Department for
Business, Energy
& Industrial Strategy

ECO FLEXIBLE ELIGIBILITY GUIDANCE:

Data sharing for determination of eligibility and fuel poverty targeting: some legal issues and general GDPR Principles of which to be aware.

February 2019

Any enquiries regarding this publication should be sent to us at:
beisecoteam@beis.gov.uk

Contents

The purpose of this Guidance

Accessing data can be crucial to enable the identification of fuel poor and/or low income and vulnerable to the cold ('LIVC') households that may benefit from support under the ECO local authority flexible eligibility scheme ('ECO flexible eligibility'). Once obtained, sharing information for fuel poverty and LIVC purposes will invariably involve the processing and sharing of personal data.[1] This must be performed in compliance with the General Data Protection Regulations (EU 2016/679) ('GDPR') and the Data Protection Act 2018 ('DPA 2018), both of which came into force on 25 May 2018, replace the 1998 Data Protection Act and together combine to provide the regulatory and statutory framework for data protection in the UK. The DPA 2018, with minor exceptions, extends and applies to the whole of the UK. For the most part, local authorities will only be concerned with the 'general processing' provisions of Part 2 of the DPA 2018.

It is important to note that this Guidance is intended merely to provide guidance on the processing of data for the purposes of ECO flexible eligibility. **It is neither intended to be an exhaustive list of considerations – it cannot be, as circumstances will vary - nor does not it constitute formal legal guidance. Local authorities are ultimately responsible for their own data protection procedures and compliance with legislation.** Essentially, the Guidance should not be used in place of advice from your legal team or the data protection officer or other person(s) within the local authority responsible for information governance (hereafter the 'data protection officer')[2].

To assist you in understanding the changes made by the GDPR and the DPA 2018 and for additional information and advice on data sharing and usage, please refer to:

1. The Information Commissioner's Office (the 'ICO'). The ICO is the UK's independent body set up to uphold information rights in the public interest. They are a key point of information on data protection, processes and legalities. This document should be read alongside the ICO Guide to Data Protection.

2. The Local Government Association whose mission statement is to support, promote and improve local government. It offers a range of programmes to 'promote understanding of open data and transparency, and has created a customisable 'Record of Processing Activities' tool to assist local authorities in maintaining a record of their processing and sharing activities: Local Government Association Support; and

3. The Centre for Excellence for Information Sharing. While the Centre is not currently operating, their website continues to make available many of their published resources aimed at 'supporting the public sector in overcoming information sharing challenges': informationsharing.org.uk

References in this document to the GDPR should be taken to include reference to the relevant section of the DPA 2018 and all references to Articles are to Articles of the GDPR unless otherwise stated.

[1] See the following section.
[2] Note the GDPR introduces a duty for public authorities or bodies to appoint a data protection officer: Article 37; recital 97 refers.

Key data considerations when designing your proposals before sharing or exchanging personal data.

The consideration of data protection and privacy issues from the outset of any project lifecycle has always been advocated as 'best practice'. The GDPR makes it a legal requirement to consider data protection as part of the project design.[3] You are now required to put and have in place 'appropriate technical and organisational measures' in order to implement the GDPR and to protect the rights of data subjects. It is important, moreover, to ensure that the personal data you process is 'adequate, relevant and limited to what is necessary in relation to the purposes for which the data is being processed'[4] and that you are able to demonstrate your compliance with the GDPR[5] in respect of the data's collection, use and retention. These are some of the GDPR Principles underlying and fundamental to the data protection regime (the 'Principals')[6].

In short, handling data appropriately is important, and while a 'good in itself' to be adopted, it is worth bearing in mind that failure to comply with the GDPR may leave the local authority open to substantial fines, with infringements of the GDPR Principles and the other basic conditions for processing personal data attracting the highest tier of administrative fines. This could mean a fine of up to €20 million.

Particular Elements to be considered

There are a number of questions that you will need consider when planning or proposing to share personal data as part of ECO flexible eligibility. Your legal team and/or data officer may ask you questions around these points, or it may be that your organisation has a process or template which helps you to think through each of these questions (for example it may be that you need to complete a business case, which would answer each of these points). In any event, it is important that development of your project and deliberation of questions are considered alongside the ICO Guide to Data Protection.

Generally, initial questions to consider are:

[3] Article 25 of the GDPR.
[4] Article 5(1)(c).
[5] This is a new 'accountability principle' introduced by the GDPR: Article 5(2).
[6] Article 5 sets out the seven GDPR Principles that underlie and are central to the protection of personal data required by the GDPR.

Does the data being shared need to be personal data?

2.1 What is personal data?

'Personal data'[7] means any information that relates to an identified or identifiable living individual.

Note:

- An 'identifiable living individual' is someone who can be identified, *directly or indirectly*, by for example, a name, an identification number (e.g. council tax reference number; electoral roll number), an online identifier (e.g. email address; response ID to an online council survey; IP address) etc.;
- The reference to 'directly or indirectly' means, from the data itself or in conjunction with other information which is either in the possession of the local authority, or is reasonably likely to come into its possession; and,
- 'Relates to' means that the data must concern the individual, i.e. the data subject, and, in the context of processing that data, could affect their privacy rights.

Illustration

[I]

'*LA Declaration - Address of Premises*

1 Overton Way, Hovering. HX1 2XX – Fuel Poverty'

Even without the specific name of the individual, the postcode and house number may be sufficient to identify the individual in which case the data will be classed as personal data.

[II]

The local authority will have a list of households included on statements in writing ('LA Declarations') and a list of households who receive flexible eligibility measures ('List File'). Personal details of the individuals concerned are not included on those lists. Individuals are however linked to a specific household through a dedicated local authority account number that is held on a separate database.

Although the data on the List File does not identify individuals directly, the List File data are nevertheless personal data as the individuals can be identified "from other information in the possession of" the local authority.

Making the data, in the form of the LA Declaration, available to suppliers will count as 'sharing data' and will fall within the scope of the GDPR.

[7] Section 3 of the DPA 2018.

Remember: It should not be presumed that the GDPR and DPA 2018 prevent the disclosure of personal data. Any processing of personal data must be 'fair, lawful and transparent' and further processing must not be incompatible with the purposes for which it has been collected.

2.2 What is sensitive personal data?

Under the DPA 1998, data concerning health was classed as 'sensitive personal data' and its processing strictly controlled. This continues to be the case under the GDPR, albeit this type of data is now referred to as a 'special category of personal data'. As well as a new name, the range of data previously classed as 'sensitive personal data' under the DPA 1998 has been extended to include genetic data and some biometric data but criminal offences and convictions data have been removed[8].

In addition to the other requirements of the GDPR, and specifically identifying a lawful basis for processing under Article 6, data concerning health may only be processed if one of the conditions set out in Article 9 of the GDPR is met. These include where *'the processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.'*[9] ECO Flexible eligibility is not a legal obligation imposed on local authorities and as such does not of itself meet this particular criterion for processing of health data.

Illustration [I]

The Local Authority published a statement of intent…and has made a statement in writing that the premises are occupied by a household living on a low income and vulnerable to the effects of living in a cold home.

Details of an individual's specific health condition are classed as a 'special category of personal data'. Although statements of intent will set out the terms of eligibility in relation to 'low income and vulnerable to the effects of the cold', local authorities are not being asked to disclose 'special category personal data' to energy suppliers or other third parties. It is sufficient for energy suppliers merely to be informed that a household satisfies the published eligibility criteria noted in the Statement of Intent, namely that the household is of 'low income and vulnerable to the effects of the cold'.

Illustration [II]

When assessing whether an individual falls within the criteria of its published Statement of Intent, the local authority is likely to have regard to special category data to make its assessment of the individual's eligibility. On the basis of that assessment, the local authority will then decide whether to make a requisite declaration.

[8] Note: Article 10 places strict controls on processing of personal data relating to criminal convictions and offences.
[9] Article 9(2) GDPR and Schedule 1(1) DPA 2018 refers.

When performing that assessment, the local authority will be processing the individual's data, whether that processing is carried out with the explicit consent of the individual concerned or to meet one of the conditions of article 9, such as 'the substantial public interest' provision.

In relation to Illustration II above, note:

Explicit 'consent': Unless certain strict circumstances apply that justify processing of sensitive categories of data without explicit consent, obtaining an individual's consent is to be the norm. Scenario 1 on page 28 is an example of where such processing is performed with the data subject's consent.

'**Substantial public interest'**: Part 2 of Schedule 1 of the DPA 2018 sets out a number of situations when processing of special category data will be permissible and legitimately used without the explicit consent of the data subject, for example, for statutory etc and government purposes (paragraph 6) or safeguarding the economic well-being of individuals (paragraph 19). Note there are a number of additional limits and restrictions on the use of this provision. That said, the key objective behind the concept of 'substantial public interest' is the desire that *'organisations are able to continue lawfully processing data whilst also achieving a balance between individuals' rights.'*

Illustration [III]

Local authority processes data for the purposes of evaluating the racial or ethnic mix of households named on Declarations in order to determine the racial or the ethnic category and their numbers receiving ECO measures.

Processing of racial or ethnicity data is prohibited by virtue of Article 9(1), except where, for example, the processing of that data by the local authority is necessary for the performance of a task carried out in the public interest (Article 6(1)(e)) and, in also satisfying a necessary Article 9(2) condition, it also, for example, satisfies Article 9(2)(g) GDPR and, per the requirement of s.10(3) DPA 2018, meets a 'substantial public interest condition' of Part 2,Schedule 1, for example, paragraph 8.

Illustration [IV]

A charity, working with vulnerable individuals across a number of geographic areas, is concerned about the economic well-being of the individuals with whom they work: specifically, the total amount of money they have to spend on consumption and their inability to keep adequately warm at reasonable cost, given their available income and their household energy requirements. The charity refers these individuals to their relevant local authority for inter alia, assistance under ECO flexible eligibility.

Protection of economic wellbeing is a substantial public interest and as such, one that may permit the transfer of personal data of the data subject without the data subject's consent if the transfer will safeguard their economic wellbeing.

In this instance the local authority will be the recipient of that data. The local authority may be able to process that data for the purposes of ECO flexible eligibility if the processing continues to be necessary for reasons of substantial public interest and meets, for example, the condition set out in paragraph 6 of Part 2, Schedule 1, namely necessary in exercising a function conferred on the local authority by legislation.

NB: In this example the charity concerned (i) must meet a condition in Part 2, Schedule 1 as well as (ii) comply with the "requirement for an appropriate policy document when relying on conditions in Part 2, in accordance with Part 4, Schedule 1, 'additional safeguards'. In brief, the charity would need to have implemented certain safeguards and have outlined in a policy document how and when they would use the legal bases of Schedule 1.

Important: The identification of a household as 'LIVC' is likely not to fall within Article 9 of the GDPR concerning 'special categories of personal data' although it will still remain personal data. This is on the basis that the household being defined as "low income and vulnerable to the cold" is classified as such without:

- a distinction being made between 'low income' and 'vulnerable to the cold'; or
- a specific health condition being attributed to 'vulnerable to the cold',

and on the assumption that the local authority's published criteria on eligibility is generic.

Pseudonymisation or anonymisation for the purposes sharing data?

2.3 Pseudonymised data

The GDPR introduces the concept and use of pseudonymised data[10], which is to be differentiated from anonymised data.

Pseudonymised data is personal data that is processed in such a way that it can no longer be attributed to a 'living person'[11] *without the use of additional information*[12]. Accordingly, pseudonymous data still allows for some form of re-identification (even indirect and remote), but what is key, is that the additional information, (that would allow access to sensitive information, for example) is kept separately by means of 'appropriate technical and organisational measures'[13].

Illustration

Date of Birth; Gender; Postcode

In isolation, each of the above are 'indirect identifiers'. However, combine them and an individual may be uniquely identified.

[10] See for example, Recitals (28)-(29) and Articles 25 and 32
[11] The reference to 'living person' is to serve as a reminder that the GDPR does not apply to data of a person who is deceased.
[12] Recital 26 and Article 4(5)
[13] Recital 39: 'processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing'.

When acting as a 'data controller, a local authority must ensure that the level of security measures it adopts is 'appropriate to the risk' inherent or attaching to their processing of personal data for the purposes of ECO flexible eligibility. This includes being able to ensure the 'ongoing confidentiality' of the personal data and preventing the 'unauthorised disclosure of, or access to personal data transmitted',[14] for example, by using an encryption scheme.

While the GDPR allows pseudonymisation of data as a means of reducing the risks of breaching a data subject's privacy, this does not mean that such data is exempt from the scope of the regulations.

Illustration

Local authority publishes its Statement of Intent setting out the criteria they intend to use to identify households meeting their eligibility criteria for flexible eligibility. From its separate Health and Social Care Service database the local authority is able to determine persons eligible under LIVC. Local authority refers an individual to an energy supplier for the purposes of an ECO measure and, at acceptance of the individual for a measure, issues a Declaration confirming the individual's eligibility.

The Declaration, which is accorded a unique URN number, only sets out the address(es) of eligible individual(s) and the category under which they qualify for a measure or measures under ECO Flexible eligibility ie. FP, LIVC or In-fill.

The Declaration is shared with the energy supplier and its service provider. In due course, a copy of the Declaration will be provided by the energy supplier to Ofgem for auditing purposes.

The local authority will need to be able to demonstrate that the energy supplier or its installer are unable to access the Health and Social Care Service database directly and accordingly, that 'identifying' special category data is held separately and securely from processed data to ensure the specific details, in this case health details, of the data subject cannot be identified.

2.4 Anonymised data

In contrast, truly anonymised data is not subject to the GDPR.

In order to be classified as 'truly' anonymous data:

[14] Article 32.

- The information must not relate to an identified or identifiable natural person;

OR

- The personal data must have been made anonymous such that the data cannot be linked to a living individual and identification is not likely to take place. For example, where the anonymised data, whether by being combined with information or knowledge already publicly available, cannot lead to individuals being identified.

The ICO Anonymisation Code is based on the DPA 1998. Whilst it will in due course be updated by the ICO to take account of the GDPR and DPA 2018, it remains a useful source of information on aspects of anonymisation.

Illustration

Local authorities are asked to provide the number of:

** Households included on declarations (breakdown by FP, LIVC & in-fill)*

** Households who received LA flex measures (breakdown by FP, LIVC & in-fill),*

within their local authority for statistical purposes

To the extent the information is provided in aggregated form (namely, the combinations of certain indirect identifiers, concern more than one person and it is not possible to identify specific individuals through that data or other data that is in the possession or likely possession of the person receiving those statistics without reasonable effort) then the data set will be sufficiently anonymised.

Lawfulness of processing

When speaking of processing, 'processed' or to 'process' personal data, reference is being made to any activity in relation to personal data such as collecting, consulting, using, storing, sharing, destroying etc. such data.[15]

As noted at section 2.1 above, processing of personal data must be 'fair, lawful and transparent' and not used in a manner that is incompatible with the purpose for which it has been collected. In addition to the other requirements of the GDPR, processing data is lawful only if one of the conditions in Article 6 of the GDPR is met. Three of those conditions are mentioned here.

For the reasons set out within Illustration I on page 7, we would not anticipate local authorities sharing special category data for the purposes of ECO Flexible eligibility, although some processing of such data might occur for the purposes of determining a person's eligibility.

[15] See Article 4(2) of the GDPR and Section 3(4) of the DPA 2018.

2.5 If processing personal data – do you have the individual's (the data subject's) consent?

The condition set out in Article 6(1)(a) of the GDPR is that the *'data subject has given consent to the processing of his or her personal data for one or more specific purposes'*.

Local authorities must be wary of assuming consent on the part of the individual.

In comparison to the DPA 1998, the GDPR significantly enhances the criteria required for consent and to prove that the individual has given consent. It states that consent should be '*given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her…'*[16]

Illustration

An individual contacts the local authority directly, either to ask about a different service or to enquire about getting support through ECO. The local authority asks the individual some questions to verify their potential eligibility for the scheme. The local authority informs the individual about the support that might be available and asks the individual if they agree to their details being passed on to a participating energy supplier. The individual gives their consent.

The local authority must:

Be sure they have received and record the individual's informed consent and provided a privacy notice. Namely, that the individual understands not just the nature of the potential support they might receive under ECO, but also, that they explicitly agree to their personal data (name, address, telephone details etc.) being passed to a third party for the stated purpose. This will satisfy the condition for processing under Article 6 (1)(a).

Assure itself that the processing of that data is necessary and can therefore satisfy the data protection GDPR Principles, particularly around the scope and purpose of why the data is being processed.

The GDPR specifies that:

"the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language"[17];

To paraphrase:

The request for consent must:

[16] Recital (32)
[17] Article 7 refers.

- Be clear and concise;
- State any other persons (ie. identify any delegated local authority partner, energy suppliers etc. that it will be shared with) who will rely on the consent given; and
- Explain that the individual can withdraw their consent and how they can do so.

From the consent given it must be:

- Clear that the individual is in agreement;
- Is consenting to the processing of their data for the purposes of ECO Flexible eligibility; and
- That that consent is separate from any other matters/terms and conditions raised.

Note:

- Is consent '*freely given*'? In making this assessment, the local authority must take into account whether, the data subject will suffer any adverse consequences if they withhold consent. 'Adverse consequences' in this context means a result that goes beyond what would automatically result if the local authority were unable to carry out the data processing to which the consent relates. **For example**, if the data subject is required to give consent to data processing for ECO flexible eligibility, in order to be eligible for the local authority's own home heating grant scheme. In this scenario, refusal of assistance via ECO flexible eligibility, would have the adverse effect of making the individual ineligible for the local authority's own scheme.
- Where the data subject's consent is to be given following a request by electronic means (for example while using a local authority's online energy advice service), the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.
- As there is a requirement to be able to *'demonstrate that the data subject has given consent to the processing operation'*[18] a record should be kept to evidence consent.

2.6 If sharing personal data – is it required to be shared (processed) pursuant to law/a court order?

Article 6(1)(c) of the GDPR states that processing will be lawful if it: *'is necessary for compliance with a legal obligation to which the controller is subject.'*

Note:

'compliance with a legal obligation' refers to law laid down by the UK or EU[19] and includes, amongst others, subordinate legislation[20]. Any processing under article 6(1)(c) is to be determined on that legal basis.

[18] Article 7 and Recital (42) refer.
[19] Article 6(3) refers.
[20] Section 205 DPA 2018 refers.

'necessary': means the processing must be a reasonable and proportionate way of achieving compliance, and that there is no other reasonable way to comply. Note: 'the lawfulness basis will not apply if you can reasonably achieve the purpose by some other less intrusive means, or by processing less data'.[21]

The local authority will need to be able to refer to the specific legal provision or, for example, point to relevant governmental (central or local) guidance that clearly sets out their obligation.

Illustration

The Home Energy Conservation Act 1995 (HECA) places a statutory obligation on local authorities to prepare and publish a biennial report on what is being done to improve energy efficiency in all residential accommodation in their area and progress made in implementing measures.

Using powers under section 5(1)(b) of the Act, the Secretary of State for Business, Energy and Industrial Strategy requires Authorities to report on, inter alia:

Measures that take advantage of financial assistance and other benefits offered from central Government initiatives, to help result in significant energy efficiency improvements of residential accommodation.

In line with the reporting requirements outlined in the HECA Guidance 2019, participating local authorities will be able to include their ECO Flexible Eligibility Statements of Intent in their reports to outline how they intend to target fuel poor households or households on low income and vulnerable to the effects of living in a cold home and outcomes achieved. With respect to reporting outcomes, this will likely require the processing of personal data by participating local authorities to comply with their HECA obligation notwithstanding that the information actually reported will be in anonymised form.

2.7 As a public body do you have a 'public interest task' or 'official authority' basis to share information?

The condition set out in article 6(1)(e) GDPR 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 controller.'*

As with Article 6(1)(c), the basis for the processing must be laid down in UK or EU law and the local authority would need to be able to demonstrate that its processing of data is 'necessary' for the purposes of the task in hand.

It should also be noted that local authorities will not be able to rely on the 'legitimate interests' provision of article 6(1)(f) for any processing carried out in the performance of their tasks as local authorities.

[21] ICO guide to the GDPR, Lawful basis for processing.

Section 6(1)(e) may be available for data processing for ECO flexible eligibility because the local authority's role in ECO flexible eligibility is set out in legislation (the ECO3 Order)[22]. The objective of addressing fuel poverty is an objective of public interest. The Government considers that the procedures for flexible eligibility set out in the ECO3 Order are proportionate to the legitimate aim pursued.

In Summary:

In establishing the lawful basis for processing personal data, it will be for the local authority to determine to what extent it has an express or implied statutory power to act in relation to fuel poverty and/or energy efficiency following the obtaining of the data subject's consent or that falls within the parameter of:

- compliance with a legal obligation;
- a 'task carried out in the public interest'; or
- in the exercise of official authority.

Illustration

Processing data for the specific purpose of following through on an ECO request following determination of eligibility may fall within a local authority's implied statutory powers under the Local Government Act 2000 Part 1 section 2 and/or the Localism Act 2011 (territorial limitations apply). It will be for your legal team to confirm relevance and applicability of such powers to the processing of personal data for flexible eligibility purposes.

2.8 A Legal Gateway

The 2017 Digital Economy Act (the 'DEA 2017')[23], additionally provides a 'legal gateway' for the disclosure of information between specified public authorities for specified purposes. Local authorities[24] are included in the list of specified public authorities, for the purpose of assisting people living in fuel poverty by reducing their energy costs, improving efficiency in their use of energy, or improving their health or financial well-being. Sections 36 and 37 of that Act also enable the disclosure of data between those local authorities and licensed gas and electricity suppliers for use for those purposes under the ECO scheme.

The legal gateways provided by the DEA 2017 override statutory barriers to the disclosure of data and can provide a legal basis for the disclosure of data. *But* all the requirements of the GDPR continue to apply, along with other restrictions and requirements set out in the DEA 2017. These include restrictions on the onward disclosure of the data and requirements to

[22] The Electricity and Gas (Energy Company Obligation) Order 2018, Part 4 section 17 refers
[23] Part 5 refers: http://www.legislation.gov.uk/ukpga/2017/30/part/5/enacted
[24] Schedule 4: specified persons for the purposes of section 35(11) to (17) are: '… A county council in England; a district council in England; a London borough council; a combined authority established under section 103 of the Local Democracy, Economic Development and Construction Act 2009: The Common Council of the City of London in its capacity as a local authority; The Council of the Isles of Scilly; and The Greater London Authority.'

have regard to the Codes of Practice issued under Part 5, Chapter 1 of the DEA 2017, in addition to the relevant codes of practice issued by the ICO.

A local authority will not necessarily need to use the legal gateway provided by the DEA 2017, for example, if it is relying on other powers for the data sharing.

Who is to have access to the personal data shared – can 'need to know' GDPR Principles be adopted?

Some factors to take into account[25]:

- What information needs to be shared? The fundamental premise: only share the data required. For example, you may need to share a local authority resident's current name and address, but not other information held about them.
- Who requires access to the shared personal data? Adopt 'need to know' principles. Namely, energy suppliers or other third parties you are to liaise with in connection with ECO flexible eligibility should only have access to the local authority data required for the specifics of ECO flexible eligibility and the individual household concerned. In addition, only relevant staff within those organisations should have access to the data.
- How is the personal data to be shared? Ensuring 'appropriate technical and organisational measures' are in place applies to the local authority as well as the recipient of the personal data you are proposing to share.
- To what extent can pseudonymisation or anonymisation be used?

Illustration

An individual contacts the local authority directly, either to ask about a different service or to enquire about getting support through ECO. The local authority asks the individual some questions to verify their potential eligibility for the scheme. The local authority informs the individual about the support that might be available to the individual and asks the individual if they agree to their details being passed on to a participating energy supplier. The individual gives their consent.

The local authority should only make available such information as the energy supplier or its intermediary will need to contact the individual to conduct the requisite follow-up. Given the likelihood that the energy supplier will need to share the information (whether intra group or with an external installer), the local authority should consider restricting access to only those at the energy supplier and its service providers who need to know/use the data in addition to addressing the sharing of that information with other third parties, such as ECO auditors or regulators. These details can be set out in a data sharing agreement, so all parties are aware of their obligations.

[25] Adapted from the current ICO Data Sharing Guide, p.14. Note that the guide is in the process of being updated to take into account the changes made by the DPA 2018, the GDPR and other legislation.

Privacy Impact Assessments:

Considered as 'best practice' in relation to the DPA 1998, the GDPR states that where processing is 'likely to result in a high risk to the rights and freedoms' of data subjects, the data controller is required to have carried out a privacy impact assessment ('PIA') prior to and before the processing anticipated.[26]

A PIA is a tool that helps not only to identify and reduce the privacy risks of data processing but can highlight cases in which data processing should not happen. The ICO has provided guidance on a range of issues in respect of these assessments, including the benefits of conducting privacy impact assessments and practical guidance on the process required to carry one out: see Data Protection Impact Assessments.

How will you tell individuals how you will use their data?

Individuals must be informed how their data will be used and for what purpose(s). This is a requirement of the 'transparency' principle stated in Article 5(1)(a) of the GDPR and commonly fulfilled by providing a 'Privacy Notice'.

Articles 13 and 14 of the GDPR set out the information that must be contained in the Privacy Notice (see the Insert boxes below). Moreover, in order to be compliant, the information must be presented and written in clear, concise language so that it may be easily understood. A Note is provided below (see further insert box) to aid consideration and drafting of a notice for the purpose of ECO flexible eligibility: **please note it is not a definitive list**.

The privacy notice must be provided at the time the data is collected from the data subject or within a reasonable period where the data is collected from a different source[27].

[26] Article 35
[27] Namely, no later than when the data is disclosed onwards to anyone else. Articles 12 to 14 refer.

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

a. the identity and the contact details of the controller and, where applicable, of the controller's representative;

b. the contact details of the data protection officer, where applicable;

c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d. where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

e. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and…

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

a. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

c. where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

d. the right to lodge a complaint with a supervisory authority;

e. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

f. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Article 14

Information to be provided where personal data have not been obtained from the data subject

1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

a. the identity and the contact details of the controller and, where applicable, of the controller's representative;

b. the contact details of the data protection officer, where applicable;

c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d. the categories of personal data concerned;

e. the recipients or categories of recipients of the personal data, if any;

f. that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

a. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b. where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

c. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

d. where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

e. the right to lodge a complaint with a supervisory authority;

f. from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; and

g. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

a. within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

b. if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

c. if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

a. the data subject already has the information;

b. the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or insofar as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

c. obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

d. where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

Note:

Some of the key points the privacy notice should address are:

What is personal data? See paragraph. 2.1 above.

Define what is meant by processing? e.g. Include a statement on the activities related to, performed on or with personal data for the purposes of ECO flexible eligibility.

How is personal data processed in terms of the application process proposed by the local authority for ECO flexible eligibility? e.g. what personal data is collected, for example, and who collects the data? How is the data used? etc.

What is the legal basis for processing the data? See pages 11-16

With whom, including energy suppliers, another local authority delegated to act on behalf of the local authority, and any others, will personal data be shared for the purposes of ECO flexible eligibility? And how will that information be used?

Make reference to the right of the data subject to:

Withdraw their consent;

Have access to their personal data (‘Subject Access Request’);

Raise a complaint: e.g. internally with the LA and externally with the ICO.

The name and contact details of the person within the LA responsible for the administration of ECO flexible eligibility.

Do you have appropriate technical and organisational measures in place for sharing personal data?

The GDPR does not specify the security measures that you must have in place. It requires that you have 'appropriate technical and organisational measures to ensure a level of security appropriate to the risk'[28] and suggests some of the controls that may be appropriate. For example:

- pseudonymisation and encryption of data;
- ability to ensure ongoing confidentiality, integrity and availability of processing systems and services;
- in the event of a technical incident, the ability to restore availability and access to personal data; and
- regular testing of technical and organisational measures.

Illustration

Local authority establishes an online application process for individuals to apply for consideration of their eligibility for flexible eligibility and in requiring proof of eligibility enables applicants to append details relating to, amongst others, their income.

As with any and all data held by the local authority and shared internally and externally, regard must be had to the local authority's internal IT and physical data security policies and procedures, and in the case of doubt, appropriate contact and referral made to the data protection officer/advisor prior to data being processed.

How long may shared personal data be retained – are there any applicable statutory requirements for retention?

While not prescribing retention periods, the GDPR does state that personal data 'which permits identification of data subjects' should be kept 'for no longer than is necessary for the purposes for which the personal data are processed'. Longer retention periods may be justified in the cases of 'processing solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.'

In assessing retention criteria, local authorities should take into account that by virtue of the powers conferred on Ofgem as the ECO Scheme Administrator under article 37 of The Electricity and Gas (Energy Company Obligation) Order 2018, energy suppliers may at any time before 30th September 2022, for audit purposes, be required to produce to Ofgem:

[28] Article 32

- a signed copy of the local authority declaration;
- other information relating to a household's eligibility under flexible eligibility; and
- the relevant URN number of the declaration.

The Administrator does not require energy suppliers to hold or retain these documents or data but stipulates that the energy supplier must be in a position to make such documents and data available to an auditor within required timeframes. It would therefore be for the local authority and energy suppliers to determine an arrangement that would satisfy their individual audit-based requirements in addition to taking into account the justification requirements for such data retention periods under the GDPR. At the same time, local authorities should consider what processes will be required to ensure that data is deleted or destroyed when this becomes applicable, how notification of deletion is to be carried out and to whom the notification is to be sent in those instances where data is shared.

Data Sharing Agreements

A data sharing agreement has always been held to be good practice, ensuring the governance of personal data that is to be shared by detailing, amongst other matters, to what extent third parties may use such data for the purpose and in accordance with the data subject's consent. In light of new data protection obligations placed upon controllers and, for the first time, on processors in their own right, the GDPR takes this requirement and its content further.

2.9 Data Sharing between Controllers and Processors

As between a controller[29] and a processor[30], there **must** be a contract or 'other legal act' in place that at a minimum includes the specific terms set out at Article 28(3) of the GDPR (see next text box).

In terms of the situation where the local authority acts as a controller and for example, engages an external entity on its behalf and under its control and instruction to simply process personal data in relation to the administration of its ECO flexible eligibility application process, the relationship between the two is that of controller and processor. Further information of this form of relationship may be found on the ICO website, which includes a handy checklist dealing with contracts and liabilities between controllers and processors.

[29] Article 4(7): a ''controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.' Regard must also be had to Section 6 of the DPA 2018, which qualifies the definition of 'controller' stipulating that:

'*For the purposes of the GDPR, where personal data is processed only—*
(a) for purposes for which it is required by an enactment to be processed, and
(b) by means by which it is required by an enactment to be processed,
the person on whom the obligation to process the data is imposed by the enactment (or, if different, one of the enactments) is the controller.'

[30] Article 4(8): a ''processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'

Article 28(3)

Processing by a processor shall be governed by a contract or other legal act under [EU or UK] law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

a. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by [EU or UK] law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

b. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c. takes all measures required pursuant to Article 32;

d. respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

e. taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

f. assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

g. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless [EU or UK] law requires storage of the personal data; and

h. makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other [EU or UK] data protection provisions.

2.10 Data Sharing between Controllers and between Joint Controllers

Please note the following must be considered as a subject under advisement and one that local authorities should consider carefully with their legal advisers.

The DPA 1998 defined a controller as 'a person who (either alone or in common with other[s]…) determines the purposes for which and the manner in which any personal data are, or are to be, processed'. Accordingly, it drew a distinction between 'joint controllers' and those who processed data 'in common' with others. Per the interpretive guidance given by the ICO:

- 'jointly': referred to the situation where 'two or more persons act together to decide the purpose and manner of any data processing'; and
- 'in common': referred where two or more persons share a pool of data that they process independently of each other'.

From the perspective of ECO flexible eligibility, it was more than likely that the 'data sharing' undertaken between a local authority and an energy supplier or its representative fell under the umbrella of processing 'in common'.

On the face of it, Article 26 of the GDPR does not expressly refer to processing of personal data 'in common with others' and appears only to be concerned with 'joint controllers'. It states:

'Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them…'.

The phrase: *'determine the purposes and means of processing'* is important to note. If there is a collaboration of this nature, then the controllers will be held to be acting jointly and their respective duties are to be recorded in 'an arrangement'. [31]

From the context of ECO flexible eligibility, the local authority and energy supplier will need to determine whether their processing of personal data falls within the terms enunciated for 'joint controllers' or is distinct. To the extent that it not distinct, then they will be held to be 'joint controllers' and their 'collaboration' and their respective obligations - including who takes the primary responsibility for, inter alia, the transparency requirements - for the purposes of ECO flexible eligibility must be set out in an arrangement.

It is anticipated that the 'arrangement' will, or ought to be, some form of formal agreement. However, given that it must be made available to data subjects[32] something concise and in plain language would seem required. It is also worth noting that notwithstanding the agreement specifying a particular party as primarily responsible for meeting the transparency

[31] Whether the notion of 'controllers in common' is in fact retained and to be applied as part of the new law, appears to be open for debate. Hopefully this is a matter that will be addressed by the ICO in due course.
[32] Article 26(2)

requirements, data subjects will be able to exercise their individual rights against either controller[33].

The ICO has provided detailed guidance on its website that will enable local authorities to assess when they are acting as a controller or joint controller.

Need for an arrangement?

If the local authority and energy supplier are acting as 'joint controllers' then:

- The requirements for an arrangement as set out in Article 26 is applicable.

Accordingly,

- Their respective obligations will need to be clearly defined, including;
    - The provision of information to data subjects about their rights (ss.13(2) and 14(2) refer);
- Be in clear and concise language, so as to be
- Made available (and therefore understood) by data subjects.

If the local authority and energy supplier are acting as independent controllers, then the need for an arrangement is not stipulated. However, in accordance with best practice, a data sharing agreement is advisable. This should take into account:

- a mutual obligation to a comply with the GDPR in respect of the all personal data and processing covered by the arrangement;
- the purposes for which each party will be providing personal data;
- the types of personal data concerned and categories of data subject;
- set out arrangements for subject access requests and for giving effect to the other rights of data subjects;
- that in the data sharing process appropriate organisational, security and technical measures will be taken to:
    - ensure only people with a genuine business need have access to the data;
    - prevent accidental loss, destruction or damage of data;
    - ensure data will be retained securely and deleted once it has been used for the purpose for which it was provided.

Reference should also be made to the ICO's Data Sharing Code of Practice. This is currently under review to take account of the changes made by the GDPR, the DPA 2018 and other

[33] Article 26(3)

legislation as well as taking into account responses received following the ICO's Call for Views on updating the Data Sharing Code of Practice.

Illustration

Under ECO Flexible Eligibility a participating local authority:

Is required to make a Statement of Intent as to the eligibility criteria it will use to determine households eligible for a measure or measures under the scheme;

Must, where applicable, make a statement in writing ('LA declaration') that, in the opinion of the local authority, particular premises are occupied by a household living on a low income in a home which cannot be kept warm at a reasonable cost; or a similar statement that the household is living on a low income and vulnerable to the effects of living in a cold home; and

Must be willing to make the LA declaration available to the energy supplier promoting the installation of (an) ECO measure(s) in that premises; and

Must be willing to confirm that the LA has been consulted on the installation of the ECO measures in that premises.

Participant energy suppliers may use the LA declarations that a local authority makes available to them to help meet their obligations under the ECO3 Order.

As the sharing of data for the purposes of flexible eligibility may not be a direct requirement placed by law on local authorities (legislation places an obligation on energy suppliers), a data sharing agreement will be necessary and the means by which local authorities can restrict the purpose and use of declarations by energy suppliers and/or their intermediaries.

It is to be noted that the information required by the LA from energy suppliers or their installers vis-à-vis measures installed for the purposes of LA Flex reporting, may not be to the same degree required for other schemes operated within the LA. A point to be considered when determining the type and extent of personal data to be shared.

Scenarios

These are illustrative scenarios of data sharing that might occur between a local authority, intermediaries and energy suppliers in the context of flexible eligibility. A local authority will only be able to issue ECO flexible eligibility declarations once it has published a statement of intent outlining how it intends to identify households in fuel poverty or living on a low income and vulnerable to cold.[34]

Scenario 1: Direct customer query

The customer contacts the local authority directly, either to ask about a different service or to enquire about getting support through ECO. The local authority asks the customer some questions to verify their potential eligibility against the local authority's published statement of intent. If they conclude that the customer is eligible, they inform the customer about what support might be available and ask the customer if they agree to their details being passed on to a participating energy supplier. The customer gives their consent. The local authority provides the customer with a privacy notice. There is an information sharing agreement between the local authority and the energy supplier. The local authority shares the customer's information with the energy supplier and makes a statement in writing ('Declaration') concerning the customer's eligibility. This is made available to the energy supplier. The energy supplier, or their intermediaries, contacts the customer to discuss potential measures.

Scenario 2: Third party referral

The customer is referred to the local authority by a third-party organisation, such as a health or social care organisation or a charity working on fuel poverty. The local authority, or third-party organisation, asks the customer some questions to verify their potential eligibility for the scheme. They inform the customer about what support might be available and ask the customer if they agree to their details being passed on to a participating energy supplier. The customer gives their consent. A privacy notice is provided to the customer. There is an information sharing agreement between the local authority and the third- party organisation. There is also an information sharing agreement between the local authority and the energy supplier. The local authority shares the customer's information with the energy supplier and makes a statement in writing concerning the customer's eligibility. This is made available to the energy supplier. The energy supplier, or its intermediary, then contacts the customer to discuss potential measures.

Scenario 3: Supplier-led route

From their existing data, an energy supplier or its intermediary, satisfied that the processing of this data complies with the GDPR[35] and any other applicable legislation, identifies customers who may be eligible for support. The supplier, or their intermediary, would like a declaration from the local authority to confirm this. Having informed the customer of the measure

[34] See paragraph 2.2
[35] Refer to the 'accountability principle' introduced by the GDPR: Article 5(2).

potentially available to the customer under ECO, the energy supplier or its intermediary obtains the direct consent of the customer to pass on their details to the local authority for the purpose of seeking an ECO flexible eligibility declaration from the local authority. A privacy notice is provided to the customer and the customer's details are then passed to the local authority. The local authority checks the customer's eligibility. There is an information sharing agreement drawn up between the local authority and the energy supplier. There is also an information sharing agreement between the energy supplier and its intermediary. The local authority having assessed the customer as eligible makes a statement in writing. The statement is made available to the energy supplier or its intermediary. The energy supplier, or its intermediary, then gets back in contact with the customer to discuss potential measures.

Scenario 4: Local authority held data route

From their existing data, the local authority, satisfied that the processing of this data complies with the GDPR[36] and any other applicable legislation, identifies customers who may be eligible for support pursuant to the terms of their published Statement of Intent and contacts them to inform them of their eligibility and to ask for their consent to pass their details on to a participating energy supplier. Updated privacy notices are provided to the customer. There is an information sharing agreement drawn up between the local authority and the energy supplier and between the energy supplier and its intermediary. The local authority makes a statement in writing and makes this available to the energy supplier or the energy supplier's intermediary. The energy supplier, or its intermediary, then contacts the customer to discuss potential measures.

[36] The identification of individuals from an existing database is processing of data. Accordingly, the local authority or energy supplier, as the case may be, would need to be able to demonstrate that the *re*processing of data satisfies a valid condition under the GDPR.

This publication is available from: www.gov.uk/government/publications/energy-company-obligation-eco-help-to-heat-scheme-flexible-eligibility

If you need a version of this document in a more accessible format, please email enquiries@beis.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.