Data Protection and Freedom of Information Legal Update

December 2023

Contents

Legislation and guidance

This section features legislative developments from the Scottish and UK Parliaments and also any highlights from data protection and information law related policy changes from the UK or EU.

Data Protection and Digital Information (No. 2) Bill 2022-23

The UK Government's Data Protection and Digital Information (No. 2) Bill was the subject of a lively debate in the House of Commons on 29 November following the Government's introduction of 240 amendments to the Bill at a late stage in proceedings.

The UK Government asserts that the Bill "seizes on a post-Brexit opportunity" to create an innovative, flexible and risk-based data protection regime. Further, the UK Government considers that this bespoke model will unlock the immense possibilities of data use to improve the lives of everyone in the UK and help make the UK the most innovative society in the world through science and technology.

Opposition MPs expressed concern on behalf of their constituents that any material deviation from existing standards, particularly European Union data adequacy, would actually entangle them in more red tape, rather than remove it.

In response, the Government confirmed that there is nothing in these proposals that puts data adequacy at risk. However, it is not necessary to replicate every aspect of GDPR in order to be assessed as adequate by the European Union for the purposes of data exchange so there are some changes.

A full review of the Bill is not possible in this summary article but there is commentary on each provision of the Bill as it currently stands within the accompanying explanatory notes at: https://bills.parliament.uk/publications/53323/documents/4144

Some notable amendments include:

- Regulations will be made requiring new open and common standards for access to customer data and business data to allow for interoperability across the UK economy.
- In the future, organisations will need to keep records of their processing activities only when those activities are likely to result in a high risk to individuals.
- More time for data controllers to report data breaches; they will now have to be reported without undue delay and, where feasible, no later than 72 hours after the breach. This change will allow organisations to gather more detailed information about the breach before the reporting deadline and allow the ICO to focus its efforts on assessing that information once it has been achieved.
- Organisations will be allowed to raise data breach complaints on behalf of data subjects generally, in the absence of a particular subject who wishes to bring forward a claim about misuse of their own personal data.
- There will be a review of the operation of the "Tell Us Once" programme, which seeks to provide simpler mechanisms for citizens to pass information regarding births and deaths to government, and consideration of whether the progress of "Tell Us Once" could be extended to non-public sector holders of data.
- Data controllers will be required to provide evidence of why a request has been considered vexatious or excessive if the controller is refusing to take action on the request.

- New protections for decisions based on automated processing would apply where a decision is based either solely or partly on automated processing, not only where it is based solely on such processing.

The Bill has now passed over to the House of Lords where a second reading will take place on 19 December.

Access the Bill papers: https://bills.parliament.uk/bills/3430

Proposed Freedom of Information Reform (Scotland) Bill

The final proposal for the Freedom of Information Reform (Scotland) Bill, put forward by Scottish Labour MSP Katy Clark, was lodged on 7 December. The proposed Bill aims to modernise FOI rules and extend coverage to all bodies delivering public services and services of a public nature. For example, private social care providers, COSLA, charities and sports governing bodies would all be within scope, amongst others.

The proposed legislation is backed by the Campaign for Freedom of Information in Scotland (CFOIS) but the Scottish Government, which carried out its own consultation on FOI reforms earlier this year, has apparently ruled out new legislation in favour of secondary reforms and further consultations so we will keep an eye on how things progress.

Access the proposed Bill: https://www.parliament.scot/bills-and-laws/proposals-for-bills/proposed-freedom-of-information-scotland-bill

---

ICO and European Data Protection Supervisor Memorandum of Understanding

The UK ICO has signed a Memorandum of Understanding (MoU) for cooperation in the application of laws protecting personal data with the European Data Protection Supervisor (EDPS).

The ICO says that this reinforces the shared mission to uphold people's data protection and privacy rights across the UK and Europe. Together with European regulators, the ICO is committed to:

- sharing experiences and best practices;
- cooperating on projects of interest;
- sharing information or intelligence to support regulatory work; and
- promoting dialogue among data protection authorities and other digital regulators.

The MoU will not involve the sharing of any personal data and is in line with the ICO's legal responsibilities and with the UK commitment to protect the personal data of its citizens, while enabling the opportunities of digital innovation.

The European Union AI Act

The European Parliament and Council have reached a political agreement on the AI Act, which was first proposed by the European Commission back in April 2021.

The AI Act takes a risk-based approach whereby "minimal risk" systems – which the EU says covers the majority of AI systems – will only be lightly regulated, while "high risk" systems will be strictly regulated and those with "unacceptable risk" will be banned altogether.

AI systems which will be banned include those which manipulate human behaviour to circumvent users' free will, such as toys using voice assistance encouraging dangerous behaviour of minors or systems that allow 'social scoring' by governments or companies, and certain applications of predictive policing.

In addition, some uses of biometric systems will be prohibited, such as emotion recognition systems used at the workplace and some systems for categorising people or real time remote biometric identification for law enforcement purposes in publicly accessible spaces, with some exceptions.

The AI Act provides for the creation of a new European AI Office within the European Commission to ensure coordination at European level, whilst national market surveillance authorities will supervise the implementation of the new rules at national level.

The political agreement is now subject to formal approval by the European Parliament and Council. The legislation will not take effect until at least 2025 but to bridge the transitional period before the regulation becomes generally applicable, the Commission will launch an AI Pact; inviting AI developers to commit to implementing key obligations of the AI Act on a voluntary basis ahead of the legal deadlines.

Artificial Intelligence (Regulation) Bill

The Artificial Intelligence (Regulation) Bill is a UK Private Members' Bill originating in the House of Lords. It proposes the creation of a regulatory body called the AI Authority to monitor the use and regulation of AI in the UK.

The proposed legislation sets out regulatory principles for the AI Authority to follow and suggests a regulatory sandbox to allow for the testing of AI products. It also proposes that any business which develops, deploys or uses AI should have a designated AI officer.

The Bill received its first reading in the House of Lords on 22 November 2023 but, as a Private Members' Bill this particular legislation is unlikely to become law. It does however raise some of the issues that the UK Government will need to think about in their own approach to AI regulation.

AI and data protection are inextricably linked due to AI models' use of data to generate output and as AI is being used increasingly for the processing of personal data. It is therefore important to understand how AI is to be regulated and the relationship with existing data protection rules.

Access the Bill papers: https://bills.parliament.uk/bills/3519

Cases

Our case law update focuses on developments from the past few months which change or clarify the law in respect of data protection and information law issues or are examples of how breaches can arise.

Information gathered by an independent expert is "held" by the authority

An important Freedom of Information decision was issued by the Inner House of the Court of Session this month in an appeal brought by the Scottish Ministers against a decision of the Scottish Information Commissioner.

In March 2018, former First Minister Mr Alex Salmond was notified that an investigation had been commenced against him by the Scottish Government, as a result of complaints received by two civil servants regarding his behaviour during his time as First Minister. Mr Salmond's successor, the (now former) First Minister Ms Nicola Sturgeon met Mr Salmond's former Chief of Staff and, thereafter, met Mr Salmond three times, and spoke with him by phone three times.

Ms Sturgeon subsequently referred herself to the independent advisers on the Scottish Ministerial Code for an alleged breach of the Code. The breach was said to concern whether Ms Sturgeon failed to record the meetings and phone calls in accordance with the Code, and/or whether she attempted to influence the conduct of the internal investigation into Mr Salmond's behaviour. An independent adviser, Mr James Hamilton, investigated. In March 2021, he issued his report in which he determined that Ms Sturgeon had not breached the Code.

Two weeks later, the Ministers received a request under the Freedom of Information (Scotland) Act 2002 for all written evidence ingathered by Mr Hamilton's investigation. The Ministers declined to provide the information on the basis that Mr Hamilton was independent of them. Any information held by Mr Hamilton was not "held" by or on behalf of the Ministers within the meaning of section 3(2) of the Act. Therefore, the information held by Mr Hamilton did not fall within the scope of the Act and did not require to be disclosed by the Ministers. The Minsters also relied on the exemption in section 30(c) of the Act that disclosure of the information would cause substantial prejudice to the effective conduct of public affairs. They upheld that decision upon review.

The applicant appealed to the Scottish Information Commissioner who determined that the Ministers were wrong to find that they did not "hold" the information ingathered and held by Mr Hamilton and his team. There was an appropriate connection between the information and the interest of the Ministers. The fact that access to the information had been restricted to Mr Hamilton and his team was a procedure which was put in place by the Ministers; they could revoke it if they wished. He ordered the Ministers to carry out a further review and respond to the FOI request anew.

The Ministers appealed the Commissioner's decision. They argued that this was an overly technical approach to the word "held", and that it would be destructive of Mr Hamilton's independence if the Scottish Ministers were entitled to access the evidence he has ingathered. The information has not been ingathered or held for the purposes of discharging any of the Ministers' functions. Any connection between them and the information is therefore not an "appropriate" connection.

However, the Inner House upheld the Commissioner's decision, noting that whether information is or is not held by a public authority is fundamentally a question of fact.

In this case, the information was part of an internal decision-making process conducted by the Ministers in the context of determining whether the Scottish Ministerial Code had been breached. Mr Hamilton was essentially an adviser to the Scottish Ministers and the information was gathered on the instructions of the Ministers. There was nothing in Mr Hamilton's remit to suggest that the Ministers were only entitled to receive his report and not the information on which it was based. This all points strongly towards the existence of an appropriate connection between the information and the Scottish Ministers.

Further, the information was held on the Scottish Government's IT systems. Internal restrictions had been imposed on who could gain access to the information but the very fact that the Scottish Ministers had the requisite control over the information to be able to regulate access to it infers that they held the information.

The court found that the information ingathered by Mr Hamilton and his team in the course of the investigation is "held" by the Scottish Ministers for the purposes of the Freedom of Information (Scotland) Act 2002 so the Scottish Ministers must consider the FOI request anew.

This decision has potential wider implications for information which is gathered or created by independent third party experts who are appointed by authorities which are subject to the FOI regime.

Access the judgment: https://www.scotcourts.gov.uk/docs/default-source/cos-general-docs/pdf-docs-for-opinions/2023csih46.pdf?sfvrsn=b234127a_1

Vexatious FOI requests

Generally speaking, FOI requests should be treated as 'requester-blind'. However, the Scottish Information Commissioner has recognised that a requester's identity can, in limited circumstances, be relevant when deciding whether a request is vexatious.

In Decision 083/2023, the Commissioner accepted that the requester's identity was relevant in determining whether their requests were vexatious because of the history, nature and volume of their previous correspondence on similar matters.

The Applicant had asked the University of Edinburgh for information on several matters, but her requests primarily focused on information relating to Roxburgh Street/Place, Edinburgh. The University declined to comply with the requests as it considered them vexatious or manifestly unreasonable. The Commissioner investigated and found that the requests were vexatious or manifestly unreasonable, and so the University was not obliged to respond.

The Commissioner considered it relevant that the requester had previously been warned that their requests were in danger of becoming vexatious, that their campaign was not well founded and that they had failed to take their concerns up with the relevant authorities.

The Commissioner therefore agreed that the requests were vexatious (under FOI) or manifestly unreasonable (under the EIRs).

Access the decision: https://www.itspublicknowledge.info/decision-0832023

Guidance on the 'neither confirm nor deny' provision

Over the last month, a number of the Commissioner's decisions have considered the application by authorities of section 18 of the FOI Act. Section 18 allows public authorities, in some circumstances, to refuse to confirm or deny whether certain information exists, or is held.

In each of these recent cases, the Commissioner did not uphold the authority's use of section 18.

When applying section 18, public authorities must consider the public interest in confirming whether or not the information is actually held or exists. In Decision 100/2023 the Commissioner found that an authority's submission focussed more on the actual content of the information. He therefore concluded that the authority had not been entitled to refuse to reveal whether the information was held.

In two other cases (Decisions 101/2023 and 104/2023), although the Commissioner accepted that the authority would be entitled to refuse to disclose the requested information under exemptions in the FOI Act, he was not satisfied that the harmful effects suggested by the authority would occur if it confirmed whether or not relevant information existed or was held. He therefore concluded that there was not a strong public interest argument to refuse to confirm or deny whether the information was held.

These decisions provide an insight into the Commissioner's considerations when determining whether it is reasonable for an authority to apply section 18 of the FOI Act in response to a request.

Paragraph 15 of the Commissioner's Content of Notices guidance also has advice for authorities when considering this provision.

Court of Appeal finds against ICO in interpretation of public interest exemption rules

The Department for Business and Trade v The Information Commissioner & Anor concerned the proper interpretation of section 2(2) of the Freedom of Information Act 2000 (which has equivalent provisions to the Freedom of Information (Scotland) Act 2002) and how to approach the public interest test where there are two or more different statutory provisions exempting information from disclosure.

The background to this case was that a journalist made an FOI request about trade working groups which were set up ahead of trade negotiations with other countries post-Brexit. The department disclosed some of the information requested but refused to disclose the minutes of the meetings of trade working groups, relying on the fact that the minutes were exempt information within the meaning of sections 27 (International relations) and also 35 (Formulation of government policy, etc.) of FOIA.

The applicant appealed to the Upper Tribunal, submitting that the two separate interests under sections 27 and 35 should not be aggregated when weighing them against the public interest in disclosure, they should each be considered separately. The Upper Tribunal agreed that aggregation was not permitted.

This is the same view held by the ICO - that the public interest in each individual statutory provision exempting information from disclosure has to be weighed separately against the public interest in disclosing the information; two separate interests cannot be combined together to be weighed against the public interest. This effectively means that at least one of the potential exemptions must be strong enough on its own to prevent disclosure; it is not permitted to look at all of the different points in the round and conclude that together they are sufficient to override the public interest.

However, the Department for Business and Trade appealed further to the Court of Appeal which found against the ICO. The Court of Appeal held that section 2(2)(b) of FOIA does permit the public interest to be aggregated when deciding whether the public interest in maintaining the exemption of information from disclosure outweighs the public interest in its disclosure. It is therefore the overall weight of all of the factors combined which determines whether or not the information requires to be disclosed.

The ICO is considering this outcome and its next steps.

Access the judgment: https://caselaw.nationalarchives.gov.uk/ewca/civ/2023/1378

FOISA appeal refused on public interest grounds

William Beggs, the "limbs in the loch" killer, brought an appeal against a second decision by the Scottish Information Commissioner to uphold Police Scotland's refusal to disclose information in response to a Freedom of Information (Scotland) Act 2002 (FOISA) request made by Mr Beggs.

Mr Beggs believes that the information requested – CCTV footage and police investigations into an alternative line of inquiry - will assist him in establishing that there has been a miscarriage of justice. Police Scotland believes that the public interest lies in the information being withheld. The request was

refused by Police Scotland when it was first made in 2010. That refusal was upheld by the Scottish Information Commissioner and by the Court of Session. Since then Mr Beggs has made various applications to the Scottish Legal Aid Board for funding to pursue an appeal against this decision to the UK Supreme Court. This was unsuccessful so a fresh FOISA request was made.

This time round, Mr Beggs' challenge is on the basis that the Commissioner erred in that he did not acknowledge and then apply a presumption in favour of disclosure; he failed to engage with the specific circumstances of the request; and he did not provide adequate reasons for his decision.

Under FOISA, a person who requests information held by a Scottish public authority is generally entitled to it (section 1(1)). However, the Commissioner submitted that no starting presumption in favour of disclosure applies when an exemption is engaged; information shall be disclosed only where the public interest in disclosure is not outweighed by the public interest in maintaining the exemption. The weight is a matter for the Commissioner.

Further, the Commissioner submitted that there is no statutory duty on the Commissioner to provide reasons for the decision. Even if there is a right to intelligible reasons, which was denied, full reasons for the decision were provided. It was entirely clear why Police Scotland's refusal to comply with the request was upheld.

The court found that the Commissioner is a specialist tribunal. He made a decision which was reasonably open to him and the judges agreed that the appeal amounts to little more than a disagreement with the Commissioner's decision, rather than a challenge on the basis of an error of law. It is not the court's function to review its merits.

The appeal was refused.

Access the judgment: https://www.scotcourts.gov.uk/docs/default-source/cos-general-docs/pdf-docs-for-opinions/2023csih344489ba50-9403-4398-b30e-11e01a5b4789.pdf?sfvrsn=6d771c0f_1

Ministry of Defence fined for email data breach during Afghanistan evacuation

The Information Commissioner's Office (ICO) has fined the Ministry of Defence (MoD) £350,000 for disclosing personal information of people seeking relocation to the UK shortly after the Taliban took control of Afghanistan in 2021.

On 20 September 2021, the MoD sent an email to a distribution list of Afghan nationals eligible for evacuation using the 'To' field, with personal information relating to 245 people being inadvertently disclosed. The email addresses could be seen by all recipients, with 55 people having thumbnail pictures on their email profiles. Two people 'replied all' to the entire list of recipients, with one of them providing their location.

The original email was sent by the team in charge of the UK's Afghan Relocations and Assistance Policy (ARAP), which is responsible for assisting the relocation of Afghan citizens who worked for or with the UK government in Afghanistan. The data disclosed, should it have fallen into the hands of the Taliban, could have resulted in a threat to life.

Soon after the data breach, the MoD contacted the people affected asking them to delete the email, change their email address, and inform the ARAP team of their new contact details via a secure form. The MoD also conducted an internal investigation, made a statement in Parliament about the data breach, and updated the ARAP's email policies and processes, including implementing a 'second pair of eyes' policy for the ARAP team when sending emails to multiple external recipients. Such procedure provides a double check whereby an email instigated by one member of staff is cross checked by another.

In addition to the 20 September 2021 incident, the MoD's internal investigation found two other similar data breaches, including on 7 September 2021 involving 13 individual email addresses, and on 13 September 2021 involving 55 individual email addresses – both using the 'To' field. In some instances, the same email address was involved and so the total number of unique email addresses disclosed was 265.

This case shows that even the most experienced teams operating on issues of national security can make errors if appropriate procedures are not in place. The ARAP team did not have such measures in place at the time of the incident and was relying on 'blind carbon copy' (BCC), which carries a significant risk of human error.

ICO preliminary enforcement notice for use of AI

The ICO has announced a preliminary enforcement notice against Snap, the company behind Snapchat, for failing to assess the data protection risks posed by generative AI technology, particularly to children.

Earlier this year, Snap launched the 'My AI' feature for its UK Snapchat+ subscribers and then rolled out the feature to its wider Snapchat user base in the UK. The chatbot feature, powered by OpenAI's GPT technology, is the first example of generative AI embedded into a major messaging platform in the UK.

The ICO's investigation has provisionally found that the risk assessment Snap conducted before it launched 'My AI' did not adequately assess the data protection risks posed by the generative AI technology, particularly to children. The assessment of data protection risk is particularly important in this context which involves the use of innovative technology and the processing of personal data of 13 to 17 year old children.

The ICO's preliminary findings in the notice are provisional and Snap now has an opportunity to make representations before the ICO takes a final decision.

Information Commissioner seeks permission to appeal Clearview AI Inc ruling

The dispute between the UK Information Commissioner (ICO) and Clearview AI Inc continues as the ICO seeks permission to appeal the judgment of the First Tier Tribunal (Information Rights) (Tribunal) which concluded that the ICO did not have jurisdiction to impose a £7.5m fine on Clearview for failures in its data processing activities.

Clearview is a US based company which has collected billions of facial images from websites and social media, including images of UK citizens, to create a global online database. Clearview's customers can then upload an image of a person to be checked against all the images in the database for a match using facial recognition technology. The app provides a list of images that have similar characteristics with the photo provided by the customer, with a link to the websites from where those images came from. The question for the Tribunal was whether Clearview's activities are within the scope of UK GDPR.

The Tribunal was clear that even if a company is not established in the UK, it is still subject to UK data protection law if it is engaged in the monitoring of people living in the UK. As such, where Clearview provides its services commercially, it will be subject to the ICO's jurisdiction. Since 2020, however, Clearview's service is only available to law enforcement and national security services. It is no longer available to commercial clients.

The Tribunal found that Clearview's processing fell outside the reach of UK data protection law on the basis that it provides its services to foreign law enforcement agencies. The Tribunal held that the ICO did not have jurisdiction to issue its penalty notice because Clearview did not undertake relevant processing for the purposes of the UK GDPR.

The ICO disagrees with this view, arguing that, regardless of the end user, Clearview did not carry out the processing of data of UK citizens for foreign law enforcement purposes when it harvested the images and should not be shielded from the scope of UK law on the basis that the images are now used for a more restricted purpose than when they were originally collected. Clearview collected the personal data (facial images) without a lawful reason to do so, without making individuals aware of how their data would be used and with no process in place to stop the data being retained indefinitely.

The ICO awaits the outcome of its application for permission to appeal.

Equifax fined £11m for role in major cyber-security breach

The Financial Conduct Authority (FCA) has fined Equifax Ltd more than £11 million for failing to manage and monitor the security of UK consumer data it had outsourced to its parent company based in the US. The breach allowed hackers to access the personal data of millions of people and exposed UK consumers to the risk of financial crime.

In 2017, Equifax's parent company, Equifax Inc, was subject to one of the largest cybersecurity breaches in history. Cyber-hackers were able to access the personal data of approximately 13.8 million UK consumers because Equifax outsourced data to Equifax Inc's servers in the US for processing.

Equifax did not treat its relationship with its parent company as outsourcing. As a result, it failed to provide sufficient oversight of how data it was sending was properly managed and protected. There were known weaknesses in Equifax Inc's data security systems and Equifax failed to take appropriate action in response to protect UK customer data.

The breach was exacerbated by Equifax's conduct following the incident. Equifax made several public statements on the impact of the incident to UK consumers which gave an inaccurate impression of the number of consumers affected. Equifax also treated consumers unfairly by failing to maintain quality assurance checks for complaints following the cybersecurity incident, meaning complaints were mishandled.

This case is a reminder that the data controller, who determines the purposes and means of the processing of personal data, remains responsible for ensuring the security of that data even when it is being processed by a third party – be that an arms length organisation or a group company.

Access the Final Notice: https://www.fca.org.uk/publication/final-notices/equifax-limited-2023.pdf

---

Former NHS secretary found guilty of illegally accessing medical records

A former NHS employee has been found guilty and fined for illegally accessing the medical records of over 150 people.

The medical secretary worked within the Ophthalmology department of a hospital when a patient complaint prompted an investigation which revealed that the secretary had accessed this individual's records 33 times between March 2019 and June 2019, without consent or a business need to do so.

It further discovered that she had accessed a total of 156 patient records without consent or a business need, viewing them over 1800 times within the three-month period. This included the records of family members and individuals with postcodes local to where she lived at the time.

As part of her role as a medical secretary, the employee was required to access clinical and personal information of patients within the ophthalmology department. However, the individuals whose records were accessed had no medical conditions relating to ophthalmology. She pleaded guilty to unlawfully obtaining personal data in breach of Section 170 of the Data Protection Act 2018 and was ordered to pay a total of £648.

This case is a reminder that all staff should be aware of the limits of their right to access personal data held by the organisation. There may be significant consequences for the employee and to the organisation if they look at personal records without due cause, even if the records relate to an individual who is a friend or family member or is otherwise known to the employee. Data protection training, including refresher training, should always include this warning. Technical solutions can also be implemented to ensure that employees do not have access to personal data beyond that which is necessary to fulfil their duties.

Consultations

Scottish Information Commissioner's FOI Christmas wishlist

The Scottish Information Commissioner is inviting views on FOI by asking people to submit their "FOI wish list" for 2024.

Whether it be changes to the FOI Act itself or areas where the FOI Codes of Practice could be helpfully updated, the Commissioner would like to hear about it – no matter how big or small.

Access the survey: https://foiscotland.onlinesurveys.ac.uk/christmas-wish-list

---

Draft biometric data guidance

The ICO ran a consultation on the first phase of its draft biometrics guidance and the accompanying draft summary economic impact assessment between 18 August to 20 October 2023.

The draft guidance explains how data protection law applies when organisations use biometric data in biometric recognition systems. The guidance is aimed at organisations that use or are considering using biometric recognition systems as well as suppliers of these systems for example, facial recognition technology or fingerprint recognition entry systems. It is for both controllers and processors.

The second phase of this guidance (biometric classification and data protection) will include a call for evidence early next year.

ICO guidance on keeping employment records

The Information Commissioner's Office (ICO) is producing an online resource with topic-specific guidance on employment practices and data protection. Drafts of the different topic areas are being released in stages and a draft of the guidance on keeping employment records is now out for public consultation.

The draft guidance aims to provide practical guidance about how to comply with data protection law when keeping records about your workers and to promote good practice.

Deadline for responses: 5 March 2024

Access the consultation: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/keeping-employment-records-consultation/

ICO guidance on recruitment and selection

A draft of the ICO's guidance on recruitment and selection is also out for public consultation. The draft guidance aims to provide practical guidance about how to comply with data protection law when carrying out recruitment exercises and to promote good practice.

Deadline for responses: 5 March 2024

Access the consultation: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/recruitment-and-selection-consultation/

Other News

In this section we bring you commentary on any other data protection and information law developments or news items that may be of interest to you.

Calculating FOI request response times over Christmas and New year

As we approach the festive break, public authority staff and requesters are reminded that the following public holidays are counted as non-working days when calculating response times under FOI law:

- 25 and 26 December 2023 - Christmas Day and Boxing Day
- 1 and 2 January 2024 - New Year's Day and the day after

How data protection law can prevent harm in the housing sector

The ICO has published a blog about how data protection law can prevent harm in the housing sector.

Complaints received by the ICO suggest that there is a lack of understanding about data protection law by some organisations in the UK housing sector. Additionally, the recent report from the Housing Ombudsman Service (HOS) into Rochdale Boroughwide Housing identified record-keeping and data accuracy as key areas for improvement.

The blog is intended to be a reminder for housing organisations of their obligations under data protection law and an opportunity to bust some data sharing myths that might mistakenly prevent an organisation from safeguarding its residents.

Access the blog: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/12/how-data-protection-law-can-prevent-harm-in-the-housing-sector/

Data breaches can put domestic abuse victims' lives at risk

The ICO has reprimanded seven organisations in the past 14 months for data breaches affecting victims of domestic abuse. These include:

- Four cases of organisations revealing the safe addresses of the victims to their alleged abuser. In one case a family had to be immediately moved to emergency accommodation.
- Revealing identities of women seeking information about their partners to those partners.
- Disclosing the home address of two adopted children to their birth father, who was in prison on three counts of raping their mother.
- Sending an unredacted assessment report about children at risk of harm to their mother's ex-partners.

The organisations involved include a law firm, a housing association, an NHS trust, a government department, local councils and a police service. Root causes for the breaches vary, but common themes are a lack of staff training and failing to have robust procedures in place to handle personal information safely.

A further incident occurred in November when the ICO issued a reprimand to an English council after it disclosed the new address of a domestic abuse victim to her ex-partner. The ICO's recommendations to reduce the risk of such incidents includes:

- Put alerts on files if staff need to be especially vigilant when someone is a vulnerable service user
- Ensure a proper process is in place for address changes
- Carry out data protection training, including refresher training.

ICO guidance on issuing spreadsheets in FOI responses

The UK Information Commissioner's Office (ICO) recently issued an advisory note calling for an end to the publication of excel spreadsheets on online platforms when responding to FOI requests.

This follows a number of recent breaches where personal information was inadvertently included in spreadsheets which were shared as part of an FOI response. The ICO is currently preparing further regional guidance on this matter, which will set out the jurisdictional boundaries in relation to FOI enforcement.

ICO guidance on monitoring workers

With the rise of remote working and developments in the technology available, some employers are looking to carry out checks on workers.

In response to this trend, the Information Commissioner's Office has published guidance to help employers fully comply with data protection law if they wish to monitor their workers.

The guidance provides an overview of how data protection law applies to the processing of personal data for monitoring workers. It is aimed at employers across both the public and private sector and provides clear direction on how monitoring can be conducted lawfully and fairly. The guidance also considers specific types of monitoring practices, including the use of biometric data to monitor timekeeping and attendance.

Updates from the Digital Directorate - the potential of open data

Scotland's Open Government Action Plan 2021-25 includes a digital and data commitment to 'support government openness, transparency and empowerment through open data'. The Digital Directorate's Data Division (quite the tongue twister!) has been working on this and produce regular blogs with updates on how the project is going.

Progress with the commitment so far includes:

- a data discovery tool that is making it easier to find and access public data. Currently available as a beta version, it discovers datasets other search engines cannot reach.
- two cohorts of public sector organisations have completed the data maturity programme. A third cohort started in Autumn 2023 and there is a trial of a self-serve modular approach.
- a thriving public sector community of practice for data standards and open data with over 200 members who meet for regular drop-in sessions on topics such as data quality, metadata and version control.
- changes to Scotland's official statistics open data publishing platform informed by user research to simplify navigation.
- identifying data relevant to other open government themes that could be published openly and supporting that process.
- the Scottish AI Register which provides information on artificial intelligence being used or developed in the Scottish public sector. It gives members of the public a way to engage and have their say to help ensure trustworthy, ethical and inclusive AI.

ICO focus on website cookies

The Information Commissioner has warned some of the UK's top websites that they face enforcement action if they do not make changes to comply with data protection law.

The ICO has previously issued clear guidance that organisations must make it as easy for users to "Reject All" advertising cookies as it is to "Accept All". Websites can still display adverts when users reject all tracking, but must not tailor these to the person browsing.

Although many of the biggest websites have got this right, the ICO is giving companies who haven't managed that yet a clear choice: make the changes now, or face the consequences. The ICO will publish an update in January, including details of the companies that have not addressed their concerns.

This is a reminder to ensure that appropriate cookies are running on your website and that there is a clear option to reject all tracking cookies.

Update on Scottish Government's FOI performance

The Scottish Information Commissioner has published a progress report as part of the ongoing intervention to improve the Scottish Government's performance when responding to freedom of information (FOI) requests.

Despite the intervention having started six years ago, the commissioner remains of the view that the Scottish Government's improvement activity has not yet reached the point where this work can be appropriately concluded.

The 2023 Progress Report is very much a report of two halves: first, progress and performance during Phase 1 between 1 July 2022 to 31 March 2023 raised significant concerns on a wide range of issues. These included: a deterioration in on-time FOI performance levels; an increased average response time for FOI requests and reviews (particularly where the case was marked 'sensitive'); a failure to urgently progress a significant number of 'late' cases, resulting in a backlog of historic late requests; significant variance in the FOI knowledge of case-handlers, reviewers and approvers; and widespread failure to comply with internal records management requirements leading, in some instances, to ambiguity surrounding the role of Special Advisors in the decision-making process.

However, the report then records evidence of improvements in the period between May and September 2023, following the implementation of measures to address the commissioner's concerns.
The report concludes that more work is to be done if performance is to be sustained and further improved but the commissioner is "cautiously optimistic" that this can be achieved, allowing his successor to finally bring the intervention to an end.

Access the report: https://www.itspublicknowledge.info/sites/default/files/2023-10/2023%20Scottish%20Government%20Intervention%20Report.pdf

About us

Harper Macleod is a leading independent Scottish law firm that is driven to deliver.

Our growth and success is determined by your success, which is why we always try harder. We don't just see ourselves as lawyers, we see ourselves as problem solvers and business advisers, who focus on understanding your needs. We work side by side with you, using law as a tool to provide innovative solutions that are tailored to organisations and individuals.

It's this drive that sets us apart and delivers a better outcome for you or your organisation.

harpermacleod.co.uk info@harpermacleod.co.uk @HarperMacleod