HOUSING
BCM lessons learned
Damp & mould

DATA PROTECTION
The new DP regime
HE breaches

TECH TALK
Lithium-ion battery
fire risk

RISK MANAGEMENT
EDI risk framework
Policing e-scooters

stronger

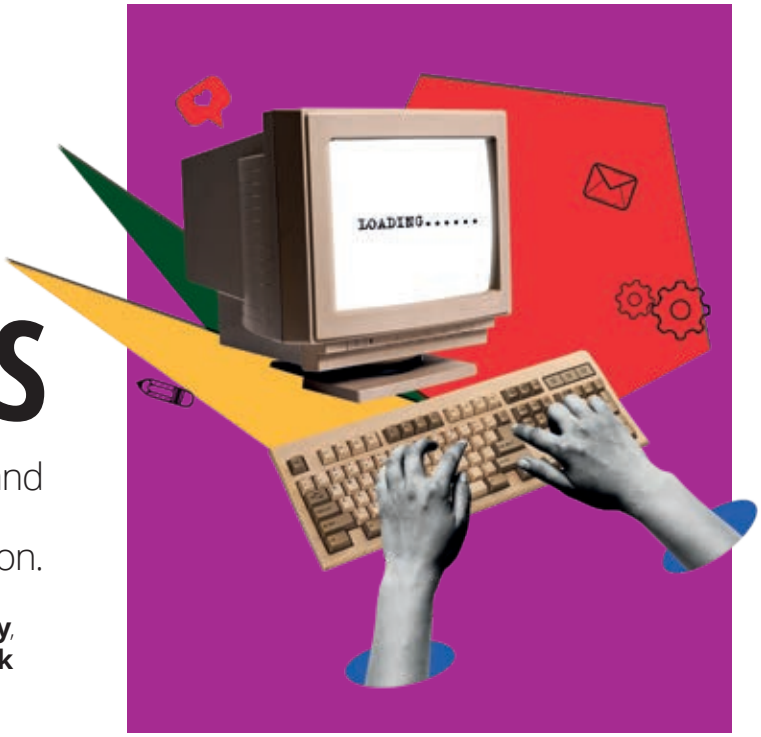
THE ALARM JOURNAL

July
2023

SUSTAINABLE SOLUTIONS

Tackling air pollution
Nurturing nature
Managing food security
Engaging with ESG

Data protection REGIME CHANGES



Organisations should understand and prepare for a new data protection regime on the horizon.

AUTHORS: **Lesley Allan**, **Richard Beaty**, **George Chaisty**, **Weronika Dorociak** and **Edward Le Gassick**, Kennedys

After almost eight months of political wrangling, a revised draft of the *Data Protection and Digital Information (No. 2) Bill*[1] (the *Bill*) was re-introduced to Parliament on 8 March 2023.

The *Bill* will reform the existing data protection regime following Brexit, namely the *UK General Data Protection Regulation* (*UK GDPR*) and the *Data Protection Act 2018* (*DPA*). The *Bill* is not expected to receive Royal Assent until 2024 and the implementation process will take some time. The *Bill's* main aims are to simplify data protection rules for businesses and organisations and ensure that data can be used to empower citizens.

Data protection is of key importance to public service organisations. The essential services they provide give them access to and require them to process the most sensitive data. Those engaging with services need to be confident their data is safe and will be used appropriately.

The reputational risk to an organisation from any data breach is significant. Leaving aside negative press coverage, if those relying on services do not feel safe and confident sharing detailed information, it can adversely affect the ability of an organisation to provide suitable, necessary and timely services.

What is changing?

Record keeping and high risk processing

One of the biggest changes proposed by the *Bill* concerns record keeping. If adopted, organisations will only be required to keep records of processing if there is a high risk to the rights and freedoms of individuals. They will also have to conduct less extensive impact assessments and only consult the Information Commissioner (IC) prior to processing high risk data if deemed necessary.

The May 2023 draft of the *Bill* outlines what data controllers and processors should consider when deciding whether the data they are dealing with is high risk. This includes the nature, scope, context and purposes of processing, possible risks for the rights and freedoms of individuals arising from processing, and the available resources. However, the Bill does not provide specific examples of high-risk processing. The IC will be expected to clarify this aspect of the legislation further down the line. Examples of processing that might result in a high risk are unlikely to differ from those outlined in the European Commission's current *Guidelines on Data Protection Impact Assessment*[2].

One of the biggest changes proposed by the *Bill* concerns record keeping.

In terms of maintaining 'appropriate records' (high risk data records), the *Bill* provides minimum information that controllers and processors should keep on file. It also states that, where possible, records should include information about how data is stored and kept secure.

Senior responsible officers (SRIs) have to be members of an organisation's senior management, with appropriate knowledge and skills.

Although the provisions included in the *Bill* may simplify some data-related processes, a significant proportion of data that councils access will still fall into the high risk category. For example, they have responsibilities for child and adult support and protection. They are also required to hold and process data to permit them to tailor education, care and social work support services to the needs of the most vulnerable in society.

Senior Responsible Individuals (SRIs)

If the *Bill* is enacted, public bodies and organisations that process high risk data will be required to designate a senior responsible individual SRI. They will be responsible for data protection risks and will effectively replace Data Protection Officers (DPOs).

SRIs have to be members of an organisation's senior management, with appropriate knowledge and skills, and their contact details will be publicly available and shared with the IC. The *Bill* outlines the exact tasks that SRIs would be required to perform for data controllers and processors. Within a council, these will include monitoring compliance, organising training for employees, dealing with data breaches and complaints, advising the controller as well as acting as the first point of contact for the IC.

The legislation will introduce provisions to the *DPA* outlining the tasks of a SRI, which for a council would include informing and advising the data processors engaged by the council. Councils were obliged to appoint a DPO under the current law. This is a challenging and substantial role, and it is hoped that councils will similarly be able to identify candidates for the SRI role.

Subject access requests (SARs)

Under the current regime, an organisation is obliged to share data it holds about an individual if they request a copy of the records, unless the request is 'manifestly unfounded or excessive'. The proposed legislation would make it easier for organisations to refuse to respond to SARs, as well as enable them to charge a reasonable fee in instances where a request is 'vexatious or excessive'. Examples include requests intended to cause distress, those not made in good faith or those that are an abuse of process. Councils will be familiar with the concept of vexatious requests as the language is taken from *Section 14* of the *Freedom of Information Act 2000*.

Although the *Bill* recommends organisations should consider certain factors when determining whether a request falls under the category of vexatious or excessive, it states that it does not have to satisfy all factors for the provision to apply. However, an organisation will have to prove it has refused a SAR on reasonable grounds if questioned by the subject or the IC.

The *Bill* also proposes to amend the time limits for responding to SARs. Organisations will have to respond to SARs during the 'applicable time period' that will depend on the context and circumstances of the request. In some instances, the applicable time period will commence when the request is received. However, if an organisation decides to charge the data subject for the request, it will be counted from the moment the fee is paid.

Data controllers will still be able to extend the standard one-month response period by two months if the request is a complex one or if they received many requests in relation to the data subject. Any delay will have to be communicated and explained to the data subject within one month, beginning with the relevant time.

Furthermore, an organisation will also be able to pause the response time if it requires more information from the data subject in order to proceed with their request.

These are provisions which will provide some comfort to councils, where the burden of SARs and Freedom of Information requests is considerable. Councils will want to ensure wide awareness of these changes if enacted, and consider how best to co-ordinate information about requests, to identify those where new provisions could be invoked.

Surveillance

The *Bill* proposes to simplify the oversight framework for the use of surveillance cameras by abolishing the Biometrics and Surveillance Camera Commissioner, as well as the *Surveillance Camera Code*. Currently, overt surveillance (for example, CCTV) is governed by both the Biometrics and Surveillance Camera Commissioner and the IC. The new regime would remove this duplication and make it easier for councils to understand what is required of them when they are investigating offences and how they can comply with any surveillance-related rules.

This is going to be of particular interest and relevance to those organisations seeking to manage anti-social behaviour, including in tenanted properties, and to councils and police forces using cameras to monitor compliance with traffic measures such as cycle and bus lanes. Where community safety work leads to close co-operation with police, the clarification of what is required by councils is likely to be welcome.

Enforcement

The *Bill* proposes the replacement of the office of the Information Commissioner (ICO) with a new board of directors, comprised of a chair, chief executive and board members, with the current functions of the Information Commissioner (IC) being discharged by the board of the new body, the Information Commission, rather than being vested in and formally discharged by the IC, as present.

The *Bill* proposes significant extensions to the powers of the IC, particularly in relation to its enforcement powers and reporting requirements. Proposed new powers would enable the IC to issue 'interview notices'. These require a relevant individual (an SRI) within an organisation to attend an interview and answer questions concerning suspected data breaches. An interview has to be held within 24 hours of the notice, but interview notices can be appealed.

If an organisation fails to comply with an interview notice, the IC will be able to charge the higher maximum amount. That's up to £17.5 million for councils, in line with fines currently available for breach of an assessment notice. In reality the ICO presently reserves large fines for publicly funded bodies to the most 'egregious' cases, choosing instead to use other powers, for example, a reprimand or an enforcement notice. This is part of a two-year trial, until June 2024, culminating in a review of work to raise data standards in the public sector. We would expect this approach to extend to failure to comply with an interview notice at least during that trial period, and hopefully beyond.

The *Bill* proposes to simplify the oversight framework for the use of surveillance cameras by abolishing the Biometrics and Surveillance Camera Commissioner, as well as the *Surveillance Camera Code*.

These changes need to be considered within the context of the IC's new strategic approach to regulatory action piloted since last November, where the IC indicated that public reprimands rather than monetary penalties would be the likeliest regulatory action for public bodies all but the most egregious infringements.

How can councils prepare for the new data regime?

The *Bill* is not expected to receive Royal Assent until 2024 and the implementation process will take a considerable time. However, organisations should not put this on the back burner.

Although the *Bill* is not expected to receive Royal Assent until 2024, organisations should not put this new regime on the back burner.

Organisations should start preparing for the upcoming changes as early as possible. There can be public relations implications of even the enforcement that stops short of a financial penalty, as all enforcement is reported on the IC's website. However, councils for instance, do maintain high standards in this area: of the 76 reported episodes of enforcement in the last year, only six related to council practice.

Public service organisations are accustomed to data protection management. They are required to achieve compliance with statutory public records management obligations and freedom of information obligations, in addition to data protection obligations. A great deal of time and effort has been expended on developing a culture of commitment to good data management standards.

Improvements can always be made, and the new regime provides an opportunity to review all related processes. A sound data audit, knowledge of what data is held, where it is held and how it is used will be key to preparing for this new regime, as it was in preparing for the arrival of *GDPR*. It will also be useful to reach an early view on who within the organisation will need to know about these changes, and to prepare stakeholder education and training on the legislative changes and on what differences to existing policy and practice are required.

It will be important to collate all existing policy on data management issues and to review those areas where change is needed to reflect the changes the *Bill* aims to make. It is also worthwhile being aware of anything your organisation's website has to say about your approach to data protection. For example, is your privacy policy up to date? Will your website and hard copy publications need to be revised to reflect these changes?

Under the current regime, it is already necessary for organisations to act in a prompt and ordered manner in an event of a data breach and/or cyber attack. The proposals included in the *Bill* compound the importance of contingency plans and being able to draw on third-party, partner and supplier expertise, including reliable and nuanced legal advice, swiftly.

References

[1]*The Data Protection and Digital Information (No. 2) Bill 2022-23*, UK Parliament
[2]*Guidelines on Data Protection Impact Assessment,* European Commission

Lesley Allan (lesley.allan@kennedyslaw.com) is a Partner in Kennedys' Celtic Team specialising in defending employers' liability, public liability and historic childhood abuse claims for public and third sector organisations across Scotland.

Richard Beaty (richard.beaty@kennedyslaw.com) is a Consultant Barrister at Kennedys who specialises in data protection law.

George Chaisty (george.chaisty@kennedyslaw.com) is a Partner in Kennedys' Global Cyber and Data Risks Team, specialising in cyber incident response and advising clients in the immediate aftermath of ransomware attacks, business email compromises and other cyber attacks.

Weronika Dorociak (weronika.dorociak@kennedyslaw.com) is a UK Government Relations Advisor at Kennedys, responsible for monitoring and influencing policy, legislation and regulation on behalf of clients.

Edward Le Gassick is a Trainee Solicitor in Kennedys' Cyber and Data Risk Team. He assists clients with responding to international incidents, as well as providing advice on reducing exposure to new and unforeseen risks from emerging technologies.

Kennedys is a leading law firm in dispute resolution advisory services. It has specialist cyber, data protection and local authority teams. **kennedyslaw.com**