ICO privacy seals project

Consultation on framework criteria: summary of responses

1. Objective of the consultation

This report summarises the key themes which emerged from the responses to the ICO's consultation on the draft framework criteria (which ran from 3 September – 3 October 2014). The draft framework criteria document is comprised of:

- the principles that must underpin an ICO endorsed scheme; and
- the detailed criteria on scheme requirements.

Proposals for schemes will be assessed by how well they fulfil the framework criteria.

The consultation provided an opportunity for organisations to provide their views on the draft framework criteria document to ensure the ICO requirements for privacy seal schemes are robust, credible and achievable. The ICO sought feedback on the following specific areas of the framework criteria document:

- Roles and responsibilities (of ICO, UKAS and scheme operators);
- The underpinning principles;
- The scope and objectives of the scheme requirements;
- Sustainability of schemes;
- The certification process; and
- The quality criteria for organisations.

We have updated the framework criteria, and accompanying invitation documents in light of the comments received in this consultation.

2. Summary of responses

We received 28 responses; 14 responses came from private sector organisations, mainly from those with a specific privacy or security interest; the remaining responses came from the finance sector (three responses), academics (three), public authorities (five responses) and a telecoms company, a legal firm and a trade / representative body.

The majority of responses were generally supportive of the ICO's approach and confirmed that the proposed approach was consistent with expectations around certification processes.

The themes that emerged from this consultation exercise are consistent with the previous stakeholder feedback:

- Interaction of the ICO's scheme with the European Commission's draft proposals for a new data protection Regulation;
- Limitation of the scheme to cover UK processing only;
- Impact on ICO's regulatory role - including complaints resolution;
- Clarity around the role of United Kingdom Accreditation Service (UKAS).

Two strongly critical responses were received, raising two specific concerns:

- **The rationale for limiting the first invitation for proposals to new schemes only**

ICO response: The ICO has extended the scope of its invitation to allow proposals covering existing schemes to be put forward for ICO endorsement - as long as such schemes are adapted to meet the standards of the framework criteria and under-go the UKAS accreditation process if necessary.

For the first endorsement phase – subject to the number of proposals received - the ICO may choose not to endorse all schemes that meet the criteria. There will be further selection based on the scheme proposals which best meet the criteria and the ICO's broad regulatory objectives and current priorities. This is to enable the ICO to adequately resource and support implementation.

- **A strong recommendation that we should wait until a final text of the proposed EU data protection Regulation is agreed**

following the 26 September leak of the Council's draft text on the Article 39 provisions.[1]

ICO response: The ICO does not share the same concerns about the Council's latest proposals for the provisions on certification mechanisms in Article 39 of the draft Data Protection Regulation (the Regulation). In fact, we welcome the latest Council text, which amends Article 39 to introduce an approach that more consistent with the co-regulatory model proposed by the ICO. Specifically, Article 39a introduces the use of certification bodies who are accredited by the supervisory authority and/or the National Accreditation Body named in accordance with Regulation (EC) 765/2008 of the European parliament and the Council of 9 July 2008) (ie, the United Kingdom Accreditation Service).

We do not agree that we should delay our progress and intention to introduce a privacy seal scheme in the UK. We are taking this opportunity to build the ICO's expertise in an area that will become significant in the near future because of the Regulation. Ideally, we would like to see ICO endorsed schemes to be consistent with the provisions at the European level once the Regulation is in force, and are watching developments closely.

At the same time, there is a risk our plans for a privacy seal won't fit with the requirements in the final provisions for a European wide seal. But there is no suggestion that a national level seal will be made redundant either.

3. Key themes

This section summarises the key themes that emerged from the consultation responses.

The ICO's regulatory role

There were a range of comments on various aspects of the ICO's regulatory role and its relationship with scheme operators.

Jurisdiction and the European Commission's proposal for a new General Data Protection Regulation

In line with previous consultation exercises, many comments were received on the decision to limit the ICO's endorsement to the UK, and how the scheme will interact with the provisions in the new Regulation. Comments included:

[1] Presidency Note to COREPER <http://www.statewatch.org/news/2014/oct/eu-council-dp-reg-chap-IV-12312-rev3-14.pdf>

- Where processing occurs outside the ICO's jurisdiction – clarity is required on whether the scheme is applicable for international organisations operating in the UK but processing data outside the UK. From the document it is assumed data must be processed in the UK and the scheme can only apply to an international company's UK operation.

- Limiting the coverage of the scheme to the processing of personal data in the UK may not be aligned with the objectives and scope of the new EU Regulation. With the new EU regulation coming into force, the expectation would be for companies to certify processes against the requirements and scope of the new Regulation. Hence, a mechanism for allowing seals to be used / applied in other jurisdictions may need to be introduced.

- More explicit recognition of EU legislation.

ICO response: The ICO confirms that it will only endorse schemes in so far that they cover the processing of personal data subject to UK data protection law and accordingly, within the limits of its supervisory powers.

A scheme operator may wish to replicate its scheme in another jurisdiction, or for its scheme to be used for processing that occurs outside of the UK. This will be possible, but the ICO will not have a role in relation to any processing that is outside the UK. The UK data protection authority can only operate within the limits of its own jurisdiction – it cannot endorse a scheme that is subject to other states' data protection legislation.

It is unlikely that, in the absence of legislation, that there would be mutual recognition between data protection authorities where schemes are based on their own national laws' requirements.

Link to new Regulation

We are using this opportunity to build ICO expertise in an area that is likely to become more significant in the near future because of the provisions at Article 39 of the draft Regulation. As highlighted above, the ICO's proposed co-regulatory approach is very similar to provisions added in the Council's latest texts, which envisage a role for independent certification bodies accredited by the national accreditation body. Ultimately, we hope that ICO endorsed schemes will be consistent with the provisions in the Regulation, and we expect potential scheme operators to consider this when forming their proposals.

We recognise there is a risk ICO endorsed schemes won't fit with the requirements in the final provisions for a European wide seal. But there is no suggestion that a national level seal will be made

redundant. It will still be a useful tool in fulfilling the Information Commissioner's duty to promote compliance and good practice.

Scheme operator and interpretation of data protection compliance

Some respondents expressed concern about:

- the expertise of the scheme operator to assess data protection compliance; and
- consistency in the interpretation of the law if there are a number of scheme operators.

ICO response: Our aim is to overcome these challenges by setting a high minimum standard at the outset through the robust framework criteria and quality criteria for organisations. The framework criteria mandate that the schemes' objectives must be aligned to ICO guidance and codes of practice where relevant, and must reflect our broad regulatory objectives. We hope this will ensure a consistent minimum standard.

We will only endorse scheme operators that demonstrate they are committed to maintaining and encouraging a high level of data protection compliance. Any scheme operator who is found not to be upholding the standard will risk revocation of the ICO's endorsement.

Dealing with complaints

There was some perceived confusion about the proposal for the scheme operator to deal with complaints or concerns about an organisation's non-compliance with the scheme. Several respondents expressed concern about the risk of the ICO delegating its legal duties to the scheme operator. Comments included:

- The consultation advises that scheme operator will deal with complaints or concerns about an organisation's non-compliance with the scheme […] If the scheme operator is responsible for dealing with these complaints then this would interfere with the ICO's role and create uncertainty for the organisation concerned. This could lead to situations where [two] contrasting rulings could be made in respect of the same complaint.

- [The] ICO should accept and investigate public complaints about scheme otherwise [there is] no effective whistle-blower mechanism

if a scheme is failing. Costs of investigation should be passed onto schemes where schemes operate for-profit basis.

- There is likely to be some consumer confusion, resulting in people complaining to the provider when a complaint to the ICO would be more appropriate.

ICO response: The scheme operator must deal with complaints about non-compliance with the scheme by certified organisations.
We see advantages for consumers having their concerns dealt with at the source by the certified organisations and the scheme operator where possible. This approach should lead to more expedient resolution of complaints about compliance with the scheme.

The ICO will not have a role in complaints about non-compliance with a scheme, unless a complaint is about a breach of the DPA and the issue/concern raised by an individual is not resolved directly by the certified organisation and scheme operator. The ICO will have a consultative role, whereby the scheme operator can seek advice about complaints and legal compliance and direct the certified organisation to self-report breaches of the law. The ICO will work with the scheme operator to ensure that we have consistent outcomes in cases where this may be appropriate.

Inevitably, there will be overlap where a breach of the scheme will be a breach of the DPA. Ideally, we would like to see the issue or concern resolved by the certified organisation where possible. The ICO does not believe that this will create conflict with its statutory role. The objective of the co-regulatory approach is to encourage data controllers to take a more accountable, pro-active position in relation to compliance, ensuring they are receptive to concerns raised by consumers.

This approach fits with the ICO's strategic approach to complaints handling - encouraging performance improvement by data controllers – putting the onus on them to remedy issues at the source as soon as errors/issues/breaches come to light – without intervention from the regulator where possible. None of this precludes an individual from complaining directly to the ICO about a breach of the law.

Ultimately, we are aiming for the most efficient and effective outcomes for consumers – in some cases this will mean concerns being dealt with appropriately by the data controller, and in others, through complaints to the ICO.

The role of the United Kingdom Accreditation Service (UKAS)

Many respondents requested more information about the technical details of UKAS's role. For example:

- What ISO/IEC standard UKAS will be accrediting against;
- When the scheme operator should apply for UKAS accreditation; and
- Clarity / confirmation that UKAS accreditation is required of the organisation which is responsible for the audit/certification process i.e. either the scheme operator or their audit partner.

ICO response: There was a lack of detail in the draft framework criteria around the UKAS accreditation process and requirements. These issues have been addressed in more detail - in consultation with UKAS - in the accompanying invitation documents, which will be published alongside the framework criteria.

The latest draft of the invitation document :

- explains the status and role of UKAS;
- specifies the relevant ISO/IEC standard that scheme operators will be accredited against (ISO/IEC 17065 *Requirements for bodies certifying products, processes and services*);
- clarifies that UKAS accreditation is relevant for the body which carries out the audit function for the purposes of the certification (whether that is the scheme operator, a partner organisations or a separate organisation that is appointed to carry out this function).
- explains that a scheme operator / relevant body does not need to have existing UKAS accreditation in order to put forward proposals; and
- clarifies that if a scheme operator / relevant body does not have UKAS accreditation, it must be sought once the ICO has provisionally indicated that it will endorse the specific scheme.

This will make the role of UKAS and its relationship with the ICO and the scheme operators clearer to potential applicants.

ICO endorsement - revocation

The section on the ICO's endorsement and circumstances when it may be revoked generated many comments. Comments included:

- Notifying the scheme operator to give them an opportunity to rectify any issues within a limited timeframe before revoking endorsement or clarify that revocation is subject to an appeal.

- Need for transparency – firstly around the protocols for revocation, and secondly around informing the public.

- Further consideration should be given to the impact on certified organisations if the ICO withdrew its endorsement of the scheme operator – mainly around the fees that have been paid by such organisations.

- Further consideration should be given to the liabilities that will be incurred by scheme operators.

ICO response: The consultation responses raised some valid comments on the complex issues around the process for revoking ICO endorsement, and the various implications for involved parties.

We are committed to transparency about the processes involved in our endorsement of schemes and will publish the protocols around potential revocation. The invitation documents will provide more detail about the process of revocation – and make clearer that the ICO will provide opportunities for scheme operators to:

- resolve issues where appropriate before withdrawing its endorsement; and
- review the final decision to revoke endorsement before public announcement.

We are currently exploring the potential implications for certified organisations should revocation take place and the legal issues that might surround this. We expect scheme operators to consider this as part of their proposals.

We emphasise that revocation of ICO endorsement will be a last resort in specific limited circumstances.

Proposed ICO costs recovery

Several respondents expressed concern about the potential implications of the ICO recovering costs. Concerns mainly related to the lack of detail provided and the implications for potential applicants' business planning.

ICO response: The ICO is keen to ensure that it is not put at a financial disadvantage for the support it offers to the scheme operators, particularly in the context of restricted resources. It is already placing significant investment in the development of the project in terms of branding and marketing.

The ICO is only permitted to charge on a costs recovery basis for specific relevant services, defined in the Protection of Freedoms Act 2012 as providing copies of materials, training or conferences. The ICO is currently

liaising with the Ministry of Justice to explore the possibility of implementing of secondary legislation to expand the definition of 'relevant services' to allow the ICO to recover costs incurred as a result of endorsing privacy seal schemes.

More information about what about the types of costs that the ICO may recover will be provided in the invitation documents. We envisage that ICO costs recovery is likely to be limited to:

- ICO staff time in providing advice and assistance to scheme operators; and
- the licence for use of the seal and associated branding.

We may set a maximum amount that can be charged to scheme operators to help them with business planning. While the amount charged will need to reasonably cover the ICO's costs, it will not be prohibitive or unfair for scheme operators.

Obviously, these are some provisional thoughts and are subject to change.

Marketing and branding

Respondents welcomed the ICO's proposals around its involvement in marketing and branding the schemes, with several stressing the importance of visible ICO association. Some respondents suggested that the seal design must be agreed by ICO and that it is essential to implement a set of branding guidelines to prevent conflict between multiple scheme operators.

ICO response: The ICO welcomes this feedback and has developed its branding strategy since the consultation was initiated.

The ICO will licence the use of a single, universal seal to be used by endorsed schemes. The seal design is being currently being developed by the ICO. We are exploring the potential of trade-marking the seal logo. This will also the ICO to licence the use of the seal in in accordance with guidelines set out by the ICO.

As previously indicated, the ICO is committing to working in partnership with scheme operators to promote and market schemes.

Underpinning principles

Advantages

Respondents welcomed:

- The focus on good practice – rather than just compliance with the letter of the law.

- That the scheme is not expected to cover all aspects of DP compliance.

- The strong focus on ensuring ICO endorsed schemes are relevant to consumers.

Disadvantages

Several common themes emerged from the consultation responses:

- UK focus is understandable, but should be careful not to exclude organisations that are based in the UK but operate internationally from being encouraged to participate.

- Three respondents had reservations about limiting ICO endorsement to new schemes.

- Several respondents put forward that 'personal data issues' was vague or difficult to specify, and suggested focusing on outcomes.

- Conflict between saying that the scheme should address issues that are relevant to a broad range of people; but focus on 'a particular product, process or service'. Scheme requirement 1e says it could be applicable across multiple sectors, and scheme requirement 4d says it should 'have the potential to be scaled across other sectors, products, processes or service'.

ICO response: As indicated earlier in the paper, the draft framework has been redrafted to reflect the extension of the scope to allow existing schemes to be put forward for ICO endorsement. We have also clarified our approach of limiting ICO endorsement to schemes to the extent they cover processing of personal data subject to UK data protection law. We accept this may discourage some data controllers that operate on a multi-national level from applying to be certified.

We have made further amendments to clarify the specific issues raised above. We have removed the ambiguous references to 'personal data issues'. We have explained that the scheme must have a clearly defined audience – whether it is a multi-sector scheme or focused on a more niche area – we think that there is room for different types of seal schemes to suit different types of processing and consumer audiences.