exemption we shall explain our reliance on it below this response.

Please note: The ICO is currently developing a Transgender Policy which covers both staff and stakeholders.

5-7. No specific information held. We handle complaints, breach reports and investigations on a case by case basis and this includes political parties.

Please note: Our investigations-manual-final-disclosure-redacted-3.pdf (ico.org.uk) covers our general processes when engaging in investigations, including the prioritisation of cases.

8. Each case is considered on its own merit and decisions taken based on the case circumstances. To the extent that we hold information, it is contained in our:

Regulatory Action Policy (ico.org.uk)
Data Protection Regulatory Action Policy V2 (ico.org.uk)
ico-prosecution-policy-statement.pdf

9-11. Our Regulatory Action Policy (ico.org.uk) details that failure to report to the ICO or inform data subjects may constitute an aggravating factor when considering regulatory action.

12. (i) Please see our Protected disclosures to the ICO – Whistleblowing | ICO
(ii) This would most likely be our Data protection and personal information complaints tool | ICO

13 -15. Each case is considered on its own merit and decisions taken based on the case circumstances. Again, our Regulatory Action Policy (ico.org.uk) constitutes what information we have within scope.

16. No information held. Each case is considered on its own merit and decisions taken based on the case circumstances. Corroborating evidence may be requested should investigating officers not be satisfied with what has been provided. In terms of detecting offences, again this is down to individual cases and reports brought to us. Anyone with evidence can make a report top the ICO, but the engagement and support of the data subject would be required.

Whistle-blowers are covered by the Public Interest Disclosure Act 1998, not the DPA 2018.

17. No specific information held. We handle complaints, breach reports and investigations on a case by case basis.

Please note: the links provided above demonstrate that the information within scope signposted by them is available to you by other means. This means that such information is technically exempt from disclosure under section 21 of the FOIA.

Section 31

We have withheld an internal email address under section 31(1)(g) of the FOIA. We can do this when the disclosure of information "*would, or would be likely to, prejudice…the exercise by any public authority of its functions for any of the purposes specified in subsection (2)*."

In this case the relevant purposes contained in subsection 31(2) are 31(2)(a) and 31(2)(c):

" *a. the purpose of ascertaining whether any person has failed to comply with the law, and*
c. the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise."

Misuse of internal email addresses that exist to support ICO staff would likely prejudice our ability to perform our regulatory functions. Disclosure would leave us vulnerable to phishing or other cyber-attacks, spam, or an increased volume of irrelevant correspondence which it would take us time to process.

There are other channels that the public can use to contact us, and they are publicly available via our website.

The exemption at section 31(1)(g) is not absolute. When considering whether to apply it in response to a request for information, there is a 'public interest test'. We have to consider whether the public interest favours withholding or disclosing the information.

In this case the public interest factor in favour of disclosing the information is:

- Increased transparency in the way in which the ICO conducts its operations.

The public interest factors in maintaining the exemption are as follows:

- Internal email addresses being used inappropriately will reduce the effectiveness and efficiency of our regulatory functions.
- The information of primary relevance to your request is not affected by the redaction of our internal email addresses.

- The public interest in transparency is met by the public provision of other more appropriate means of contacting us.

Having considered all of these factors we have taken the decision that the public interest in withholding the information outweighs the public interest in disclosing it.

This concludes our response.

We hope you find this information helpful.