Response to Consultation: A future demand-led fuel poverty scheme to succeed Welsh Government Warm Homes – Nest

Submitted by: Information Commissioner's Office
2nd Floor, Churchill House, Churchill Way,
Cardiff CF10 2HH

Tel: 029 2067 8400

Email: wales@ico.org.uk

Background to the Information Commissioner's Office

The Information Commissioner has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations (EIR) and the Privacy and Electronic Communications Regulations. The Information Commissioner's Office (ICO) is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

The ICO will provide a response only to consultation issues relevant to the scope of this office. In this instance we would like to take the opportunity offered by the consultation to emphasise the importance of undertaking a Privacy Impact Assessment on your proposals, and ensuring that appropriate provisions are in place to ensure that all personal data used by the scheme is handled in accordance with the Data Protection Act 1998.

A) Fair and Legal Processing of Personal Information

Our understanding from the consultation document is that the Nest scheme as currently operated and also in the proposed new scheme, requires consideration of a significant amount of personal information about members of potentially eligible households. Some of the information required - such as information relating to health or disability

status of occupants – falls into the DPA's category of sensitive personal data.

Under principle one of the DPA, for processing of personal data to be legal, it must – amongst other things – satisfy at least one condition for processing as set out in Schedule 2 of the Act. Where the data to be processed falls within the definition of sensitive personal data, then at least one condition from Schedule 3 of the Act must also be met. These are known as conditions for processing, and clear identification of which ones are to be relied upon is the first step to ensuring that any project involving personal data is legal.

If the *consent* of individuals is being relied on as a condition for processing, please note that Schedule 3 requires that for sensitive personal data this must be *explicit,* ie that the individual understands exactly why you need their sensitive data and has expressly consented to the actions you have told them you want to take with that data. In addition, individuals have a right to revoke consent at any time and your information systems should take this into account.

Principle one also states that that handling of peoples' personal data must be fair. A key element to meeting this requirement is to provide individuals with clear information about why you need the data, what you intend to do with it, and what organisations (or types of organisation) you may share it with. You must also state clearly the identity of the organisation that is the data controller, and how to contact them if the individual has any queries or wishes to request a copy of their personal data. This is known as a fair processing or privacy notice, and the ICO's new Code of Practice on Privacy Notices, Transparency and Control provides detailed guidance.

Please note that the EU General Data Protection Regulation (GDPR) is due to come into force in May 2018. Whilst the result of the EU referendum means that the implications of this for the UK are currently unclear, the ICO is advising organisations to give GDPR careful consideration in their policy making. Even if the UK does not adopt the EU law, in order to support trade with the EU it will need to put in place very similar legislation.

B) Data Sharing

The existing and proposed schemes involve sharing personal data between various organisations about individuals who may be eligible for support, for example the third party referral organisations, Nest, service providers and DWP. The points in the paragraph above relating to the

importance of fair processing and a clear legal for processing basis also apply to information sharing.

The sharing of personal data should be underpinned by a clear Information Sharing Agreement, such as those made under the Welsh Government's WASPI scheme (Wales Accord for Sharing Personal Data). WASPI sets out a clear template to help organisations through the complex process of sharing personal data legally, and fully reflects the ICO's comprehensive Data Sharing Code of Practice.

The EU legislation referred to above also contains measures in relation to data profiling which may be relevant if this scheme is seeking to identify eligible individuals through data matching.

C) Privacy Impact Assessment

Privacy Impact Assessments (PIAs) are an excellent way of ensuring that data protection matters are taken into account at the early stages of planning any project that uses personal information. ICO strongly recommends their use so that risks are identified and appropriate measures to protect individual's data can be built in throughout the project. If the EU data protection reforms come into effect in the UK in 2018, PIAs will become a legal requirement in certain situations, and the ICO will expect organisation to have a process for conducting PIAs embedded into their procedures.

For guidance on how to undertake a PIA, see the ICO's Conducting a Privacy Impact Assessment Code of Practice.

Please contact Helen Thomas at the ICO's Cardiff Office on 01625 545298 if you would like to discuss any aspect of the above response.

14 October 2016