North Ayrshire Council's use of Facial Recognition Technology in its schools

As you will be aware, the Information Commissioner's Office (ICO) has responsibility for monitoring and enforcing the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018). Our functions include promoting public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data.

In October 2021 concerns were raised both in the media and directly with the ICO regarding the use of Facial Recognition Technology (FRT) in nine North Ayrshire Council (NAC) schools.

Given the nature of the concerns and the public interest, the ICO commenced engagement with NAC to establish whether the processing raised any concerns in respect of data protection law. We note that NAC have proactively engaged with the ICO during this process.

We took a detailed look at the information provided by NAC and concluded that, whilst it may be possible to deploy FRT in schools lawfully, in this case we are concerned that the technology had been deployed in a manner that is likely to have infringed data protection law under the following Articles of the UK GDPR:

- Lawful, Fair, and Transparent (Article 5(1)(a), Article 6, Article 9 and Article 12);
- Right to be Informed (Article 13);
- Retention (Article 5(1)(e)); and
- Data Protection Impact Assessment (Article 35).

We recommend improvements that NAC can make in the following areas when considering similar issues in the future:

- Data Minimisation (Article 5 (1)(c)); and
- Data Accuracy (Article 5(1)(d))

Our initial observations and analysis of the main areas of concern are explained in detail in Appendix 1.

Actions for NAC to undertake

New technologies such as FRT can offer benefits and efficiencies, but their use is not without risk from a data protection point of view. That risk is heightened where children's data is being processed. Recital 38 of the UK GDPR makes clear that children are to receive specific protection when processing their personal data as "*they may be less aware of the risks,*

consequences and safeguards concerned and their rights in relation to the processing of personal data."

It is critical that NAC fully understands its obligations under data protection law in relation to the deployment of new technologies that process children's special category biometric data. Risks must be identified, assessed and mitigated as appropriate.

Appendix 1 sets out in more detail our concerns that the processing carried out by NAC is likely not to have been in compliance with data protection law. NAC should ensure that these concerns are taken into account in the future to avoid infringing data protection law. In particular, NAC should ensure that the advice provided by the ICO is understood by NAC staff and applied in the future.

Specifically, NAC should:

1. **Ensure that there is a valid lawful basis for processing children's data.** Our view is that Consent was the appropriate lawful basis for processing children's special category biometric data for the purpose of cashless catering in this case. However, as identified in Appendix 1, the requirements for valid consent were unlikely to have been met in this case.

2. **Ensure that the processing is transparent.** It is vital that NAC is able to explain in age-appropriate language how children's data will be collected, used, stored and retained. The risks associated with its use should be clearly set out. We note that NAC has developed and published a children's privacy notice.

3. **Ensure that a comprehensive DPIA that complies with Article 35 requirements has been completed and that the DPIA identifies, assesses and mitigates the risks to pupils' rights and freedoms.** The DPIA should consider the necessity and proportionality of the processing, the potential for 'function creep' (ie using personal data for purposes beyond those you originally identified), and ensure that risks of bias and discrimination in the use of FRT are identified, assessed and mitigated. There must be a signed, dated DPIA in advance of the processing commencing. The DPIA process should also document the Data Protection Officer's (DPO) advice and the controller's consideration of that advice.

We note that NAC has taken proactive steps to improve its data protection compliance including through the development of a children's specific privacy policy and a revised DPIA template specifically for processing children's data. We will engage further with the DPO on these matters as necessary.

Next steps

We intend to draw out the key learnings from this enquiry and promote them through social media and in a case study within our guidance. This will benefit other education authorities considering the use of FRT or similar technologies. We therefore plan to publish a copy of this letter and the appendix on our website. Please also find the case study and the content of the social media posts attached for your information.

Please note that this correspondence and any response received do not prejudice the potential future use of the Commissioner's enforcement

powers should evidence of further potential infringements of data protection law come to light.

Yours sincerely

Ken Macdonald
Head of ICO Regions

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice

Appendix 1

Background

Introduction of FRT to North Ayrshire schools

NAC is the controller of personal data processed by the schools under its control. FRT was introduced in nine North Ayrshire schools on 6 September 2021 - affecting 2,569 pupils - as part of a replacement for its existing cashless catering system. Subsequently, concerns about the processing of children's special category biometric data and the use of FRT and its compliance with data protection law were raised in the media and directly with the ICO.

The FRT was introduced as a means by which to verify pupil's identity at the lunch till in order to deduct money from an online account. There is a camera at the cash till which is operated manually by a member of catering staff. The operator takes a single still image of a pupil. The FRT then attempts to match the photo to a biometric facial template that had been captured over a number of days in September 2021. If a match is found, the software opens that user's account and the transaction is approved or declined by the catering staff member. If there are multiple potential matches (for example, when dealing with identical siblings), the potential options are presented to the operator and they manually select the user to complete the transaction.

Overview of the engagement between ICO and NAC

Following a review of the Data Protection Impact Assessment (DPIA), the ICO wrote to NAC on 6 October 2021 to arrange a meeting. In advance of that meeting we wrote to NAC on 20 October 2021 with a list of questions related to NAC's use of FRT. A meeting between NAC and the ICO was held on the 21 October 2021. NAC then advised the ICO on 22 October 2021 that the use of FRT for payments in schools had been paused. A written response to our questions, along with supporting documents, was received on 29 October 2021. NAC confirmed on 11 November 2021 that all facial templates, including back-up templates, had been deleted meaning the processing had ceased. We wrote to NAC on 17 November 2021 with further questions and NAC responded to those questions on 26 November 2021. We had a concluding meeting with NAC on 25 May 2022 where we set out our concerns in relation to NAC's compliance with data protection law.

ICO's initial conclusions

Lawful, fair and transparent – a summary

Following our enquiries into the use of FRT by NAC we have concerns that the processing is likely not to have been in compliance with Article 5(1)(a) of the UK GDPR, lawful, fair and transparent. In particular:

- NAC were unable to demonstrate that there was a valid lawful basis for the processing

In this case it was not clear initially which lawful basis NAC was using. There was a disparity between what was stated in the DPIA and the written response to our questions. The DPIA stated that Public Task was the lawful basis being relied upon whereas in response to our questions on 29 October 2021, NAC confirmed on 25 May 2022 that "*Given the nature of the data being processed, consent forms the legal basis for such activity under Articles 6 and 9*".

Our guidance on lawful basis advises controllers to "*Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason. In particular, you cannot usually swap from consent to a different basis*." It is imperative to decide on the lawful basis before the processing begins and to be clear throughout the process about which lawful basis is being relied upon.

Consent

In relation to consent, in this case, the necessary requirements for freely given, specific, informed and unambiguous consent were unlikely to have been met.

- In relation to the processing of special category data NAC were unable to demonstrate that valid explicit consent was obtained as the consent statement was not specific and could apply to a broad range of processing activities.

The information provided to children and their parents did not contain all of the information required under Article 13 of the UK GDPR. Specifically:

- the privacy notice did not include '*information about the right to lodge a complaint with the ICO (Article 13(2)(d))*' or '*the period for which the personal data will be stored, or where that is not possible, the criteria used to determine that period (Article 13(2)(a))*.'

- Information on retention was not sufficiently transparent. There was a broad reference to personal data being retained "for as long as necessary." School children should be given a clearer indication of how long their biometric data will be retained.

Lawfulness – our initial conclusions in more detail

In order to process data lawfully, controllers must be able to identify a lawful basis from Article 6 of the UK GDPR before the processing begins. There are six available lawful bases, all of which are of equal status. The controller must identify the most appropriate lawful basis for the particular purpose it has identified and consider its relationship to the individual.

The facial templates and images generated by the FRT system were used "*for the purpose of uniquely identifying a natural person*" and are therefore classed as special category biometric data under data protection law. In order to lawfully process special category data, both a lawful basis under Article 6 of the UK GDPR and a condition for processing special category data under Article 9 of the UK GDPR are required.

Consent and Explicit Consent

NAC confirmed in the meeting of 25 May 2022 that it was relying on Consent (Article 6(1)(a) UK GDPR) as a lawful basis for the processing and in the DPIA it stated it would rely on Explicit Consent (Article 9(2)(a)) for processing special category biometric data.

There were two "groups" of individuals who NAC asked to provide explicit consent for the processing of special category biometric data. The first group comprised the parents of students from S1 to S3 (aged 11-14), and the second were students providing their own consent, ie those between S4 and S6 (aged 14-18). NAC produced two consent forms, one for each group. We considered whether the consent and explicit consent sought for this processing met the high standard that the UK GDPR requires – was it freely given, specific, informed and unambiguous?

Our observations apply to both forms as they were almost identical in their content. The only difference between the forms was a subtle change in who it was addressed to and who was directed to use it, ie 'your child' was altered to 'you'.

Freely given

Public authorities must be able to demonstrate that consent is freely given. To fulfil this there needs to be a **genuine choice** for individuals. Although NAC is not prohibited from relying on consent or explicit consent under Article 6 and 9, NAC as a public authority, needs to pay particular attention to the inherent imbalance of power between itself and the individuals who are being asked to give their consent in this context.

In this case the facial recognition consent form states that "*A new pupil method for catering within our secondary school is being introduced…*". The facial recognition consent email stated "*facial recognition will be used for authenticating **all** secondary school pupils that require access to school meals and/or snacks, including those eligible for free school meals.*" This does not present FRT as an option. The wording used implies that the system will be introduced (regardless of the wishes of the children or their parents). Whilst the FAQs clarified there would be an alternative method, it did not explain how this would work or whether those pupils would receive the same treatment as those who did consent.

Because of the power imbalance between NAC and the parents/children, individuals may have felt compelled to consent because of the way the information was worded and how the introduction of FRT was being presented. It therefore appears unlikely that consent was freely given. It should have been made clear to pupils and parents that there was no requirement to consent to FRT to obtain a school lunch and alternative options as easy to use as the FRT, should have been provided.

Specific and informed

The consent forms did not identify the controller but rather the individual school. Recital 42 of the UK GDPR (which can be used as an aid to our interpretation of the UK GDPR) states that for consent to be informed, the pupil should be aware at least of the identity of the controller – in this case, NAC. Technical terms such as 'encryption' and 'AES 256' are used but these may be unfamiliar concepts to many parents/children. Although the consent statement states that the system "*converts physical characteristics into a unique digital signature*", it would benefit from more explicit wording that images of children's faces will not be stored. The system was not clearly explained in a way that was easy to understand, and information was missing (for example, the identity of the controller). Therefore, in our view it is unlikely that the consent provided was specific or informed.

Explicit and Unambiguous

Our guidance on explicit consent states that "*Explicit consent is not defined in the UK GDPR, but it is not likely to be very different from the usual high standard of consent.*" Our guidance goes on to outline that the extra requirements for consent to be 'explicit' are likely to be:

- explicit consent must be confirmed in a clear statement (whether oral or written), rather than by any other type of affirmative action;
- it must specify the nature of the special category data; and

- it should be separate from any other consents you are seeking.

Therefore, a key feature of 'explicit consent' is that it must be affirmed in a clear oral or written statement. The element of the processing that requires explicit consent needs to be specifically referred to. This clarity is particularly important when seeking consent from a child. The statement "*I do wish to grant consent to participate in the use of facial recognition systems within the school"* is vague and potentially quite far reaching and therefore, the consent is unlikely to be explicit or unambiguous.

Our detailed Consent guidance details how to obtain, record and manage consent.

Consent and Children over 12 in Scotland

We raised concerns about seeking parental consent rather than consent directly from children aged between 12 and 14. NAC stated that "*The DPO advised that under the Data Protection Act 2018 the legal age of consent for data processing purposes is 12 years of age if the child is deemed competent. After extended discussions with project team members, it was decided that to provide an additional level of process assurance, parental consent was to be sought for pupils in S1-S3.*" However NAC must have regard to section 208 of the DPA 2018 which states that:

> *(1) Subsections (2) and (3) apply where a question falls to be determined in Scotland as to the legal capacity of a person aged under 16 to—*
>
> *(a) exercise a right conferred by the data protection legislation, or*
>
> *(b) give consent for the purposes of the data protection legislation.*
>
> *(2) The person is to be taken to have that capacity where the person has a general understanding of what it means to exercise the right or give such consent.*
>
> *(3) A person aged 12 or over is to be presumed to be of sufficient age and maturity to have such understanding, unless the contrary is shown.*

Therefore, in Scotland, those aged over 12 are presumed able to provide their own consent.

The ICO guidance[1] on processing children's data states:

> *"The general rule in the UK is that you should consider whether the individual child has the competence to understand and consent for themselves (the 'Gillick competence test'). However, in Scotland a person aged 12 or over is to be presumed to be of sufficient age and maturity to have such understanding, unless the contrary is shown. In practice, you may still need to consider age-verification measures as part of this assessment and take steps to verify parental consent for children without competence to consent for themselves."*

Where seeking consent for children over 12 from their parents, the onus is on NAC to demonstrate on a case-by-case basis that the child in question is unable to provide their own consent rather than applying a blanket approach across an entire group of children. Consideration should be given to how to protect children's rights. It is not clear, for example, whether children aged 12-14 understood that parental consent was being sought on their behalf or whether they understood how to object, or were given the opportunity to do so.

Fairness and Transparency

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR as set out under Article 5(1)(a) and in Articles 12 and 13. Recital 58 clarifies that "*Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand*" and our guidance on children emphasises that "*You should write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have*."

NAC advised us that it took steps to alert children and parents to the processing of biometric data via a number of channels, including direct emails, social media and through the provision of FAQs. Whilst this was positive, our view is that NAC was unlikely to comply with the requirements of Article 12 as it did not ensure that the content of its privacy notice was provided to children in *a concise, transparent, intelligible and easily accessible form, using clear and plain language*. In particular, it did not attempt to explain to children, in child-friendly terms, the potential impact of the processing of biometric data.

In addition, the communications from NAC underplayed the complexity of the FRT technology and suggested that biometric processing is an historic and well-tested practice. This could be considered misleading to the data subjects as there was no attempt to explain the fact that this is a relatively new technology which would result in the processing of

children's unique biometrics, nor was there any attempt to outline the potential risks this could present.

Ensuring that your communication is clear, particularly when aimed at children, and that it is not misleading in any way will facilitate compliance with the fairness aspect of the first principle of data protection law. Fairness and compliance with the data protection principles, should be central to all your processing of children's personal data.

Given that children may not fully appreciate the risks or envisage the consequences associated with the processing of their special category biometric data, efforts should be made to ensure that the children are aware of the risks and consequences of the processing as well as the safeguards put in place to minimise these risks. This will allow children to make informed decisions about what personal data they wish to share, be clear about what happens to their personal data and ultimately exercise their data protection rights.

Retention

The processing was unlikely to be compliance with Article 5(1)(e) of the UK GDPR, the storage limitation principle, in particular:

- The retention period was not specific and did not address the retention period for the various elements of personal data being processed (the facial templates, the still image etc).

The storage limitation principle requires that personal data is kept for no longer than is necessary for the purposes for which it is processed. The retention period set out in the DPIA stated that "*Requirements state that data is only used while child is at school. Thereafter data requires to be archived in line with GDPR and NAC data retention requirements which is 5 years after leaving date or date they reach 23rd birthday, whichever is later.*"

It was not clear if this applied just to the facial templates and/or the still captured at the till.

We sought clarification from NAC as to why five years was chosen as there was no justification provided within the DPIA. NAC advised that "*There is no justification for data retention beyond school leaving age or opt out from the system*" but went on to state "*The Council's Data Retention Schedule will be updated to appropriately reflect the need for biometric information to be deleted on leaving or opting out of the facial recognition process."* We were therefore of the view that it was likely that this retention period was contrary to the storage limitation principle. However, we note that NAC acknowledged this during the meeting of 21

October 2021 and advised that a different retention period would be applied.

Each new processing activity should be considered individually rather than being bundled up with other existing retention periods. NAC should ensure that processing activities, whether new or existing, and their corresponding retention periods are appropriate. NAC must ensure the retention period for each item of personal data being processed (in this case the personal data involved the facial template, the stills captured at the till, and any match data) is distinct and that the data is only kept for as long as is necessary for the purpose it is being processed.

The UK GDPR does not dictate how long to keep personal data but the controller must justify the retention period, based on the purposes for processing. It is particularly important to keep retention periods under review when processing personal data relating to children. In this case, there would be no reason to keep a child's biometric information once they no longer use the system, for example because they have left the school, they object to/withdraw their consent for the processing, or their parent withdraws consent.

Data minimisation and data accuracy

The data minimisation principle requires that personal data being processed is adequate, relevant and limited to what is necessary. You should look at these elements individually and document your rationale in the DPIA for how the processing will comply with each. The accuracy principle requires personal data to be accurate and, where necessary, kept up to date;

- The DPIA did not appear to contain enough detail on how the personal data being processed complied with the data minimisation and the data accuracy principle, particularly how the data would be processed adequately and was relevant to the purpose for processing.

Before implementing any FRT, NAC should be satisfied that the statistical accuracy of the FRT system is sufficient for the processing context. For example, FRT systems have been shown to perform less well with specific gender or ethnic groups, as identified in our guidance on Human bias and discrimination in AI systems.

To ascertain whether the algorithm is sufficiently accurate NAC should seek information and assurances from the supplier about how the algorithm was trained (is the training data sufficiently representative?) and what kind of bias testing has been conducted. This should be documented within the DPIA. Then, where shortcomings are identified,

NAC must assess the associated risks and consider whether these can be appropriately mitigated. Ongoing monitoring of any bias in the system will then be critical. The DPIA should be updated accordingly.

NAC received information on the False Positive and False Negative rates from the supplier of the technology. However there was no consideration of the false positive or false negative rate in the DPIA. NAC did give consideration to adequacy of the algorithm in terms of the false positive rate in its written response to us, however there appeared to be no consideration of the relative accuracy of the algorithm with respect to protected groups. It's key that these risks are assessed within the DPIA and mitigated as appropriate.

Taking steps to avoid bias and discrimination will also assist in meeting the requirement for the processing to be fair.

We asked NAC "*Where, when, and how is the faceprint template obtained? How often does this have to be refreshed given that these are children whose faces will change over time?*" NAC stated "*To maintain accuracy of data, in accordance with Article 5(1) (d) refresh templates will be captured annually to align with Education's annual data checks. This will allow for changes in facial measurements over time to be appropriately reflected, and prompt at least annual reassessment of consent by parents and/or pupils."* This detail should be in the DPIA and supplemented with a description of the processes in place to ensure that the previous templates would be deleted so that NAC is not processing more data than is necessary. The DPIA should detail what measures are in place in relation to the processing of biometric data generated at the point of sale. This data should only be processed for as long as it is necessary for the purposes for which it is being processed.

Data Protection Impact Assessment (DPIA)

We consider that the DPIA we reviewed is unlikely to have complied with Article 35 of the UK GDPR. In particular:

- There was a residual high risk identified in the DPIA when the processing commenced.
- The risk assessment did not address risks to individuals' rights and freedoms and specifically did not consider risks related to bias and discrimination.
- No consultation was undertaken with pupils and/or parents.
- The DPIA was not signed off and was provided to us in draft form.

The assessment contained in Part 5 of the DPIA appeared to show that there was still a residual high risk relating to unlawful access after the

processing commenced on 6 September 2021 when the first facial templates were captured. NAC advised us that that *"Encryption to AES-256 standard has been in place since processing of data was initiated and consequently at no time has there been any residual high risk to data."* The assessment had not been updated to reflect this mitigation. It is crucial that the DPIA is updated as and when appropriate, especially where high risks are being considered. This is because if a DPIA has identified a high risk that cannot be mitigated, prior consultation with the ICO is required under Article 36(1) of the UK GDPR. Processing cannot commence until we have been consulted - a failure to consult with us would be a breach of the legislation and may result in regulatory action.

Further, we note NAC's comment that "*at no time has there been any residual high risk to data.*" However the relevant assessment is whether the processing poses an "unmitigable high risk to the rights and freedoms data subjects." The two are not necessarily the same. The assessment is about the potential impact on individuals and any harm or damage your processing may cause – whether physical, emotional or material. This is echoed in step 5 of our DPIA guidance ("How do we identify and assess risks?"). In particular, a controller should consider whether the processing could contribute to:

- inhibiting individuals from exercising their rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage.

As it stands, the risk assessment in the DPIA focused on the risks to NAC of non-compliance rather than the risks to individuals which arose from the processing itself. For instance, the assessment considered a data breach, which may have presented a serious risk to individuals rights and freedoms but this was not drawn out. Our view is that the DPIA required a more considered risk assessment.

Our Data Protection Harms contains an overview of data protection harms and the ICO's taxonomy that can be useful when identifying harms that may arise from identified risks.

Recital 38 of the UK GDPR states that "*Children merit specific protection with regard to their personal data, as they may be less aware of the risks,*

consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child".

None of the risks identified in the DPIA related to the processing of children's biometric data or the risk of bias and discrimination in the data matching algorithm. We asked NAC what consideration had been given to the specific risks arising from the processing of children's biometric data and how these had been documented. We were advised that the DPIA process had been undertaken and that "*Given the nature of the data being processed, consent forms the legal basis for such activity under Articles 6 and 9.*" However, a reliance on consent does not abdicate a controller from the responsibility of undertaking an assessment of the risks to individuals' rights and freedoms that may arise as a result of the processing.

Our opinion on live facial recognition in public places gives some detail on risks associated with processing of biometric data and may be useful for future instances where the processing of biometric data is being considered. Specifically, it states that biometric data "*is more permanent and less alterable than other personal data; it cannot be changed easily. Biometric data extracted from a facial image can be used to uniquely identify an individual in a range of different contexts. It can also be used to estimate or infer other characteristics, such as their age, sex, gender or ethnicity.*" It also considers the risk of bias and discrimination that could lead to unfair treatment of individuals from protected groups. More detail on this can be found in our blog on bias and discrimination in AI. These risks should be identified, assessed and mitigated and the risk assessment and mitigations should be documented in the DPIA.

Article 35(9) of the UK GDPR states that "*Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations*." Our guidance on conducting a DPIA and step 3 of our detailed guidance on undertaking a DPIA advises controllers to '*seek and document the views of individuals (or their representatives) unless there is a good reason not to'* and incorporate the details and findings into the DPIA. NAC did not undertake consultation with parents or children prior to the processing. The reasoning provided for this was that the processing would be "*… entirely consent based*."

Relying on consent, or explicit consent, does not preclude a controller from undertaking a consultation exercise. Indeed, the views of the data

subjects might help shape the DPIA. Controllers can use the views of data subjects in the DPIA to justify why particular action was or was not taken. Data subjects may raise specific privacy concerns that can be addressed in the risk assessment. The controller can then identify mitigations and safeguards in order to address that specific risk, this may foster further trust between the data subjects and controller.

A signed, dated DPIA is a record of whether mitigation measures have been approved by the controller. The DPIA was not signed off by either the DPO or a senior employee of NAC prior to the processing commencing. NAC advised that the DPO was consulted throughout but the DPO's recommendations are not recorded within the DPIA and our understanding is that there was only verbal approval of the processing by the DPO. However, Article 35(2) of the UK GDPR requires that DPO advice is sought and our guidance states that DPIAs should include "*the advice and recommendations of our DPO (where relevant) and ensure the DPIA is signed off by the appropriate people.*" It is necessary for a controller to demonstrate its compliance with the data protection framework as part of its accountability obligations and a thorough and comprehensive DPIA is one way in which to do this.

The Accountability Framework, and specifically the section on Risks and data protection impact assessments (DPIAs), is a useful tool to assess compliance and ensure our expectations are met.

NAC should have ensured that its DPIAs contain advice from its DPO to show that the controller had considered all relevant risks, and what -if any- changes had been made as a result of the risk assessment. Even if the advice was verbal, there should have been documentation confirming what was said and the controller's response – otherwise there is no evidence that any advice was sought. Furthermore, where the controller decides not to follow DPO advice, the justification for so doing should be documented.

End