Framework criteria for an ICO endorsed privacy seal scheme

Purpose of the framework criteria

This document provides the framework that proposals for an ICO endorsed privacy seal scheme must follow. The document is structured as below:

- Section 1 explains the ICO's role in endorsing a scheme and how it will work with the scheme operator.
- Section 2 sets out the underpinning principles for an ICO endorsed scheme.
- Section 3 provides the framework criteria for proposals.

Applicants must ensure their proposal for a scheme:

- is consistent with the ICO's broad regulatory objectives;
- demonstrates how it fulfils the 'underpinning principles' for an ICO endorsed scheme (see section 2); and
- addresses each of the scheme requirements using the guidelines (see section 3).

While the framework and principles provide clear guidelines and a minimum standard that applicants must meet, they have been designed to allow for flexibility to encourage innovation and development.

1. The ICO's endorsement

1.1 ICO endorsement

The ICO will endorse at least one scheme for a minimum of three years and will review all endorsed schemes in the final year. The review will examine whether the scheme continues to meet the framework criteria and whether the scheme operator has maintained its UKAS accreditation. The ICO will continue to endorse the scheme providing these conditions are met and there are no other factors that make the scheme unviable or mean endorsement from the ICO would be inappropriate.

ICO endorsement is separate to UKAS accreditation. Achieving UKAS accreditation is a condition of gaining ICO endorsement. The ICO will participate in the UKAS accreditation process by offering technical expertise and advice to UKAS.

The ICO will monitor general progress of the scheme throughout the three year period. This will be separate from the processes carried out by UKAS for the purposes of official accreditation.

The ICO reserves the right to endorse additional privacy seal schemes in different areas at any time, but would not expect to endorse schemes with significant overlaps in scope.

The ICO may recover costs from the scheme operator where appropriate, for example where the certification scheme generates a profit.

1.2 Revocation of ICO endorsement

The ICO will have the power to revoke its endorsement of a scheme in the following circumstances:

- the scheme no longer meets the guidelines set out in the 'underpinning principles' or framework criteria;
- UKAS accreditation ceases for any reason; or
- any other general failing or action by the scheme operator or the scheme which means it is unfit for ICO endorsement. This could include the scheme operator breaching information rights law.

The ICO will provide proper notice to the scheme operator when it has concerns relating to its endorsement of the scheme.

1.3 Operation of the scheme

The scheme operator takes responsibility for the day-to-day operation of the scheme and retains ownership of the scheme. It is responsible for the general administration of the scheme including:

- its own liabilities and indemnities associated with the operating the scheme; and
- ensuring it has the necessary resources required for the successful delivery of the scheme throughout the period of the endorsement.

The ICO will not provide the scheme operator with additional resources, including staff or funding, to support the day-to-day operation or administration of the scheme.

The scheme operator will be the contact point for queries about the scheme. We expect complaints or concerns about non-compliance with the scheme to be directed to and dealt with by the scheme member and scheme operator. Individuals will still be able to complain to the ICO directly if their concern with the scheme equates to a breach of the Data Protection Act (DPA) or the Privacy and Electronic Communications Regulations (PECR). The scheme operator must report the complaints it has received about the operation of the scheme to the ICO.

1.4 ICO's regulatory role

The ICO's statutory responsibilities, as set out in the DPA, will not change as a result of the scheme. The ICO cannot hand over any of its regulatory responsibilities to the scheme operator or any other body.

In line with the ICO's general complaints handling process, in cases where a clear and serious breach of the legislation has taken place, the ICO will take direct action on the specific concern raised. If the ICO decides that there has been a serious failure to comply with the law, it will provide advice and support to help ensure the organisation gets it right in the future. If an organisation isn't taking its responsibilities seriously, the ICO may also take enforcement action. In the most serious cases, we can serve a monetary penalty of up to £500,000.

Certified organisations must continue to comply with their obligations under the Data Protection Act.

1.5 Promotion of the scheme

The ICO will only have arms-length involvement in the day-to-day operation of the scheme. However, the ICO is committed to working with the scheme operator in the marketing and promotion of the scheme for the full period of its endorsement. The ICO will work with the scheme operator on:

- the branding and design of the seal;
- the launch of the scheme;
- public awareness campaigns throughout the endorsement period; and
- working with relevant representative and trade bodies, consumer groups and government agencies where appropriate to maximise support and recognition of the scheme.

The scheme operator will still need to ensure that it has the resources in place to carry out all necessary branding, marketing and promotion.

2. Underpinning principles for an ICO endorsed scheme

Applicants must make sure that their proposals address the following principles.

The scheme must:

1. have privacy and data protection as its core focus;
2. cover the processing of personal data in the UK;
3. be a new scheme, rather than an existing certification scheme;
4. cover personal data issues that are relevant to a broad range of people;
5. demonstrate a positive approach to the adoption of good practice in information rights, rather than just compliance with the letter of the law;
6. provide evidence to show that there is a demand for the scheme in the area proposed;
7. should not be a 'test' of every aspect of data protection compliance; and
8. will support the objectives in the ICO Information Rights Strategy and the current ICO plan (2014-2017).

The ICO will look favourably on scheme proposals that:

9. have a clear focus to ensure the scheme is manageable and that its scope and function is clear to individuals; for example, by providing certification of a particular process, product or service, or limited to a specific sector; and
10. demonstrate how their approach and principles could be extended in the future to apply to other areas, for example, to other products, services, processes or services.

3. The framework criteria – scheme requirements

The framework criteria explain the key issues relating to the administration of the scheme, the actual requirements of the scheme and some quality criteria for the scheme operator. There will be some overlap with the principles in section 2. Proposals must address each of the scheme requirements.

Applicants must provide evidence and explanations to support their proposal.

	Proposals for an ICO endorsed scheme: issues to cover	Scheme requirements - guidelines
1	**SCOPE OF THE SCHEME**	a. Is a **new** privacy certification scheme.
		b. Covers the **processing of personal data in the UK**.
		c. Is **consumer facing,** promoting consumer trust and consumer protection.
		d. Focuses on a particular **product, process or service**.
		e. **Has a clearly defined target audience**. Explains: - the target organisations for certification; - the target consumers; and - the realistic level of applications. Schemes can target organisations in the public and private sectors. They can also be limited to a particular sector or applicable across multiple

		sectors.
		f. **Presents a case** for certification in the chosen area.

2	**OBJECTIVES OF THE SCHEME**	**a. Defines the data protection responsibilities and privacy practices** the seal scheme will cover. This should be aligned to published ICO guidance and codes of practice, where relevant.
		b. **Defines the processing practices** which will be covered by the scheme.
		c. **Monitors constantly evolving privacy and technology issues** and updates the scheme's requirements as necessary.
		d. **Improves data protection compliance** in the specific area.
		e. **Benefits consumers** in respect of their information rights. Explain desired outcomes for consumers.
		f. Complements applicants' **existing data protection policies or procedures** and does not require significant changes to organisations' other existing policies.

3	**CERTIFICATION – INCENTIVES FOR ORGANISATIONS**	a. Provides clear **incentives for scheme members**.
4	**SUSTAINABILITY OF THE SCHEME**	a. **Includes details of the timescales** for implementation, including the expected length of each phase in the certification process - assessment, awarding, length of certification.
		b. Provides **costs to scheme operator** and a **business case** for financing the scheme. Include: - costs of setting up the scheme; - detail about number of staff and roles; - ongoing costs of operating the scheme; and - whether the scheme is revenue generating or non-profit making.
		c. Sets out the **commercial viability** of the scheme including: • an explanation of how the scheme will be commercially viable; • information to explain how the proposal strikes a balance between the need for a commercial and affordable scheme, with ensuring that the scheme is rigorous enough to ensure credibility; and • details of the number of organisations that need to be signed up to make a profit, or cover overheads if the scheme is not-for-profit.
		d. Provides a **marketing and promotion strategy** to improve public awareness of the seal and attract applicant organisations while making the seal visible to consumers. Please include a forecast analysis showing the targeted number of sign ups and the subsequent

		potential reach to consumers.
		d. Explains the scheme's **longer-term objectives**. Remember, in the longer-term, the scheme should have potential to be scaled across to other sectors, products, processes or services. The scheme could be operated by more than one party.

5	**TRANSPARENCY & ACCOUNTABILITY**	a. Makes the certification **scheme requirements** - including criteria - and other relevant information **publicly available**.
		b. Ensures **appropriate confidentiality** practices are in place. We do not expect information about applicants who are not approved or certified to be disclosed publicly, or to the ICO.
		c. **Discloses details of any business interests** that could be potentially linked to the operation of the certification scheme. For example, provision of data protection audit services, or training.
		d. Includes information about the scheme operator's acceptance of **liabilities and ability to support legal proceedings** in the event of legal action.
6	**CERTIFICATION - INITIAL ASSESSMENT**	a. Includes **measurable, realistic and robust requirements** that the certification scheme is able to meet.
		b. Provides a thorough and robust **explanation of the assessment process**.
		c. Explains why the certification process is **efficient and not burdensome** for scheme operator or the applicant organisation.

7	**CERTIFICATION – AUDIT AND REVIEW – MINIMUM STANDARDS**	a. Has **monitoring, audit or review processes** in place. There must be an appropriate level of regular audit and review as part of this practice.
		b. Provides details on **triggers for ad hoc audit reviews**. For example: • where a certain number of complaints about non-compliance with the scheme are made; • where intelligence suggests an organisation is not complying with the schemes; or • where an organisation changes its practices in a way which has privacy implications.
		c. Explains the process of **authentication or verification of the seal** to protect value and reputation of the scheme. This should include: - a register of scheme members; - the processes in place to prevent misuse of seal; and - allows for consumers to check what the seal is and whether it is valid.
8	**CERTIFICATION – COMPLAINTS**	a. Includes a commitment to **deal with complaints from individuals** about non-compliance with the seal scheme. The applicant must ensure a **clear complaints process is in place** that explains the responsibilities of the involved parties. **Complaints resolution must be fair and proportionate** and have credibility with the public and the organisations using the seals.
		b. Makes it a condition of certification that **scheme members self-report serious or recurring data breaches to the ICO**.

		c. Has a process in place to inform the ICO if an organisation fails to resolve a serious or recurring breach or refuses to self-report.
		c. Provides **clear guidelines for when a seal might be revoked.** This should cover: - when the requirements or standards for certification are no longer met; - when low level concerns remain unresolved; - when serious or recurring breaches occur; and - any other appropriate factors which will mean that an organisation is not fit for certification.
9	**CERTIFICATION – FEES**	a. Provides details of the **charging model** for the scheme. This should explain: - how fees are determined; - provide a certification fee and breakdown of any other costs to scheme applicants; and - any other associated costs if a scheme applicant is not successful and needs to reapply.
10	**CONTINGENCY – REVOCATION OF ICO ENDORSEMENT**	a. Provides a contingency plan if the ICO revokes its endorsement.
		b. Includes information about legal liabilities.
11	**INTERACTION WITH EXISTING STANDARDS AND SCHEMES**	a. Explains how the scheme **complements - rather than replacing or duplicating - existing standards** or schemes
		b. Shows how the scheme brings **benefits** in addition to those offered by existing schemes.
		c. Demonstrates how the scheme is broadly **compatible with international standards and other existing and international schemes**.
		d. Sets out the existing schemes that the proposed scheme will link with.

Quality criteria for organisations		Desirable requirements
1	**PROFICIENCY**	Experience in providing a similar service.
		Experience in advising and working with organisations on issues of business or industry compliance and regulation.
		Experience of the certification and standards process.
		Appropriate legal and technical expertise.
2	**KNOWLEDGE**	Understanding of UK and European data protection law and information rights issues.
		Understanding of regulatory compliance environments.