10 QUESTIONS TO ENSURE YOUR COUNCIL ISN'T COMMITTING DATA DISCRIMINATION

Abigail Burke, James Baker

Importance of Data Protection & working to eradicate data discrimination.

`In the UK, several laws, including the UK GDPR and 2018 Data Protection Act, address personal data protection. Personal data can include someone's name, email address, and location. 'Sensitive' personal data can reveal someone's race, religious beliefs, political opinions, or trade union membership status. Local authorities and Councilors will handle people's sensitive personal data in their work.
As technology embeds itself in every aspect of our lives, companies and government bodies are acquiring a wealth of data about us. From staying in touch with loved ones to searching for health information online or ordering from an online food shop, the data that is collected on us can create a highly detailed picture of our likes and dislikes and our background and personality. This information can be used for good, but it also gives companies tremendous power to profile, manipulate, and potentially unlawfully discriminate against individuals.

Good, well-managed data personal data, coupled with public data transparency, can help inform the delivery of local public services. However, poorly managed data and biased algorithms can also lead to negative outcomes with people suffering 'data discrimination'. Many Councilors will have come across situations where a local resident has had an unfair decision made about them because of either incorrect data being held about them or a flawed automatic decision-making process failing to take their personal circumstances into account correctly.
In recent years, high-profile cases of unlawful data use have occurred in sectors as

varied as policing, healthcare, housing, and politics. This July, the ICO released a statement arguing that the unlawful processing of personal data by algorithms can have "damaging consequences for people's lives" and lead to unfounded job rejections and the denial of bank loans or local service provisions that authorities might deliver.

Data Tracking on Council Websites

People rely on council websites as a pillar of local support and guidance. When people have a baby, move to a new flat, or get married, UK law requires individuals to register these life events with their local council. As councils have increasingly moved to digitise their services, companies embedded on council websites extract sensitive about individuals.

A 2020 report by Brave sounded the alarm on extensive data collection by third-party companies on local council websites across the UK. Each time you load a page on a council website, private companies embedded on the site receive the following data: the URL address of each page you visit, ID codes that identify you as the person who loaded the page at a specific time, your location, and your device's details. These details allow the company to connect your activity on the council website to what you view across the wider Internet.

Brave reports that over 400 councils expose visitor data to private companies, and "at its most dangerous, data brokers learn directly from council sites when individuals read about alcoholism and substance abuse assistance" or financial problems.

Questions for Councilors to ask in scrutiny, audit and meetings to help eliminate data discrimination

General data protection questions: for scrutiny or audit

1. When the Council considers new policies are Data Protection Impact Assessments (DPIA) undertaken to help inform decision makers of the risk of data discrimination occurring?

2. What training do staff undertake on data protection laws? Are members provided with the resources needed to understand data protection?

3. Do data protection standards feature as part of internal audits of Council services?

4. Do the risks of unlawful data processing and data discrimination feature on the Council's corporate risk register?

5. How quickly does the council respond to subject access request for personal data, and does the council adequately inform local residents of their data rights?

6. What measures are put in place to protect people's sensitive personal data from Cyber attacks

Questions specific to data processing on council websites:

7. What companies are currently allowed to operate on the council website, and what information do they collect about local residents?

8. Does the council website use Real Time Bidding ad auctions on its website?

> Real Time Bidding (RTB) "faces multiple GDPR investigations for systematic data breaches, because it broadcasts people's personal data to countless companies."[1] RTB exposes people to profiling by "innumerable companies, billions of times a day."[2]

9. Does the council use embedded Google systems on their website?

> "196 council websites use Google's RTB system. Google's RTB shares data with hundreds of companies, without any assurance of who that data is then shared with

1 Brave. (2020.). *Surveillance on UK Council websites.* p. 7. Retrieved November 3, 2022, from https://brave.com/static-assets/files/Surveillance-on-UK-council-websites_compressed_version.pdf

2 Brave. (2020.). *Surveillance on UK Council websites.* p. 7. Retrieved November 3, 2022, from https://brave.com/static-assets/files/Surveillance-on-UK-council-websites_compressed_version.pdf

or how it will be used."[3]

10. Does the council website embed social media sites like Twitter and Facebook on their website?

> "Facebook, Twitter, and many other companies are able to learn about people because of social sharing buttons that appear on council websites. More than a third (38%) of council sites have a social plug-in that tells social platforms or "audience research" companies what people are reading."[4]

The Bottom Line

Improper processing of personal data by councils and data leakage from council websites are a "data breach" under Article 5(1)f of the GDPR. Just as local councils have a duty to promote the general welfare of the communities they represent, councils have a responsibility to protect the data of visitors to their website. Individuals visit their local council website for everything from registering the birth of their newborn child to seeking help for substance abuse. When people access their local council website, they deserve to know that their data will be safe and processed in a responsible manner in accordance with the law.

Resources

- Information Commissioner's Office Local Council Data Protection Toolkit
- Brave's report: 'Surveillance on UK council websites'

---

3 Brave. (2020.). *Surveillance on UK Council websites.* p. 7. Retrieved November 3, 2022, from https://brave.com/static-assets/files/Surveillance-on-UK-council-websites_compressed_version.pdf

4 Brave. (2020.). *Surveillance on UK Council websites.* p. 10. Retrieved November 3, 2022, from https://brave.com/static-assets/files/Surveillance-on-UK-council-websites_compressed_version.pdf