Regulatory Sandbox Final Report: Seers

A summary of Seers' participation in the ICO's Regulatory Sandbox

Date: October 2021

Information Commissioner's Office

Contents

1. Introduction

1.1 The ICO introduced the Regulatory Sandbox ('Sandbox') service to support organisations who are developing products and services that use personal data in innovative and safe ways and where such products or services deliver a potential public benefit.

1.2 The ICO initially launched the Sandbox as a beta phase, for an initial group of participant organisations during 2019-2020. In August 2020, the ICO re-opened the Sandbox with a focus on projects involving one of two themes, children's privacy focusing around operationalising the ICO's Age Appropriate Design Code (AADC), also known as the Children's Code, or data sharing. The ICO stated projects submitted should be at the cutting edge of innovation and may be operating in particularly challenging areas of data protection, where there is genuine uncertainty about what compliance looks like.

1.3 Organisations who were selected for participation in the Sandbox following its reopening have had the opportunity to engage with us; draw upon our expertise and receive our advice on mitigating risks and implementing 'data protection by design' into their product or service, whilst ensuring that appropriate protections and safeguards are in place. Seers was one of the candidates selected for participation in the Sandbox after it re-opened.

1.4 Seers provides a privacy and consent management platform to help companies become compliant with UK data protection legislation (ie the UK General Data Protection Regulation and the Data Protection Act 2018). In the Sandbox, Seers has been working to enhance its Consent Management Platform (CMP) in order to provide consent management for its clients in a way which respects children's privacy. Their Child Privacy Consent Management Platform (CPCMP) aims to enable children, or their parents or guardians dependent on their age, to provide informed consent for the child's data to be processed by the cookies and scripts operating on the website they are visiting. Before the end user accesses the website's content, the CPCMP gives the end user a chance to self-certify their age and then delivers age appropriate messaging about the cookies and scripts used on the client website.

1.5 Seers' aim in producing the CPCMP is to support their clients in conforming with the ICO's Age Appropriate Design Code (AADC), also known as the Children's Code, and to ensure that children are safer online. As such they applied to enter the ICO's Sandbox. Seers were accepted into the Sandbox on 6 November 2020 and a Senior Case Officer was appointed[1]. The Senior Case Officer conducted a scoping call with Seers on 27 November 2020 to gain an insight into the organisation and to begin formulating the objectives and tasks of Seers' Sandbox plan.

1.6 Following the call in November 2020, the ICO and Seers agreed the following objectives for Seers Sandbox engagement:

- **Objective 1:** Seers and the ICO are to work together to ensure that the CPCMP consent banner collects consent in a compliant manner (ie in a manner which complies with the UK GDPR and conforms with the AADC).
- **Objective 2:** The ICO will provide steers on key data protection issues to support Seers in their development of the CPCMP.
- **Objective 3:** The ICO will provide steers on Seers development of 'phase 2' of the CPCMP tool which includes a third party age verification feature.

1.7 The content of the Sandbox plan was agreed by Adnan Zaheer, the CEO of the Seers Group, and the ICO on 27 January 2021.

1.8 In June 2021 Seers and the ICO completed the last piece of work detailed in Seers' Sandbox plan, bringing Seers' participation in the ICO's Sandbox to an end.

[1] Please note Seers' Sandbox participation, and the advice provided by the Sandbox Team, focussed solely on Seers' CPCMP, not on their original CMP product. The ICO is looking into the use of CMPs separately to the Sandbox and will publish recommendations based on its findings in the future. Organisations operating CMPs should check the ICO's website regularly for updates on this work.

2. Executive summary

2.1 Seers' Sandbox plan focussed on the ICO providing advice to Seers about how their CPCMP should operate in accordance with the standards set out in the ICO's AADC. The CPCMP product aims to collect informed and compliant consent from website users for cookies and other scripts in operation on Seers' clients' websites. The CPCMP does this by asking a website user to self-certify their age when they first access the website and then, based on the age group selected by the user, informs the user about the cookies and scripts in operations before asking for their (or their parent or guardian's) consent for the processing to take place.

2.2 In Seers' Sandbox plan the following three objectives were agreed with the organisation:

- **Objective 1:** Seers and the ICO are to work together to ensure that the CPCMP consent banner collects consent in a compliant manner (ie in a manner which complies with the UK GDPR and conforms with the Age Appropriate Design Code).
- **Objective 2:** The ICO will provide steers on key data protection issues to support Seers in their development of the CPCMP.
- **Objective 3:** ICO will provide steers on Seers development of 'phase 2' of the CPCMP tool which includes a third party age verification feature.

2.3 During Seers' participation in the Sandbox, we considered a wide range of data protection issues in order to achieve the three objectives outlined in their Sandbox plan, these included:

- **Is Seers a controller or processor?** The ICO reached the view that in the context of processing undertaken by the CPCMP only, Seers was likely a processor. The ICO reached this decision as even though they are providing technical input into the consent collection method utilised by their clients, they are doing this in their capacity as a technology provider and are only processing personal data on the behalf of their clients for the purposes of maintaining a record of

the consent provided. Please note that this finding applies to Seers itself and is not to be taken as a general position regarding all CMPs, or all CMPs that implement some form of age-declaration stage for the purposes of AADC conformance. As such Seers should ensure they are aware of and comply with their obligations as a processor.

- **Can Seers provide their clients with a standardised policy document?** The ICO formed the view that in theory Seers could produce a standard form of words for their clients to use in their privacy information, which clearly explains how the CPCMP will process personal data. However, as Seers' clients are likely to be data controllers, they would not be obligated to adopt this wording as such compliance decisions, including in relation to determining the wording of transparency and processing notices, are the sole duty of the controller.

- **What content should be blocked by the CPCMP?** The ICO informed Seers that the question of whether or not content should be blocked will likely depend on the nature of the content of Seers' clients' websites. It is likely that each client will need to assess this on an individual basis and make their own decision. However, Standard 7 of the AADC, default settings, details the importance of default privacy settings for children. As such, it would be up to Seers' clients to determine if children are likely to access their website and the appropriate privacy settings for their audience.

- **What level of control should the CPCMP offer end users?** Seers were informed that it is likely that Seers and their clients should offer granular controls depending on age of the end user. However, Seers should also take into account Standard 7 of the AADC, default settings, which discusses default settings and should start from the position of enabling high privacy settings by default.

- **Is CPCMP a cookie wall?** The ICO were unable to form a firm view on this matter due to limited information about how the final CPCMP product would function in practice. Seers were informed that if users of websites with the CPCMP enabled were still allowed access to the substantive content of a website if they did not consent to cookies, it is likely that the CPCMP would not be classed as cookie wall.

- **Will Seers need to gather parental consent?** The ICO informed Seers that if Seers' clients were using consent as their basis for processing personal data, then it is likely they would need to obtain parental consent for data subjects aged 12 and below in the UK, unless the client's website is providing preventative or counselling services.
- **Would it be appropriate for Seers to use a third party age verification check in the CPCMP?** Seers were advised that, dependent of the level of risk associated with the content of a client's website, it is likely that a third party age verification check, or other suitable age verification method, would be appropriate to use (ie the more sensitive a website's content the greater the necessary assurance of the end user's age would need to be). Seers have communicated their intention to the ICO to include some form of age assurance technology in a later version of the CPCMP.

3. Product description

3.1 As noted previously in this document, Seers' CPCMP aims to enable children, or their parents or guardians, dependent on their age of the child, to provide informed consent for their data to be processed by the cookies and scripts operating on the website the child is visiting. The CPCMP does this by changing the way website users provide consent for the cookies and scripts present on a website, replacing a single banner with layers of banners to ensure that website users are provided with age appropriate information about how their personal data will be processed so they can provide informed consent.

3.2 Currently, Seers' CPCMP is believed to feature the four following layers of banner:

- **Layer 1: Self certified age verification**
  This banner asks website users to select their age range (ie are they aged between 0-5 years, 6-9 years, 10-12 years, 13-15 years, 16-17 years or 18+ years).

- **Layer 2: Parental consent required**
  If a website user indicates that they are under 13 years of age (ie the age of data protection consent mandated by the DPA18) they will be taken through to the second layer of the CPCMP which, dependent on the website's settings, will either:
    a. indicate that they are too young to access the particular websites content altogether[2], or
    b. explain that cookies are in use on the website, describe in general what cookies are and request that the child hands the device to their parent or guardian. Parents and guardians will then have to select a 'I am a Parent/Guardian' button the banner to proceed to the next layer.

- **Layer 3: Request for consent**
  When they consent to processing, website users, or their parent or guardians, will be given age appropriate and informative messaging. This messaging will be different for each age group (eg children aged 13-16 will receive more simplified messaging, which aims to educate the users about what cookies are while asking for their consent. Whereas users aged 18+ will receive more formal, but similarly informative, messaging). Website users will be given the option to 'Accept All', 'Manage' or 'Reject All' cookies on this banner.

[2] Please note the ICO and Seers have discussed different use cases for Seers CPCMP and the ICO have advised the organisation that as the CPCMP currently uses a self-certified age selection which provides only minimal assurance of an end users age, it would not be appropriate to deploy the current CPCMP on websites with any age sensitive content. Seers have stated that they plan to include a third party age verification/estimation as part of Version 2 of the CPCMP which they will develop after their participation in the Sandbox has concluded.

- **Layer 4: Cookies management**
  This final layer will only be shown to website users (or their parents and guardians) who select the 'Manage' button on the previous layer. They will be presented with a list of the cookies and scripts in operation on the website and be able to select which cookies they will allow to run and/or not[3].

3.3 The ICO understands the personal data processed by the CPCMP is minimal, including only the IP address and a record of the end user's consent.

4. Key data protection considerations

4.1 Seers' Sandbox participation focused on its development of the CPCMP and in order to aid Seers with this work, the ICO and Seers agreed the objectives in Seers' Sandbox Plan, the details of which are outlined below.

4.2 An in-depth summary of the work undertaken to complete the objectives outlined in section 1.6 is provided below.

Objective 1: Seers and the ICO are to work together to ensure that the CPCMP consent banner collects consent in a compliant manner (ie in a manner which complies with the UK GDPR and conforms with the AADC).

4.3 In order to complete Seers' first Sandbox objective, Seers provided the ICO with a copy of their Software Requirement Specification (SRS) which outlined their initial design for the CPCMP. Over the course of Seers' Sandbox participation, the

[3] Please note all website users will be able to access this layer at any point during their active use of the main website (eg after deciding whether or not to consent to the use of cookies) by clicking on the settings button which is believed to be a gear icon shown on the bottom right of the webpage.

ICO analysed the wording of Seers' consent flow (ie the process around providing relevant information to end users, seeking and then obtaining their consent) and offered suggestions which helped Seers to iterate upon the design of the product[4].

4.4 The ICO thought that Seers' use of images, and layered banners in the CPCMP was positive as it is in the spirit of the principles of prominence and accessibility outlined in Standard 4 of the AADC, transparency. As they continue to iterate upon the banners used outside of the Sandbox, Seers should ensure that the substantive content of their banners features as early as possible in the chain of interactions with the end user (ie Seers must ensure important information is not hidden in a layer which end users are unlikely to read).

4.5 For the parental consent user journey, the ICO advised Seers to create more friction between the child using the platform and the parent or guardian granting consent, as the user story for this suggests that the CPCMP immediately asks a parent or guardian if they give consent after a child has indicated they are under 13. The AADC recommends prompting a child to go and get the support of an adult as an initial step, and it may be helpful to consider ways to build in measures to increase Seers' confidence that a child is not pretending to be their parent (eg asking for the parent's age and then year of birth to corroborate, or similar information).

4.6 Within the last version of the Seers SRS provided to the ICO, the consent banner states that cookies are used by website providers to enhance the users experience when using the website. The ICO have raised concerns with Seers that the term "enhancing experience" is not specific enough to ensure compliance with Regulation 6 (2)(a) of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). Seers should ensure that any phrasing it uses in its consent banners meets the UK GDPR consent standard, ICO guidance on this topic (below) provides advice on how Seers should look to do this:

[4] Please note the ICO only offered steers on the wording of the CPCMP product, not on Seers primary CMP product, these feedback points were for Seers use only to edit their wording appropriately. Any positive feedback points provided by the ICO do not constitute ICO approval of any of Seers products including the CPCMP.

"However, consent must be given by a clear positive action. You need to be confident that your users fully understand that their actions will result in specific cookies being set, and have taken a clear and deliberate action to give consent. This must be more than simply continuing to use the website. To ensure that consent is freely given, users should have the means to enable or disable non-essential cookies, and you should make this easy to do."

4.7 As noted at the end of this report, the ICO is currently developing its position surrounding the larger ad tech sector, including a consideration of the use of CMPs in general. Seers should ensure that moving forward they keep abreast of developments in this area of work on the ICO's website and Seers should action relevant recommendations made by the ICO in respect of the use of CMPs.

4.8 The ICO also advised Seers to complete a data protection impact assessment (DPIA) for the CPCMP product in order to demonstrate that they had, as a provider of technology, fully considered the data protection risks associated with the product and taken suitable steps to mitigate such risks. Seers, as explained in further detail below, were considered likely to be a data processor on behalf of their clients and as such are not obligated by the UK GDPR to produce a DPIA. At the time of writing this report, Seers have provided two, early-stage drafts of a DPIA document to the ICO, which the ICO has provided high-level notes on during their Sandbox participation. The ICO advised Seers to continue developing this document outside of their Sandbox participation as such a document, if completed correctly, can be used as a model for Seers' clients who are implementing the CPCMP technology into their own websites.

Objective 2: The ICO will provide steers on key data protection issues to support Seers in their development of the CPCPS.

4.9 The ICO has provided steers on several topics for Seers during their Sandbox participation in relation to this objective.

Is Seers a controller or processor?

4.10 The first steer requested by Seers was help in determining whether Seers, in its capacity of providing the functionality of the CPCMP to its clients, would be considered a controller, joint controller or processor. The ICO advised Seers that as the

CPCMP will process personal data on the behalf of their clients (for the purposes of offering a small level of age assurance of the website end users age) it is likely that Seers' clients are data controllers for data processed via the CPCMP[5].

4.11 Seers were further advised that they would likely be viewed as a processor for the data. Article 4(8) of the UK GDPR defines a data processor as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". Seers in this case would be processing some data on behalf of their clients, including a consent log which contains personal data (IP address, location, consent provided), which appears to be maintained centrally by Seers. As Seers maintain this log on behalf of their clients and not for any of its own purposes, it appears that Seers should be considered a processor for this data[6].

4.12 In order to ensure their ongoing compliance with UK data protection legislation, Seers should ensure that they comply with their obligations as a data processor, more guidance on which is available on the ICO's website. It should also be noted that this finding applies to Seers itself and is not to be taken as a general position regarding all CMPs, or all CMPs that implement some form of age-declaration stage for the purposes of AADC conformance

Can Seers provide their clients with a standardised policy document?

4.13 Seers next asked the ICO if it would be appropriate for Seers as a technology provider and data processor to provide its clients with a standardised data protection policy document for clients utilising the CPCMP. The ICO advised Seers that it would not be appropriate for the ICO as a Regulator to strictly mandate that Seers' clients (ie the data controllers for data

[5] Please note, the ICO only advised Seers that they were a processor in respect of the age assurance and parental consent element of the CPCMP. ICO are currently developing their thinking around the use of CMPs and the associated issues around data controllership in these supply chains.
[6] Please note, if Seers were to process any personal data gathered by the CPCMP for their own purposes (eg for any analytics it carries out to improve the product) then it may be considered a data controller for that processing activity.

processed via the CPCMP) must use Seers' standardised policies. It is up to each individual client or controller to make compliance decisions themselves. However, based on the information provided by Seers, it appeared likely that if Seers did provide their clients with a standardised form of wording to make their implementation of the CPCMP as frictionless as possible and the client used this standardised policy (assuming the wording of such a policy was fit for purpose[7] and had been suitably personalised for each client) they would not be in contravention of UK data protection legislation.

4.14 However, Seers' clients must recognise that the onus is on them as controllers to ensure compliance with data subject rights requests, so they must satisfy themselves that the privacy information which they use is UK GDPR compliant. Insisting on certain wording is a matter for discussion between Seers and their clients, but the most important aspect (in addition to ensuring that such wording is generally UK GDPR compliant) is ensuring that the information is appropriate for the age of the audience. Seers should refer to Standard 4 of the AADC, transparency which states that:

> 'The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent, and in clear language suited to the age of the child.'

4.15 Seers should also consider how they tailor their messages to children of different age ranges, including the potential use of audio or video aids to help children understand.

4.16 The ICO has published guidance on what information should be included in a privacy notice. Generally speaking, the information listed in the checklist in this guidance should be included in any privacy notice and, as such, any standardised policy which provides this information is likely to be compliant with UK data protection legislation.

4.17 However, any Seers' client who chooses to use Seers standardised policy format should ensure that they fully read and understand the policy before implementing it and ensure it is suitably customised for their purposes as a controller. The

[7] Please note, Seers Sandbox participation did not include a review of any such standardised policy document.

client should also ensure that the wording otherwise meets the requirements of the UK GDPR according to the specific situation in which the policy is being used.

What content should be blocked by the CPCMP?

4.18 Seers provided information to the ICO which suggested that their CPCMP is capable of blocking URLs, ads, cookies and other scripts from websites where the CPCMP is enabled. The consent banner for the CPCMP will take the form of a large pop-up, which will appear when an end user loads a website utilising the CPCMP, blocking much, if not all, of the substantive content of the website. Based on the information made available to the ICO, it appears reasonable that the CPCMP would block all website content until an age declaration and consents, or both, are gathered[8].

4.19 Following a self-certified declaration of age, the question of whether or not the content of Seers' client's websites should continue to be blocked will likely depend on the nature of such content. It is likely that each client will need to assess this on an individual basis and make their own decision. However Standard 7 of the AADC, default settings, details the importance of default privacy settings for children. As such it would be up to Seers' clients to determine if children are likely to access their website and the appropriate privacy settings for their audience. By way of a guide, the ICO has determined that in the following circumstances, high default settings are not appropriate:

- When processing is core or essential to provision of most basic elements of service;
- When processing is required to meet a legal obligation; or

[8] Please note that if all website content is blocked when a data subject refuses to provide consent for cookies this is likely to be considered a cookie-wall and would invalidate the consent given by the data subject. For more information on this subject see the "Can we use cookie walls?" section of this ICO webpage and the answer to the specific question on this topic on pages 16 and 17 of this document.

- When giving children a choice would go against their best interests (eg processing necessary to prevent grooming or other criminal activity).

4.20 But in the following circumstances such settings are appropriate:

- For non-core processing or elements of service; or
- For processing which supports a business model but isn't essential to the actual provision of the underlying service.

4.21 This means that, by default, if children are likely to access the website, Seers' clients should not collect any more personal data than they need to provide each individual element of their online service. Therefore, if any ads, cookies and other scripts are not absolutely necessary for the operation of their website they should be turned off for children by default[9].

What level of control should the CPCMP offer end users?

4.22 It is likely that Seers and their clients should offer granular controls to end users, the specifics of such controls depending on the age of the end user (for further information please see Standard 7 of the AADC, default settings).

4.23 Seers should start from the position of enabling high privacy settings by default, 'In order to give children control over when and how their personal data is used, you should provide privacy settings for any processing that is needed to provide additional elements of service that go beyond the core service' (Standard 7 of the AADC, default settings).

[9] Please note that the processing needs to be fundamentally necessary for the operation of the website – not for the website to make a profit as may be the case with ads.

4.24 If it is appropriate to offer a choice of privacy setting, Seers should provide age appropriate explanations and prompts at the point at which a child attempts to change a privacy settings, as required under the transparency standard, to help mitigate risk.

4.25 Seers should vary the content of the banners based on the reported age of the user (ie younger end users will require easier to understand controls which are easier to apply and use). Similarly, it may be necessary to vary the granularity of the controls given to certain age groups, for example:

- **People over the age of 16** should be provided with the highest granularity of privacy options.
- **Children aged between 13 and 16** may require simpler controls if Seers considers that granular controls would not be understandable to such children.
- **Children under 13 who are not accessing preventative or counselling services** would require the same controls as adults, as their parents will be the ones providing consent on their behalf. However, suitable steps would have to be put in place before the granular controls are made available to the child, to ensure that a child knows to pass their device to their parent in order for the parent to provide consent. Children under 13 may also require certain options to be disabled by default as these options may not be strictly necessary for the operation of the website.
- **Children under 13 who are accessing preventative or counselling services.** The AADC would not apply in this context as Section 123(7) of the DPA18 places 'preventive or counselling services' outside of the scope of the code.

Is CPCMP a cookie wall?

4.26 As detailed above, there was some concern that Seers' CPCMP may at certain times act as a cookie wall (ie websites using the CPCMP would require users to provide consent to access the substantive content of the website). Based on the information provided by Seers in the ICO's view, it is currently unclear whether the functionality of the CPCMP would

constitute a cookie wall. For clarity, the ICO defines a cookie wall as when a website requires users to 'agree' or 'accept' setting of cookies before they can access a service's content. This is also known as the 'take it or leave it approach'. Therefore, if the CPCMP still allowed users who did not consent to cookies to access the substantive content of a website, it would likely not be viewed as a cookie wall.

Objective 3: ICO will provide steers on Seers development of 'phase 2' of the CPCMP tool which includes a third party age verification.

4.27 The work undertaken to complete Seers third objective revolved around theoretical questions about how Seers could develop the CPCMP concept further outside of the Sandbox. Specifically, focusing on whether Seers would in fact be required to collect a parental consent and whether or not the CPCMP should include some form of age verification, rather than the self-certification currently used.

Will Seers need to gather a parental consent?

4.28 If the CPCMP is provided using consent as the basis for processing, then it appears likely that, depending on the age of the user, Seers and their clients would need to obtain a parental consent.

4.29 Existing ICO guidance states that in the UK, only children aged 13 and older can provide their own consent for processing[10].

[10] Please note in some European territories this minimum age may be as high as sixteen years old when providing consent for Internet Society Services (ISSs) so it will be up to Seers' clients to ensure that they are aware of the minimum age of GDPR consent in the territories they operate.

4.30 In the UK, Seers clients will need to seek parental consent for children aged twelve and younger unless the online service provided is a preventive or counselling service.

4.31 Seers and their clients will need to ensure that the self-certified age has a level of accuracy proportionate to the level of risk associated with the content of the website (eg a self-certified age would not be suitable for a website with 13+ age restrictions, see Standard 3 of the AADC, age appropriate application for further information). Similarly, Seers and their clients will need to ensure that they have a level of assurance that it is the parent of the end user providing consent where parental consent is necessary.

4.32 Furthermore, as Seers' app aims, at least in part, to block cookies that allow access to inappropriate content, Seers should refer to Standard 5 of the AADC, detrimental use of data, and Appendix C of the AADC, Appendix C of the AADC, when do we have to get parental consent, for guidance on the standards and codes of practice that exist that relate to children (eg the Committee of Advertising Practice code). The block should prevent processing children's personal data in ways that run contrary to those standards, codes or advice and should take account of any age specific advice to tailor online service to the age of the child.

Would it be appropriate for Seers to use a third party age verification check in the CPCMP?

4.33 Yes, depending on the level of assurance Seers' client felt was necessary based on the sensitivity of their website's content (ie the more sensitive a websites content, the greater the necessary assurance of the end user's age needs to be). Seers should refer to Standard 3 of the AADC, age appropriate application, for further information on this.

4.34 As stated above, websites such as YouTube and TikTok require, as part of their terms of service for their users to be at least 13 years of age, therefore in order to gain a greater level of assurance that the end user is the age they claim to be, a third party age verification check may be appropriate.

4.35 Seers should also consider other mechanisms for age certification (ie it is not just the case of a choice between self-certification and third party age verification) as there may be other mechanisms which are more appropriate for Seers and their clients. Seers have communicated to the ICO their intent to include some form of age assurance check in the next iteration of the CPCMP product.

5. Ending statement

5.1 Seers' participation in the ICO's Sandbox has given the ICO the opportunity to gain insight into how the Children's Code has been received by industry and the advice needed by industry partners to fully operationalise the Code's standards, some of these have been formalised in our Children's Code UX Guidance.

5.2 It is clear to us from our work with Seers that the organisation it taking meaningful steps to ensure compliance with UK data protection legislation in how it implements the CPCMS tool. The ICO is currently developing its position on the use of CMP's in the adtech sector and hopes to publish its findings soon, however the ICO has already provided the following notes in its Update report into adtech and real time bidding. In general Seers and other organisations operating in the adtech industry should ensure, if they have not already acted on the content of this report, that[11]:

- any processing of non-special category data is taking place lawfully at the point of collection (ie not using legitimate interests for placing or reading a cookie, or other technology, rather than obtaining the consent PECR requires);
- any processing of special category data is taking place lawfully by obtaining a compliant explicit consent from the data subject;

[11] Please note that the ICO have not provided advice to Seers on the CMP platform which underpins their CPCMP.

- they do not attempt to rely on legitimate interests as their UK GDPR lawful basis for processing as it is unlikely they can make a robust argument for relying on this basis;
- they have a good understanding of the DPIA requirements set out in Article 35 of the UK GDPR and ensure that suitable DPIAs are carried out to assess and mitigate data protection based risks. Further information on DPIAs is available on the ICO's website;
- the privacy information they provide to individuals is informative and provides clarity as to the overall processing activity, without being overly technically complex. These notices should inform individuals about all the other organisations who may receive and process their personal data;
- the data is adequately secured in transit and at rest and that suitable considerations are taken before data is transferred internationally (ie that suitable international transfer frameworks are in place); and
- data minimisation and retention controls are applied consistently and underpinned by sound rationale.

5.3 It is clear to us from our work with Seers that they are attempting to ensure that the CPCMP delivers consent management for their clients in a way which ensures website users are properly informed of how their personal data will be processed in a manner which is appropriate and proportionate to their age group. Moving forwards, Seers should attempt to action all ICO recommendations which have been provided and continue to monitor the ICO website for updates to our advice in relation to the adtech sector.