

Data protection law is changing



Organisations across the country are preparing for the biggest change to data protection laws since the Data Protection Act was introduced 20 years ago.



The European General Data Protection Regulation (or GDPR) comes into effect on Friday 25 May and significantly enhances the existing obligations organisations have to protect your personal information.

Tough fines face those which fail to comply.

Locally, it means residents can have a greater say on how North Somerset Council processes personal information, including having the right to:

- know why the council holds your personal information
- be informed about how it uses it before you give any personal information
- receive copies of all personal information the council holds about you

- have personal data rectified if it is factually inaccurate or incomplete, and to restrict the data processing until it is corrected
- be forgotten - you may request the council deletes all personal information about you from its systems and records
- object to certain types of data processing, such as direct marketing.

These rights apply to all organisations and businesses across Europe, not just the council.

North Somerset residents can also request these rights from the council now, and not wait until 25 May.

Once the UK leaves the European Union, these rights will continue to be covered by the UK Data Protection Bill.

Receiving further information

New GDPR rules are coming in about how organisations obtain consent to send you further information about its business or that of its partners.

From Friday 25 May:

- consent must be explicit and provided on an opt-in basis
- if challenged, organisations must produce proof that consent was freely and explicitly given.



Being forgotten

GDPR gives people the right, at any time and without notice, to withdraw any consent they may have previously given an organisation to process their personal information.

However, it is not always necessary for the council to have your consent.

It can do this where it needs to...

- process the information because of a contract the council holds with you
- comply with a legal obligation
- protect your vital interests
- carry out statutory duties.

For example, the Local Government Finance Act requires local authorities to collect council tax and processing personal information is needed to do this.

How we use your personal data

North Somerset Council is registered with the Information Commissioner's Office to process personal data for legitimate business use.

The council will:

- continue to strengthen its procedures to maintain confidentiality
- require all employees to comply fully
- hold the minimum personal information necessary to perform its functions, and erase it once the need has gone
- make every effort to ensure information is accurate, up-to-date and any inaccuracies are corrected without unnecessary delay
- obtain and process all personal data in accordance with the fair processing code
- design its systems and processes to comply with data protection principles
- not publish personal data on its website without explicit consent from the subject
- take immediate action if policies are not complied with.

Any personal information will only be disclosed for notified purposes to:

- **staff** – where information is vital to their work
- **courts** – under a court order
- **partners** – strictly in accordance with agreed protocols
- **others** – as detailed in the notified register entry.

With residents' consent, email addresses will be gathered from the information they submit when interacting with the council, to provide information and news.

An external supplier sends these emails but the council remains responsible for the data security. There is always an opportunity to unsubscribe or re-subscribe in future.

Information collected is used to:

- improve the council's website
- customise the website's content and layout
- notify users (with their consent) about updates to the website
- contact users (with their consent) for marketing purposes.

Under the Digital Economy Act, personal data may be shared with other public authorities for fraud or crime detection or prevention, to recover monies owed, to improve public service delivery, or for statistical research. This information is not shared with other organisations for commercial purposes.

Sharing data to combat fraud

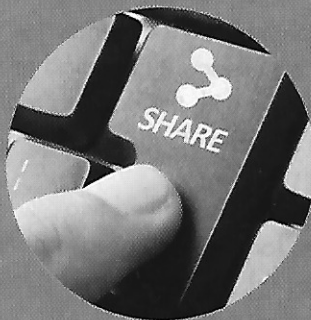
Fraud costs the public sector an estimated £20.6bn a year so it's in everyone's interests to prevent it.

Public authorities have a particular responsibility to ensure taxpayers' money is not taken fraudulently.

Computerised data matching allows potentially fraudulent claims and payments to be identified.

This is carried out by the Cabinet Office, by comparing computer records of one body to see how far they match another.

The Cabinet Office requires the council to participate in a data matching exercise. It is carried out under the Local Audit and Accountability Act and does not require the consent of the individuals concerned.



For more details visit www.ico.org.uk