Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

The Information Commissioner's response to the Department for Business, Energy & Industrial Strategy's consultation on the warm home discount scheme 2021/22

About the ICO

The Information Commissioner has responsibility in the UK for promoting and enforcing the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Privacy and Electronic Communications Regulations 2003 (PECR), amongst others.

The Commissioner is independent from government and upholds 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 and taking appropriate action where the law is broken.

Introduction

The Information Commissioner's Office (ICO) welcomes the opportunity to respond to this Department for Business, Energy & Industrial Strategy (BEIS) consultation on the warm home discount scheme (WHD) and notes the active engagement we have previously had with BEIS regarding the WHD.

Whilst the consultation is largely concerned with the financial elements of the WHD extension, this response focuses on the data protection and privacy considerations of the scheme.

Automated processing in relation to the 'Core Group'

The ICO notes that most individuals eligible for WHD through the Core Group are identified through a process of data matching with data provided by DWP. From the information available, it appears that this constitutes solely automated processing as defined in Article 22 of GDPR. Article 22 notes that data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

Organisations can therefore only carry out this type of processing if they can rely on one of the three exceptions set out in Article 22(2), but it is not clear from the consultation which exception BEIS are relying on, so further clarity is welcomed if

this applies. The ICO has produced detailed guidance on the data protection requirements when using solely automated decision making that may be of use in determining if one of the three exceptions applies in relation to any of the individuals eligible under the Core Group.

Data protection impact assessments (DPIAs)

The ICO highlights the importance of adopting a data protection by design and default approach to ensure that any risks in the processing of personal data for implementing the WHD are appropriately mitigated against and appropriate safeguards are put in place. A DPIA is a tool to help controllers ensure that they are processing personal data in a manner that is compliant with the data protection legislation.

Indeed, a DPIA must be carried out before any type of processing that is "likely to result in a high risk" to the rights and freedoms of individuals. Article 35(3)(a) of GDPR notes that any systematic and extensive evaluation of personal aspects which is based on automated processing and on which decisions that produce legal effects or similarly significantly affect the individual, a DPIA must be undertaken.

As it appears that the use of data matching for most individuals who are eligible in the Core Group relies on automated processing and results in an individual being given the WHD or refused it, such an assessment must be completed. Similarly, the consultation notes that Broader Group and Industry Initiative eligibility is determined by factors such as receipt of certain benefits or individuals having a health condition that makes them more vulnerable to the effects of living in a cold home. As this is likely to include data concerning vulnerable subjects and is likely to be processed on a large scale, this processing would also need to be considered in the DPIA.[1]

The consultation notes that letters will be sent to those in the Core Group who have not been matched but do receive a qualifying benefit to inform them that a Helpline option is available for them to verify their eligibility for the WHD. Whilst this helps ensure all individuals in the Core Group have the opportunity to be included in the scheme if eligible, the risks to the individual of the proposed processing should be assessed and all mitigating steps and safeguards in relation to the risks that have been identified should be set out in the DPIA.

The Information Commissioner has produced guidance that outlines when DPIAs are legally required, and how such assessments should be undertaken.

[1] As set out in the Article 29 working party of EU data protection authorities (WP29) guidelines available here.

Considering and mitigating the potential privacy risks at the earliest stage of the extension of the WHD will help ensure that both individuals and organisations can realise the benefits of the WHD in a way that takes account of privacy risks, integrates appropriate safeguards into the processing and helps controllers fulfil their accountability obligations. This is particularly important when the processing relates to vulnerable individuals.

ICO's Data Sharing Code of Practice

The data protection legislation obliges the Information Commissioner to produce a statutory Code of Practice on data sharing. The code is currently being finalised following public consultation. It will be submitted to the Secretary of State and then laid before Parliament.

Organisations involved in processing personal data in relation to the WHD will need to take the Code into account when sharing personal data. This not only applies to the sharing between DWP and energy suppliers for those individuals in the Core and Broader Groups, but also for the sharing between energy suppliers and other organisations, such as charities, in relation to those individuals in the Industry Initiatives group.

Adhering to the code will help to ensure good practice around data sharing and help to manage risks associated with sharing information, including the parties' approach to matters such as cybersecurity. Following the code and adopting its practical recommendations will help to give organisations confidence to collect and share personal data in a way that is fair, transparent and in line with the rights and expectations of the people whose information is being shared.

Transparency information for data subjects

The requirement to provide privacy information to individuals in relation to how their personal data will be processed is a fundamental right under the data protection legislation. Articles 13 and 14 of the GDPR specify the information individuals have the right to be given in relation to the processing of their personal data.

This is an obligation that controllers will need to comply with to ensure that consumers are provided with clear and comprehensive information about how their personal data will be processed, including what personal data will be collected, the purpose of the processing, how long it will be processed for, and who it will be shared with. Further, data should not be processed in a way which data subjects would not reasonably expect.

When processing information from any type of vulnerable individual, organisations must make sure they treat them fairly. This means drafting privacy information appropriate to the level of understanding of the intended audience and, in some cases, putting stronger safeguards in place. Particular care should be taken to ensure individuals understand the purpose for which data will be processed and the extent of this.

In particular, those individuals in the Core Group have the right to be told the details of the existence of solely automated decision-making if this applies. Whilst this type of processing may be complex, organisations should use simple, understandable terms to explain the rationale behind decisions and how they might affect individuals. Individuals should be told what information is used, why it is relevant and what the likely impact is going to be.

Additionally, individuals need to receive information about their right to have incorrect data rectified, This is of particular importance for those individuals in the Broader Group, as the WHD provided through this part of the scheme is described in the consultation as usually awarded on a first-come first-served basis. It will be necessary to consider how BEIS and others will comply with data protection legislation, including ensuring that the processing is fair, in situations including, for example, where an individual applied and it transpired that they were denied the WHD rebate because the personal data processed was inaccurate.

It is often most effective to provide privacy information using a combination of techniques, including layering and dashboards. Careful consideration should be taken regarding what format is the most appropriate under the circumstances, particularly in relation to vulnerable individuals.

Privacy information must be regularly reviewed to ensure that any new use of an individual's personal data is brought to that individual's attention before the processing begins. The Information Commissioner has published guidance on privacy information that provides further information on this requirement.

Data retention

Article 5(1)(e) of the GDPR specifies that data must not be retained for longer than necessary in relation to the purpose for which it is processed. Ensuring that personal data is erased or anonymised when it is no longer needed will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. This also reduces the risk that controllers will use such data in error.

It is also important that retention periods are reviewed regularly as appropriate in the context of the processing, and that ongoing testing of the retention periods is undertaken by using available data to test how useful it has been to keep these records for the specified time. For example, if records haven't been used within two to three years then it is likely to be deemed excessive to retain them for that length of time.

Therefore, it is important to set an appropriate retention policy for any data used to implement the WHD and to make data subjects are of this retention policy.

Smart Metering

The proposal to require suppliers to provide advice about the benefits of smart meters, as outlined on page 20 of the consultation, may constitute direct marketing as defined by section 122(5) of the DPA 2018. If suppliers are considering promoting smart meters by electronic methods then the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) may apply in addition to the GDPR.

The ICO is happy to provide further input on these matters and welcomes further engagement from BEIS on the WHD extension. We also look forward to hearing from BEIS again when the time comes to consult on changes to the WHD scheme.

Information Commissioner's Office

November 2020