The ICO exists to empower you through information.

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

The Information Commissioner's response to the public consultation from the Department for Energy Security and Net Zero (DESNZ): *Delivering a smart and secure electricity system: implementation.*

About the ICO

1. The Information Commissioner's Office (ICO) welcomes the opportunity to respond to the '*Delivering a smart and secure electricity system: implementation*' consultation (the **consultation**).

2. The ICO has responsibility for promoting and enforcing data protection and information rights. This includes responsibilities under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA), the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR), the Privacy and Electronic Communications Regulations 2003 (PECR), and the Network and Information Systems (NIS) Regulations 2018.

3. The ICO is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO does this by providing guidance and support to individuals and organisations, and taking appropriate action where needed to address instances of non-compliance.

4. In line with our regulatory remit, our comments are limited to the elements of the consultation that relate to information rights and personal data.

Continued relevance of previous consultation responses

5. The ICO has previously provided input on the development of a smart energy system, most recently through our response to the Department for Business, Enterprise and Industrial Strategy 2022 consultation '*Delivering a smart and secure electricity system: consultation on*

interoperability and cyber security of energy smart appliances and remote load control' (the **2022 consultation**).[1]

6. Although these proposals have progressed to implementation stage since the 2022 consultation, many of our comments in that response remain relevant, in particular:

    - the importance of incorporating data protection into the regulation of Energy Smart Appliances (ESAs) by design (see paragraphs 3 to 10)
    - the need for appropriate technical and organisational measures to ensure that ESAs process personal data securely (paragraphs 38 to 44), and
    - the applicability of the NIS Regulations (paragraphs 45 to 49).

Sharing of tariff data using APIs

7. The '*Tariff data accessibility for flexibility services*' consultation paper[2] seeks views on the potential technical solutions for the tariff data standard, including options to use Application Programming Interfaces (APIs) to enable energy suppliers to share the tariff data items included in the standard.

8. As the consultation paper notes, the intention is for the chosen technical solution to be able to accommodate the use of personal data, such as addresses and MPANs. The sharing of tariff data is therefore likely to involve the personal data of consumers being shared between energy suppliers and with third parties. As a result, any solution will

[1] https://ico.org.uk/about-the-ico/consultations/department-for-business-energy-industrial-strategy-consultation-delivering-a-smart-and-secure-electricity-system/
[2] https://assets.publishing.service.gov.uk/media/663b7cdb1834d96a0aa6d298/smart-secure-electricity-systems-2024-time-of-use-tariff-consultation.pdf

need to comply with applicable data protection rules and regulations, including obligations with respect to the sharing of personal data.[3]

9. Given the challenges around interoperability, data security and managing consent, the ICO's view is that a **Supplier Standard API** is likely to be the most suitable technical approach for the tariff data standard, for the reasons set out in paragraphs 10 to 18 below.

Managing consent

10. Some of the technical solution options for ensuring tariff data interoperability considered in the consultation paper refer to the need to obtain consumer consent to enable tariff data to be sent directly to the ESA. To ensure that good data protection practices are embedded in processing activities and business practices by design, a key consideration should also be each option's capability to obtain and manage consent for the processing of consumers' personal data.

11. Where consent is the lawful basis for processing, that consent must be freely given, specific, and informed in order to be valid.[4] The consumer needs to have a real, transparent choice, and the request for consent must be clear, not bundled up with other terms and conditions in ways that are difficult to understand or could be overlooked.

12. To meet this requirement, suppliers will need to consider how they can provide sufficiently detailed information to ensure that consent is properly informed. This information should include the categories of personal data to be collected, the purposes for which the data is to be processed, the processing activities to be undertaken, and any data sharing with third parties. This is particularly important where the consumer is providing consent when they first interact with a new ESA,

[3] For more information, please refer to the ICO's Data Sharing Code of Practice: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/

[4] UK GDPR, Article 5(1)(a) and 6(1)(a). For more information, see the ICO's guidance on consent: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/consent/

and where the information is delivered via a small built-in digital display, as is the case on many ESAs.

13. Suppliers will also need to consider how ongoing consent and withdrawal will be managed through an ESA. This includes:

    - ensuring that an ESA's controls are designed to enable an individual to decline or subsequently withdraw consent as easily as it is given,
    - ensuring the ESA and API solution are together capable of communicating withdrawal of consent to all third parties, and
    - ensuring that customers who do not consent are still able to access the best tariff deals.

API security

14. As outlined in the ICO's response to the 2022 consultation, organisations need to process personal data securely by means of 'appropriate technical and organisational measures', to protect against accidental loss, destruction or damage.[5] This includes appropriate cyber, physical, and organisational security measures.

15. The consultation paper explores the relative benefits of using standardised and non-standardised API solutions for the management of tariff data, which potentially includes personal data. Relying on non-standardised APIs will likely result in energy suppliers implementing individual, customised data security measures, which may lead to inconsistent security measures being implemented. Inconsistent security measures increase the likelihood of vulnerabilities across the system as a whole, and increase the risk of harm from unauthorised access to or disclosure of consumers' personal data.

[5] UK GDPR, Article 5(1)(f) and Article 32. For more information, see the ICO's guide to data security: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/

16. Non-standardised APIs may also have a negative impact on interoperability - for example, improperly designed security updates to an individual supplier's API could prevent a third party from accessing the relevant data held by a supplier, or communicating with its IT systems.

17. Given these issues, we believe that a standardised API solution is a better solution for helping suppliers implement 'appropriate technical and organisational measures' to process personal data securely. If a non-standardised API solution is selected, it will be important that these security risks are considered and appropriately addressed, to ensure that consumers using ESAs are adequately protected.

18. We would be happy to provide more detailed advice on both managing consent and implementing appropriate security measures, once more details about the specific technical solution(s) being considered are available.

Potential industry code of conduct for load control services

19. Chapter 6 of the '*Licensing regime*' consultation paper[6] discusses the possibility of industry developing a UK GDPR code of conduct covering load control services, and refers to the ICO's role in approving codes of conduct.

20. ICO-approved codes of conduct can provide significant benefits for organisations, consumers, and the public, and the ICO is committed to encouraging their development. Adherence to a code of conduct helps sector participants process personal data of consumers and the public in a transparent and consistent way. Developing a code can also help a sector proactively identify and mitigate common vulnerabilities that their customers face, which increases consumer trust and confidence in the sector as a whole. Codes can also provide a pathway for business-to-business assurance of data protection compliance without ongoing

[6] https://assets.publishing.service.gov.uk/media/661e439ad4a839725cbd3d95/smart-secure-electricity-systems-2024-licensing-consultation.pdf

regulatory involvement, and are usually more cost effective than other mechanisms such as UK GDPR certification.

21. We can provide advice and support to sector participants on developing a code of conduct, including how to meet the necessary criteria and the role of industry in developing and maintaining a code. This would include ensuring access to relevant data protection expertise, identifying and agreeing key data protection issues and compliant solutions, identifying a suitable monitoring mechanism, and developing and obtaining regulatory approval of a suitable monitoring body or bodies (depending on the size of the sector and number and range of membership organisations).[7]

22. If sector participants decide to develop a code of conduct, we would welcome the opportunity to provide more bespoke advice and guidance.

Further consultation with the ICO

23. We would be happy to engage further with both DESNZ and the smart energy industry in relation to the matters covered in this response. We also welcome formal consultation with the ICO under article 36(4) UK GDPR for any proposals requiring primary or secondary legislation that relate to the processing of personal data.

[7] For more information, please refer to the ICO's guide to codes of conduct: https://ico.org.uk/for-organisations/advice-and-services/codes-of-conduct/codes-of-conducts-a-guide/