National Fraud Initiative Privacy Notice

5th September 2023

Background

The National Fraud Initiative (NFI) is an exercise that matches electronic data within and between public and private sector organisations to prevent and detect fraud. The NFI is run by the Cabinet Office.

These organisations include police authorities, local probation boards, fire, and rescue authorities as well as local councils and a number of private sector organisations. Public sector organisations are required to submit data to National Fraud Initiative on a regular basis.

This notice sets out how we will use your personal data, and your rights in line with data Protection Legislation (including the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

As a Local Authority, we are required to share core areas of data with The NFI on a mandatory basis, these include: -

- payroll
- pensions
- trade creditors' payment history and trade creditors' standing data.
- housing (current tenants and individuals on a housing waiting list) and right to buy (completed and in progress)
- housing benefits (provided by the DWP)
- council tax reduction scheme
- council tax
- electoral register
- students eligible for a loan (provided by the SLC)
- private supported care home residents
- transport passes and permits (including residents' parking, blue badges, and concessionary travel)
- insurance claimants
- licences – market trader/operator, taxi driver and personal licences to supply alcohol (voluntary)
- personal budget (direct payments) and social care
- COVID grants (where applicable).

There are data specifications which set out exactly what data we process in the above areas for this data matching exercise. Further information can be found at www.gov.uk by searching for "National Fraud Initiative".

Criminal Convictions

Should data matching through the NFI result in a prosecution, then this may also be recorded by participating organisations. This information is for recording outcomes purposes only and the data won't be shared further.

Special categories of personal information (Article 9 of UK GDPR & Chapter 2 Section 10 of the DPA 2018).

Special categories of personal information are included in the above list.

Housing benefit and student loan data includes an indicator of physical or mental health or condition. This disability flag, which does not identify the specific condition, is shared as the information collected about the disability has an impact upon a student's entitlement to claim housing benefit.

The personal budget (direct payment) information involves sharing data relating to individuals who have a specified range of social care needs because they have a particular condition.

Information shared on blue badge holders (and applicants) will inform the NFI that you have a blue badge but the medical condition that entitles you to this will not be shared.

Purpose

The purpose(s) for which we are processing your personal data is: To assist in the prevention and detection of fraud.

Data matching involves comparing sets of data, such as the payroll or benefits records of an organisation, against other records held by the same or another organisation to see how far they match. The data is usually personal information.

The data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency that requires further investigation. No assumption can be made as to whether there is fraud, error, or other explanation until an investigation is carried out.

The processing of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under its powers in Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under data protection legislation or the GDPR.

All organisations participating in the data matching exercises will receive a report of matches that they should investigate, to detect instances of fraud, over or under-payments and other errors, to take remedial action and update their records accordingly.

This is one of the ways in which the Minister for the Cabinet Office takes responsibility within government for public sector efficiency and reform.

Automated Profiling

Your personal data will be subject to the following automated profiling (as defined in Article 4, paragraph 4 UK GDPR):

Data matching involves comparing sets of data, such as the payroll or benefits records of an organisation, against other records held by the same or another organisation to see how far they match. The data is usually personal information. The data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency that requires further investigation. No assumption can be made as to whether there is fraud, error, or other explanation until an investigation is carried out.

All organisations participating in the Cabinet Office's data matching exercises receive a report of matches that they should investigate, to detect instances of fraud, over or under-payments and other errors, to take remedial action and update their records accordingly.

Legal basis of processing

The legal basis for processing your personal data is that processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

The National Fraud Initiative is conducted using the data matching powers bestowed on the Minister for the Cabinet Office by Part 6 of the Local Audit and Accountability Act 2014. Under the Local Audit and Accountability Act legislation, the Cabinet Office may carry out data matching exercises for the purpose of assisting in the prevention and detection of fraud. The Cabinet Office requires certain organisations (as set out in the Act) to provide data for data matching exercises.

The Cabinet Office may disclose the results of data matching exercises where this assists in the prevention and detection of fraud, including disclosure to organisations that have provided the data and to auditors that it appoints as well as in pursuance of a duty under an enactment.

The Cabinet Office may disclose both data provided for data matching and the results of data matching to the Auditor General for Wales, the Comptroller and Auditor General for Northern Ireland, the Auditor General for Scotland, the Accounts Commission for Scotland and Audit Scotland, for the purposes of preventing and detecting fraud.

Wrongful disclosure of data obtained for the purposes of data matching by any person is a criminal offence. A person found guilty of the offence is liable on summary conviction to a fine not exceeding level 5 on the standard scale.

The Cabinet Office may report publicly on its data matching activities.

Sensitive personal data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The legal basis for processing your sensitive personal data is that it is necessary for reasons of substantial public interest for the exercise of a function of the Crown, a Minister of the Crown, or a government department.

The Cabinet Office conducts data matching exercises to assist in the prevention and detection of fraud. The processing of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under its powers in Part 6 of the Local Audit and Accountability Act 2014. The legal basis for processing your criminal convictions data is paragraphs 6 and 10 of schedule 1 to the Data Protection Act 2018.

Recipients

As a Local Authority we are a mandatory participant in the NFI we will share your data with the Cabinet Office for the purposes of preventing and detecting fraud. The data that is matched and the reasons for matching it for fraud prevention and detection for information summarising the match types are appropriate to us as a Unitary Authority and for the purpose of the matching please refer to the document NFI match types per participating organisation.

Retention

Your personal data will be kept by us for the periods set out in our Record Retention and Document disposal policy. If you would like to view this policy, then please contact dataprotection@southend.gov.uk to request a copy.

Your personal data will be held by the Cabinet Office for the periods set out in their Data Deletion Schedule. Further details of this can be found at www.gov.uk National Fraud Initiative.

Your Rights

You have the right to:

1. Request information about how your personal data is processed, and to request a copy of that personal data.
2. Request that any inaccuracies in your personal data are rectified without delay.
3. Request that any incomplete personal data are completed, including by means of a supplementary statement.
4. Request that your personal data are erased if there is no longer a justification for them to be processed.
5. In certain circumstances (for example, where accuracy is contested) to request that the processing of your personal data is restricted.
6. You have the right to object to the processing of your personal data where it is processed for direct marketing purposes.

Who can you contact about data protection and your rights?

The data controller for your personal data is Southend-on-Sea City Council.

We have a Data Protection Officer who makes sure we respect your rights and follow the law.

If you have any concerns or questions about how we look after your personal information, please contact the Data Protection Officer at Dataprotection@southend.gov.uk or by calling 01702 215000 and asking to speak to the Data Protection Officer.

For independent advice about data protection, privacy, and data sharing issues or to lodge a complaint about how we have handled your information you can contact the Information Commissioner's Office (ICO) at:

ico.org.uk or email casework@ico.org.uk

Alternatively, you can write or telephone: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number.

Furthermore, the data controller for the NFI is the Cabinet Office. The contact details for the data controller are:

Head of the National Fraud Initiative
10 South Colonnade
Canary Wharf
London
E14 4QQ

Email: nfiqueries@cabinetoffice.gov.uk

The contact details for the Data Protection Officer (DPO) of the data controller are:

Stephen Jones
DPO
Cabinet Office
70 Whitehall
London
SW1A 2AS

Email: dpo@cabinetoffice.gov.uk

Useful links: -

National Fraud Initiative - GOV.UK (www.gov.uk)

National Fraud Initiative privacy notice - GOV.UK (www.gov.uk)

Contact details for the NFI: National Fraud Initiative (nfi.gov.uk)