Data Protection and Freedom of Information Legal Update

June 2024

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.

The Data Protection and Digital Information (No. 2) Bill will not progress

The forthcoming UK general election on 4 July 2024 means that the Data Protection and Digital Information (No. 2) Bill will make no further progress.

The UK Parliament sat for only two more days after the election announcement, known as 'wash-up'. The 'wash-up' period is a chance to finish off any urgent parliamentary business and an opportunity to push forward any final legislation. Any unfinished business is lost at dissolution.

The Data Protection and Digital Information Bill, which was intended to create a new data protection regime for the UK as described in previous updates, was not passed before Parliament was dissolved and therefore falls. This means that UK data protection continues to be regulated by the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

It is unlikely that an overhaul of the data protection regulation regime will be a pressing issue for the new UK government. The Labour Party's 2024 manifesto does not include a strong focus on data. There is no mention of data protection in the Conservative manifesto.

Freedom of Information Reform in Scotland

Speaking at a freedom of information conference on 28 May 2024, Katy Clark MSP gave an update on her Private Member's Bill to reform FOI in Scotland. Ms Clark confirmed that the text of the draft Freedom of Information Reform (Scotland) Bill is in the final stages of preparation, and will be published in the coming months.

Scottish Government use of section 5 powers under FOISA

The Freedom of Information (Scotland) Act 2002 (FOISA) requires that the Scottish Ministers report to Parliament every two years on the use of their powers to designate new bodies under section 5.

These powers have previously been used to extend FOISA to:

- arms-length external organisations set up by local authorities to deliver recreational, sporting, cultural or social facilities and activities (2013 Order)
- grant-aided schools and independent special schools (2016 Order)
- providers of secure accommodation (2016 Order)
- Scottish Health Innovations Limited (2016 Order)
- private prison contractors (2016 Order)
- registered social landlords and their subsidiaries (2019 Order)

The most recent report confirms that no orders had been made under section 5 during the two-year reporting period, but that the Scottish Government has nevertheless acted to extend coverage of FOISA in significant ways. Both ScotRail Trains and Caledonian Sleeper were brought within the scope of FOISA during the reporting period (through becoming wholly owned by a public body).

The Scottish Government is also proposing to extend access to information rights in relation to legal services regulation in the Regulation of Legal Services (Scotland) Bill, currently before the Scottish Parliament. The Bill proposes to make legal services regulators designated as 'category 1' by that Bill subject to FOISA in relation to regulatory functions, including the Law Society of Scotland.

Case law update

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.

Housing association reprimanded for portal which exposed personal information

A Scottish Housing Association set up a new residents' information portal in 2022 to improve communication and access to information for tenants. However, an error meant that residents could access documents related to anti-social behaviour cases, and view personal information about other residents, including names, addresses and dates of birth.

The organisation had failed to test the portal before it went live and their staff were not clear on how to escalate the issue when they became aware of the problem. This led to data remaining viewable on the portal for a further five days before the Housing Association suspended the portal.

The ICO reprimand noted that all organisations require to have appropriate security measures in place when launching new products and must have tested them thoroughly with data protection in mind, as well as ensuring staff are appropriately trained and know how to respond to a data breach.

Access the reprimand: https://ico.org.uk/action-weve-taken/enforcement/clyde-valley-housing-association/

Patient data compromised in NHS Dumfries and Galloway cyber attack

A cyber-attack on NHS Dumfries and Galloway has resulted in over 3 terabytes of patient and staff data being published by a group calling itself INC Ransom after the health authority refused to meet the group's demands.

The cyber criminals did not access the primary records system for patients' health information which contains people's entire medical history in one location. Instead, the ransomware group accessed millions of very small, separate pieces of data such as individual letters from consultants to patients, letters between consultants, test results, x-rays, etc.

NHS Dumfries and Galloway has warned that, now the stolen data has been made public on the internet by the cyber criminals, there is a risk of it being further accessed, duplicated or shared on the internet, and not just on the dark web.

The health authority is now working alongside national agencies like Police Scotland, The National Crime Agency, The National Cyber Security Centre and the Scottish Government – taking their advice and direction.

On the advice of Police Scotland, no details have been made available about how the data breach occurred, so the general advice is to remain vigilant and ensure that your organisation has carried out sufficient cyber security audits to identify any potential weaknesses in your data storage systems.

To help with this, the Information Commissioner's Office published a new report - Learning from the mistakes of others – last month which focuses on five leading causes of cyber security breaches:

- Phishing – where scam messages trick the user and persuade people to share passwords or accidentally download malware.
- Brute force attacks - where criminals use trial and error to guess username and password combinations, or encryption keys.
- Denial of service – where criminals aim to stop the normal functioning of a website or computer network by overloading it.

- Errors – where security settings are misconfigured, including being poorly implemented, not maintained and or left on default settings.
- Supply chain attacks - where products, services, or technology you use are compromised and then used to infiltrate your own systems.

Ruling on Experian enforcement notice considers GDPR transparency principle

Experian is a well-known credit reference agency which holds and processes data relating to over 51 million people living in the UK. It acquires data from a variety of sources, including from publicly available resources such as the Open Electoral Register. As part of its operations, Experian processes the personal data of UK residents using data analytics tools to apply probable demographic and lifestyle attributes to the individuals. It uses the output of this processing to produce marketing datasets which are sold to third-party clients.

The Information Commissioner, who had concerns about the nature and extent of Experian's data processing in the light of the transparency requirements of the UK GDPR, issued Experian with an enforcement notice imposing a series of requirements, including a clear and prominent privacy notice. Experian appealed to the First-tier Tribunal ("FTT"), opposing the lengthy list of requirements imposed by the enforcement notice. The FTT largely allowed Experian's appeal and issued a substituted and scaled down enforcement notice. The Information Commissioner then appealed to the Upper Tribunal, seeking to have the original enforcement notice reinstated.

The appeal was primarily concerned with the principle of transparency, both the overarching duty in Article 5(1)(a) and the more detailed obligations in Article 14 GDPR.

The Information Commissioner raised five grounds of appeal, alleging that the FTT's decision involved multiple errors of law and that it failed to adequately address a number of relevant issues. In particular, that the FTT had failed adequately to apply a legally accurate interpretation of the transparency principle, under Article 5(1)(a) and Article 14 GDPR, to the issues of fact and law.

The Upper Tribunal rejected each of the ICO's five grounds of appeal. It found that, although the FTT's decision was neither well-structured nor particularly well-reasoned, there was no error of law in the FTT's approach to the transparency principle. In fact, to a significant degree, the ICO's appeal points were an attempt to take issue with the FTT's evaluative assessments and to re-argue a case that had been unsuccessful.

The Upper Tribunal agreed with the FTT's finding that transparency is central to the GDPR but found that the conditions of the ICO's enforcement notice went beyond what was necessary for Experian to satisfy the transparency principle. The ICO has confirmed that it will not be appealing the judgment.

This case suggests that there are some limitations on the transparency principle and that, in the detailed and onerous enforcement notice in this case, the ICO went too far.

Access the Upper Tribunal decision: https://www.judiciary.uk/wp-content/uploads/2024/04/Information-Commissioner-v-Experian-Judgement-1.pdf

---

Staff at private hospital investigated for trying to access royal records

It has been reported that the ICO is investigating a potential data breach by staff at The London Clinic where Kate Middleton underwent abdominal surgery earlier this year.

As well as investigating the individual employees who are suspected of unauthorised access to health records, the ICO is also investigating the clinic itself for a failure to timeously report the breach. Official guidance from the ICO is that personal data breaches must be reported to it by organisations

within 72 hours from the time of discovery, if there is a" high risk" that it will have a "significant detrimental effect" on individuals' rights and freedoms.

This case is a reminder of the requirement to ensure that staff are properly trained and fully understand their data protections duties and obligations, but also of the potentially serious consequences for an organisation for failure to report breaches to the ICO promptly.

Car rental manager fined after unlawfully obtaining customer data

In a similar case of unauthorised data access, a former management trainee at Enterprise Rent-A-Car has been ordered to pay a fine after admitting he illegally obtained customer data.

The employee had attended his workplace outside of his scheduled hours and accessed 213 client records, including customer data from different rental branches, without any business need to do so. Enterprise Rent-A-Car conducted an internal investigation and dismissed the employee for gross misconduct. They also referred the case to the Information Commissioner's Office, who launched a criminal investigation.

No evidence was found to show that the employee had sold the data or made any financial gain, so the only charge was for unlawfully obtaining the data contrary to section 170 of the Data Protection Act 2018.

This case is a reminder about the risk of employees having access to potentially valuable customer data. Enterprise could have had improved limits on the data that employees can access, for example, having a system in place to ensure employees cannot access data from other branches. In this case the ICO commended Enterprise for having an internal audit system in place which could be relied upon to show the extent of the unauthorised activity.

FOI and data protection: Employment contract of named individual

An applicant asked East Lothian Council for a named individual's employment contract. The authority refused to disclose the requested information, as it was third party personal data. The Scottish Information Commissioner investigated and agreed that the employment contract was exempt from disclosure under section 38(1)(b) of FOISA.

The relevant test to apply in these circumstances was: (a) does the applicant have a legitimate interest in the personal data? (b) if so, would the disclosure of the personal data be necessary to achieve that legitimate interest? (c) even if the processing would be necessary to achieve the legitimate interest, would that be overridden by the interests or fundamental rights and freedoms of the data subjects which require protection of personal data (in particular where the data subject is a child)?

In this case, the applicant was found to have a legitimate interest in the data requested because they intended to use the information in a court process. However, the application was made six years after the events in question and the Commissioner was not convinced that disclosure of the information requested was "necessary" to achieve the applicant's legitimate interest.

The term "necessary" here is interpreted as meaning "reasonably", rather than absolutely or strictly, necessary and the Commissioner had to consider whether the disclosure is proportionate and fairly balanced as to the aims to be achieved, or whether the applicant's legitimate interests can be met by means which interfere less with the privacy of the data subject.

In this case, disclosure of the personal information contained within the employment contract would not comply with the principles in Article 5 of the UK GDPR. The contract was therefore exempt from disclosure under section 38(1)(b) of FOISA.

Access the decision notice: https://www.foi.scot/sites/default/files/2024-04/Decision037-2024.pdf

FOI in an employee misconduct investigation

In this FOI case the authority was asked for information relating to a named employee being suspended over claims of misogyny and bullying. The authority applied section 38(1)(b) (the exemption for personal information) and refused to confirm nor deny whether the requested information existed or was held.

The Commissioner investigated and found that the authority was entitled to refuse to confirm nor deny whether it held the information.

Section 18 of FOISA provides that an authority may respond to a request by neither confirming nor denying that the information is held in circumstances when it would be contrary to the public interest to reveal whether the information exists or is held.

In this case, the Commissioner concluded that the applicant did have a legitimate interest in the information sought. The Commissioner also held that disclosure of the information (if existing and held) would be necessary to achieve the applicant's legitimate interests. However, this must be balanced against the fundamental rights and freedoms of the named individual. Only if the legitimate interests of the applicant outweighed those of the data subject could personal data be disclosed without breaching the first data protection principle.

In the case of a misconduct investigation, the Commissioner agreed with the authority that the information (if it existed and was held) would be information a person would generally expect to be kept confidential and only shared amongst limited individuals for specific purposes. Considering the potential harm or distress that could be caused by disclosure of the information, the legitimate interests served by disclosure would be outweighed by the unwarranted prejudice that would result to the rights and freedoms or legitimate interests of the individual data subject in question in this case.

The authority was justified in responding on a neither confirm nor deny basis in these circumstances.

Access the decision notice: https://www.foi.scot/sites/default/files/2024-05/Decision%20055-2024.pdf

---

Information that would harm the effective conduct of public affairs

Section 30(c) of Scotland's FOI Act allows public bodies to withhold information where disclosure would (or would be likely to) substantially harm the effective conduct of public affairs. When applying this exemption, authorities must show what specific harm would be likely to be caused by disclosure of the information, and how that harm would be expected to follow from disclosure. Where this cannot be clearly demonstrated, the exemption is unlikely to apply.

In one of a series of requests relating to Lochaber Smelter, the requester asked the Scottish Ministers for information on total fee payments and the dates of payments made. Following consideration of the detail of the case, the Commissioner accepted that disclosure of the total fee paid would (or would be likely to) substantially harm the effective conduct of public affairs. The Commissioner did however require the Scottish Ministers to confirm the dates that payments have been made.

The Commissioner was not satisfied that disclosure of the dates of those payments – without knowing the actual value of the fee payments – would result in harm. This case shows that it is important to consider the different aspects of a request and not simply apply the same blanket response to the whole request where it can be separated into parts to which the relevant considerations may apply differently.

Access the decision notice: https://www.foi.scot/decision-1122023

The importance of recording details of request-handling process

The Scottish Information Commissioner has advised that authorities must ensure they keep a record of key actions and decisions when responding to requests under the FOI Act and the Environmental Information (Scotland) Regulations 2004 (the EIRs).

If an authority wants to issue a fees notice under the EIRs, for example, it must be able to demonstrate that the fee charged is reasonable and should keep an accurate note of the calculations made.

In decision 051/2024, the Commissioner considered a case where a requester had asked for information about a Council's decision to reduce the speed limits on two local roads. The Council told the requester that the information was environmental information, so it had to be processed under the EIRs. It went on to issue a fees notice under the EIRs for £208.

When the Commissioner investigated the case, he found that the Council had not kept a copy of their original calculations, and the member of staff who had carried them out had left. The Council was asked to carry out new calculations which arrived at a substantially different cost - £2,145 as compared with the original fee of £208.

On examination of the basis for this charge, it was found that the searches on which the costs were based were inaccurate, in that they were both too broad, and covered too wide a time limit. After carrying out a new, more focused and targeted search, the Council found only two relevant documents, both of which were subsequently disclosed to the requester.

Consultations

FOI/EIR section 60 Code of Practice

Following its 2023 consultation on FOI in Scotland, the Scottish Government has committed to reviewing and refreshing key elements of the FOI/EIR section 60 Code of Practice, which provides guidance for public authorities on meeting their duties under FOI law.

As part of this review, the Scottish Information Commissioner will be sharing his thoughts on the areas where this important guidance could be refreshed and updated.

At this stage, the Scottish Information Commissioner is inviting submissions on areas that stakeholders would like to see updated in this guidance. Whether that is greater clarity around a particular issue, more advice on an existing topic, or something new altogether, you are invited to contact the Scottish Information Commissioner to submit your ideas.

ICO consultation series on generative AI models

The Information Commissioner's Office (ICO) has launched further consultations in its series examining how data protection law applies to the development and use of generative AI.

The third chapter in the series focused on how data protection's accuracy principle applies to the outputs of generative AI models, and the impact that accurate training data has on the output.

The fourth call for views (which closed on 10 June) sought evidence on individual rights, the information rights data protection confers to people over their personal information and, in particular, in relation to the training and fine-tuning of generative AI. Views on what further measures generative AI developers should take to safeguard individuals' rights and freedoms were also sought.

Access the consultation series: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-series-on-generative-ai-and-data-protection/

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.

Public awareness of FOI in Scotland

New research by the Scottish Information Commissioner found that there is strong public support for FOI key principles of openness, transparency and accountability.

The research, which surveyed 1,279 people in March 2024, found that:

- 88% of respondents had heard of the Scotland's FOI Act
- 97% felt it was important for the public to be able to access information held by public bodies
- Only 6% of respondents felt that FOI was a waste of public money (the lowest proportion since this question was first asked in 2011).

The research also found that the public attach significant value to the proactive publication of information by public bodies. For example:

- 93% agreed it was important for public bodies to publish as much information as possible about their work
- 68% reported that finding information on a public body's website was their preferred way to access information (only 12% of respondents said that sending a request would be their first preference)
- 90% said they would be more likely to trust an organisation that publishes a lot of information about its work.

The public also favoured the reform of FOI law in certain key areas. For example:

- 93% felt that FOI should be extended to cover publicly-funded health and social care services (such as care homes)
- 89% felt that all organisations that provide public services under contract to a public body should fall within scope
- 79% felt that it should be a criminal offence for public bodies or their officials to try to subvert FOI law.

The findings of this research underline the importance of FOI in building trust in an organisation and also tend to support the principles of FOI reform that are currently under consideration.

Information Commissioner calls for senior leaders to take transparency seriously

In an open letter to leaders of public organisations, the Information Commissioner has issued a reminder of the importance of transparency in the FOI regime.

The letter sets out simple steps organisations can take to stay on top of their obligations:

- Know what you need to publish and make as much information publicly available as possible.
- Look at what people are asking you about and actively publish it.
- Implement simple policies that show staff how to manage information requests effectively.
- Share the ICO's 'FOI in 90 seconds' guide and response templates with your staff.
- Provide mandatory FOI training for all staff, review it regularly and offer refresher training.
- Invest in tools and systems to manage and respond to information requests.

- Monitor performance to ensure your organisation is complying with its legal duties using the ICO's template action plan and self-assessment toolkits.

The Information Commissioner argues that being proactive will reduce the administrative burden on services and provide reassurance to service users.

Data strategy for health and social care: update 2024

Scotland's first Data Strategy for Health and Social Care, published in February 2023, set out the importance of making effective use of data to improve the delivery of care and outcomes for the people of Scotland.

The Strategy's vision is to make best use of data in the design and delivery of services. The strategy is underpinned by three core ambitions: giving individuals clear and easy access to their own health and social care data; empowering those delivering health and social care services to use and share data to improve services; to use data safely and appropriately for planning, research and innovation.

A full update sets out the progress made in the first year. The report confirms that important foundational steps have been taken. For example, work is continuing on the development of an Integrated Social Care and Health Record so people don't have to repeat their stories; a prototype of the Digital Front Door to allow people to digitally interact with their health and social care data is expected to be ready to test in 2024-25, to be made available to the public by the end of 2025; the process for researchers and innovators to access data has been improved through the recently launched Researcher Access Service.

Access the executive summary: https://www.gov.scot/publications/data-strategy-update-health-social-care-executive-summary/pages/1/

ICO guidance to improve transparency in health and social care

On a related note, the Information Commissioner's Office (ICO) has published new guidance - Transparency in health and social care - to support health and social care organisations to ensure they are being transparent with people about how their personal information is being used.

The guidance is targeted to organisations (including private and third sector organisations) who deliver health and social care services or process health and social care information, including for secondary purposes. It is designed to help organisations to understand the definition of transparency and assess appropriate levels of transparency, as well as providing practical steps to developing effective transparency information.

Access the guidance: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/transparency-in-health-and-social-care/

ICO update on artificial intelligence and data protection law

Understandably, AI is a priority for the ICO. An example of the ICO's proactive approach is the investigation into 'My AI' following concerns that Snapchat's parent company, Snap, had not met its legal obligation to adequately assess the data protection risks posed by the new chatbot.

Snapchat launched 'My AI' for its premium subscribers in February 2023 and made it available to all in April 2023. The ICO launched an investigation shortly afterwards and issued a Preliminary Enforcement Notice in October 2023.

The investigation resulted in Snap taking significant steps to carry out a more thorough review of the risks posed by 'My AI' and demonstrate that it had implemented appropriate mitigations. Following a

review, the ICO is now satisfied that Snap's risk assessment is compliant with data protection law. The ICO will continue to monitor the rollout of 'My AI' and how emerging risks are addressed by Snap.

Existing guidance on AI explains how to apply the concepts of data protection law when developing or deploying AI and an AI toolkit has been developed to help organisations identify and mitigate risks during the AI lifecycle.

The ICO guidance on AI applies equally to generative AI which is rapidly becoming embedded in many services that we use, such as Microsoft Co-pilot, online chatbots and search engines.

In April 2023, the ICO set out eight questions organisations developing or using generative AI that process personal data need to be asking themselves. In June 2023, they launched an Innovation Advice service which provides answers to AI innovators' queries within 10-15 working days.

Read more about the ICO's work on AI.

Scottish AI Register

Every public sector project using AI in Scotland is to be logged on the Scottish AI Register. This is a publicly accessible database providing a range of information about the use of the technology in projects either in use or being developed by public bodies.

The Register is currently voluntary, with public bodies encouraged to submit information, but mandatory registration will begin with Scottish Government departments as part of a phased approach across the wider public sector.

It is hoped that the register will not only give the public increased confidence that AI is being used openly and transparently but will also act as a source of best practice, helping ensure AI is used in ways which is both economically and technically viable and makes a positive impact across society.

Access the register: https://scottishairegister.com/

New web address for Scottish Information Commissioner

The Scottish Information Commissioner's website has moved to www.foi.scot/

The old address - itspublicknowledge.info - will automatically re-direct readers to the new foi.scot space.

The Scottish Information Commissioner is making some changes to the FOI statistics portal. The new interactive version will present the quarterly FOI data collected from public authorities in a more visual, user-friendly and accessible way.

Otherwise, there is no change to the services available online so, whatever you want to know about freedom of information in Scotland, this is still the first port of call.

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