Consent, GDPR and IAS services

GDPR and consent

Even since before COVID-19, services have been asking us for clarity with regards to working with children, young people and families, data protection, record keeping and more. This has been a focus again as we move from face to face meetings and the ability to gain written consent with families, to moving onto virtual platforms.

To support with this, we commissioned Steve Broach to write some legal advice for services. A summary can be found in this document to be read alongside the advice itself.

One particular issue that is too complex to be considered as part of this briefing alone is regarding safeguarding. For more information and support with regards to keeping both yourselves, your teams and those you work with safe from harm in these new ways of working, please consider the following:

https://www.gov.uk/government/publications/covid-19-safeguarding-in-schools-colleges-and-other-providers/coronavirus-covid-19-safeguarding-in-schools-colleges-and-other-providers

https://www.england.nhs.uk/coronavirus/wp-content/uploads/sites/52/2020/03/C0044-Specialty-Guide-Virtual-Working-and-Coronavirus-27-March-20.pdf

https://www.ncsc.gov.uk/files/vtc_infographic.pdf

https://www.socialworktoday.com/news/eoe_0520.shtml

https://www.basw.co.uk/media/news/2020/jun/top-tips-virtual-direct-work-children-families-during-covid-19

GDPR- Consent and Virtual Working – Steve Broach

- You do not need 'formal,' written consent to process data as there are other lawful basis for collating data. This is vital to know when working virtually with families and children and young people as it means you do not need written consent to start a formal piece of work. You can start working with a child, young person or family member without the need to meet with them face-to-face which may not be possible while we are working more virtually.
- If it is necessary for volunteers to be completing case recording, this should be done in-line with data protection policies. If necessary for volunteers to do so, there should be a written agreement/ contract that ensures they have formally agreed to adhere to those data protection policies. This will need to be done even while working virtually.
- Safeguarding of those we're working with must always be the priority and all should understand that information may need to be shared with relevant organisations should safeguarding

concerns be raised. Further information on safeguarding while using virtual platforms can be found in the above.

- As a very broad guide information and data should be retained for six years, and in-line with the host organisations' data protection policies

If you have any further questions on GDPR and data processing, especially with regards to the current need to rely on virtual platforms for the majority of communications, please be in touch.

Thanks all,

Information, Advice & Support Services Network for SEND

The IASSN team

IAS SERVICES: DATA PROTECTION

ADVICE

SUMMARY OF ADVICE

1. I am asked to advise the Information, Advice and Support Services Network ('IASSN') on a number of data protection issues in relation to IAS Services. It should be noted at the outset that my advice is for IASSN, not for any individual IAS Service. Individual Services will need to seek appropriate advice if any particular issues arise for that Service (I would of course be happy to provide such advice). In summary, my advice for IASSN on the questions posed in my instructions is as follows:

    a. Consent should not be relied upon by IAS Services as the lawful basis on which they process personal data, unless this is strictly necessary. As such generally IAS Services should not seek written (or any) consent before starting to work with families. In my view, there are other lawful bases that IAS Services can rely upon which will ensure that they comply with data protection law. Accordingly, IAS Services should adopt a data protection policy and formulate a Privacy Notice that sets out their reliance on the 'public task' and 'legitimate interests' bases for processing, as explained below. Where health data is processed, then this should be in reliance on the 'statutory and government purpose' condition wherever possible, again as explained below. Service users should be directed to the Privacy Notice when their data is collected.

    b. In a narrow set of circumstances, it <u>may</u> be necessary for IAS Services to rely on consent in order to process data. However, I would need further information in order to advise whether this will be necessary and, if so, the process that should be followed.

c. IAS Services should manage the need for volunteers to make records on case recording systems by ensuring that volunteers are provided with data protection training and sign contracts which confirm they will comply with IAS Services' data protection policy, that they will only act in accordance with instructions in processing personal data, that they are bound by a duty of confidentiality in relation to the personal data they access at IAS Services and they will not copy or remove any personal data from IAS Services. Volunteers should be given clear instructions about the data they can and cannot access on databases.

d. Sharing of personal data for the purposes of safeguarding can be carried out in accordance with the data protection regime where this is on the 'public task' or 'legitimate interests' basis, as explained below. Further, health data can be shared for safeguarding purposes where this is within the 'statutory and government purpose' condition, the 'safeguarding of children and of individuals at risk' condition or the 'safeguarding of economic well-being of certain individuals' condition, as explained below. Whenever the sharing of information for safeguarding purposes is considered, IAS Services should document the decision made and the reasons for this, including the legal bases and condition upon which they rely.

e. As a very broad guide, it seems to me reasonable for IAS Services to retain data for six years, subject in particular to whether any safeguarding concerns have arisen in that period which would justify retention for a longer period. The relevant factors to consider in determining the appropriate period for data to be retained are set out below.

LEGAL FRAMEWORK

IAS Services

2. IAS services are provided in accordance with the Children and Families Act 2014 ('CFA 2014'). Section 32 CFA 2014 provides:

> (1) A local authority in England must arrange for children and young people for whom it is responsible, and the parents of children for whom it is responsible, to be provided with advice and information about matters relating to the special educational needs of the children or young people concerned.
> (2) A local authority in England must arrange for children and young people in its area with a disability, and parents of children in its area with a disability, to be provided with advice and information about matters relating to the disabilities of the children or young person concerned.

3. Section 26(3) CFA 2014 provides:

> Joint commissioning arrangements must include arrangements for considering and agreeing - … (d) what advice and information is to be provided about education, health and care provision; (e) by whom, to whom and how such advice and information is to be provided…

4. The SEND Code of Practice: 0 to 25 years (January 2015) provides:

> §2.8 When designing Information, Advice and Support Services, local authorities should take into account the following principles:
> i. The information, advice and support should be impartial and provided at arm's length from the local authority and CCGs
> ii. The information advice and support offered should be free, accessible, confidential and in formats which are accessible and responsive to the needs of users…
>
> §2.10 Many children will access information, advice and support via their parents. However, some children, especially older children and those in custody, may want to access information, advice and support separately from their parents, and local authorities **must** ensure this is possible.

5. This statutory framework is relevant context when considering the application of data protection legislation.

The Data Protection Framework

6. The Data Protection Act 2018 ('DPA 2018'), read together with the General Data Protection Regulation 2016/679 ('GDPR'), currently set out the law governing the processing of personal data. The GDPR continues to apply in the UK until the end of the Brexit transition period, that is presently until the end of 2020. When the transition period ends, the status of the GDPR going forwards will depend on the outcome of negotiations. However, the default position is that the GDPR will be brought into UK law as the 'UK GDPR'. The content of this advice will need to be reviewed and updated in light of Brexit, although at present it seems likely the same principles will continue to apply.

7. In addition to the DPA 2018 and GDPR, the Information Commissioner's Office ('ICO') has issued a range of guidance, including a 'Guide to the GDPR' and 'Children and the GDPR'.

The meaning of 'processing' and 'personal data'

8. The DPA and GDPR apply to 'processing' of 'personal data'. These concepts are central to the application of the data protection regime:
    a. *Personal data* means any information relating to an identified or identifiable living individual: s 3(2) DPA 2018.
    b. *Processing*, in relation to information, means an operation or set of operations which is performed on information, or on sets of information, such as:
        i. collection, recording, organisation, structuring or storage,

ii. adaptation or alteration,
iii. retrieval, consultation or use,
iv. disclosure by transmission, dissemination or otherwise making available,
v. alignment or combination, or
vi. restriction or destruction: s 3(4) DPA 2018.

9. The breadth of the definition in s 3(4) DPA 2018 means that almost any action taken in relation to personal data constitutes 'processing'.

'Data controllers' and 'data processors'

10. The nature of the obligations placed on a person or organisation depends on whether they are a 'data controller' or 'data processor':
    a. A *controller* is a person who determines the purposes and means of processing of personal data: s 6(1) DPA 2018, art 4(7) GDPR.
    b. A *processor* is a person responsible for processing personal data on behalf of a controller: art 4(8) GDPR.

11. Data controllers are under an obligation to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that data processing is performed in accordance with the GDPR: see art 24 GDPR, s 56(1) DPA 2018. This will include:
    a. where it is proportionate, the implementation of appropriate data protection policies: s 56(2) DPA 2018.

b. using technology to ensure an appropriate level of data security: see art 32 GDPR.

c. the data controller taking steps to ensure that any person acting under their authority who has access to personal data does not process that data, except on instructions from the controller: art 32(4) GDPR. See also s 60 DPA 2018.

12. Data controllers must also maintain written or electronic records of all categories of processing activities the controller is responsible for, containing the following information:

a. the name and contact details of the controller,

b. the purposes of the processing,

c. a description of the categories of data subjects and of the categories of personal data,

d. the categories of recipients to whom the personal data have been or will be disclosed,

e. an indication of the legal basis for the processing operations for which the personal data is intended,

f. where possible, the envisaged time limits for erasure of the different categories of personal data,

g. where possible, a general description of the technical and organisational security measures adopted,

h. where a processor is used, the name and contact details of the processor: see art 30 GDPR, s 61 DPA 2018.[1]

13. In addition, controllers should document the lawful basis they rely upon for processing personal data. They

[1] For organisations with less than 250 employees, they only need to document processing activities that are not occasional, that could result in a risk to the rights and freedoms of individuals, or that involve processing of special categories of data: Guide to the GDPR, p 182. However as IAS Services are likely to be processing data concerning health, which is a special category of data, it is important they document processing activities, regardless of the size of the organisation.

should also keep records of consent (where applicable), controller-processor contracts, records of any personal data breaches and, in relation to processing of special category data, such as data concerning health, they should have an 'appropriate policy document', as discussed below.

14. Where processing is carried out on behalf of a controller, the controller can only use processers who provide sufficient guarantees to implement appropriate technical and organisational measures to ensure that processing will meet the requirements of the GDPR. Processing by a processor must be governed by a contract, that sets out the processing to be carried out. This contract must, amongst other things, provide that the processor will act only on the instructions of the controller, ensure that the processor has committed themselves to a duty of confidentiality and to delete or return all personal data to the controller: see art 28 GDPR, s 59 DPA 2018.

Processing personal data - principles

15. The GDPR stipulates a number of principles that apply to the processing of personal data: see art 5 GDPR. Those most relevant to the present advice are:

a. *Lawfulness, fairness and transparency.* Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject: art 5(1)(a) GDPR. This means that the controller must identify valid grounds for collecting and using personal data, must not process that data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned, and that that controller must be clear, open and honest from the outset about how personal data will be used: Guide to the GDPR, p 20.

b. *Purpose limitation.* Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those

purposes: art 5(1)(b) GDPR. The data controller should ensure the purpose(s) for which data is collected is documented and that the purpose(s) is/are specified in privacy information given to individuals: Guide to the GDPR, p 24.

c. *Data minimisation*. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed: art 5(1)(c) GDPR. You should not have more personal data than you need to achieve your purpose. Nor should the data include irrelevant details: Guide to the GDPR, p 29.

d. *Storage limitation*. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed: art 5(1)(e) GDPR. Generally speaking, a policy setting standard retention periods for different categories of information, wherever this is possible, will be necessary in order to comply with documentation requirements. Controllers should also periodically review the data they hold, and erase or anonymise it when it is no longer needed: Guide to the GDPR, p 41. The GDPR does not have specific time limits for different types of data. This is up to the controller to determine and depends on how long data is needed for the specified purposes: Guide to the GDPR, p 42. Regulatory requirements and any relevant industry standards and guidelines will be relevant considerations: Guide to the GDPR, p 45. Controllers must take a proportionate approach, balancing their needs with the impact of retention on the individual's privacy: Guide to the GDPR, p 46.

e. *Integrity and confidentiality*. Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures: art 5(1)(f) GDPR.

f. *Accountability*. The controller shall be responsible for and be able to demonstrate compliance with the principles above: art 5(2) GDPR.

16. In turn, the GDPR provides that processing can be lawful on a number of bases. Those most relevant to the current advice are:

a. *Consent:* The data subject has given consent to the processing of his or personal data for one or more specific purposes: art 6(1)(a) GDPR. The GDPR sets a high standard for consent. Consent requires an opt-in, so pre-ticked boxes and other forms of default consent will not be sufficient. Further, vague or blanket consent is not enough. Consent processes must be specific as to who the controller is, the data that is collected, the types of processing and the purposes for which it will be processed. Further, consent should be obtained using clear, plain language that is easy to understand. It is necessary for controllers to keep evidence of consent: who, when, how and what you told people: Guide to the GDPR, p 60. Consent is appropriate as a basis for processing data if the controller can offer people real choice and control over how you use their data. If the controller cannot offer a genuine choice, consent is not appropriate. If the controller would still process the personal data without consent, asking for consent is misleading and inherently unfair (and therefore unlawful). If you make consent a precondition of a service, it is unlikely to be the most appropriate lawful basis. Further, public authorities and other organisations in a position of power over individuals should avoid relying on consent unless they are confident they can demonstrate it is freely given: Guide to the GDPR, p 62-3

b. *Public task:* Processing is necessary for the controller to perform a specific task in the public interest or in the exercise of their official functions, and the task or function has a

clear basis in law: art 6(1)(e) GDPR and s 8(c) DPA 2018. While this 'public task' basis for processing is most relevant to public authorities, it can apply to any organisation that carries out tasks in the public interest (including an IAS Service provided by a charity or other body external from the local authority). The organisation need not have a specific statutory power to process personal data, but their underlying task, function or power must have a clear basis in law. 'Necessary' in this context means that the processing must be a targeted and proportionate way of achieving the purpose in question: Guide to the GDPR, p 75-6

c. *Legitimate interests:* Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child: art 6(1)(f) DPA 2018. This is likely to be the most appropriate basis for processing where controllers use people's data in ways they would reasonably expect and where there is a compelling justification for the processing. To rely on this basis, a controller must identify a legitimate interest, show that the processing is necessary to achieve it and balance it against the individual's interests, rights and freedoms. If the individual would not reasonably expect the processing or if it would cause unjustified harm, their interests are likely to override a processor's legitimate interests. Extra care must be taken to ensure the interests of children are safeguarded, if children's data is being processed: Guide to the GDPR, p 80-1. It should, however, be noted that this basis for processing data is not generally available to a public authority: art 6(1) GDPR.[2] While a public authority cannot rely on legitimate interests for processing carried out in order to perform their tasks as a public authority, if they have legitimate purposes outside the scope of their tasks as a public authority, they may

[2] Local authorities are 'public authorities' for the purposes of the data protection regime, but independent IAS Services – such as those run by charities – are not 'public authorities': s 7 DPA 2018 and Freedom of Information Act 2000.

rely on this basis for processing data: Guide to the GDPR, p 83. However in my view this is unlikely to be relevant to 'in house' IAS Services.

Processing of special categories of personal data, including data concerning health

17. Particular rules apply to the processing of special categories of personal data, including data concerning health. *Data concerning health* means personal data related to the physical or mental health of a person, including the provision of health care services, which reveal information about his or her health status: art 4(15) GDPR.

18. In order to process data concerning health, it is necessary to identify both a lawful basis and also to satisfy one of a number of possible conditions. The conditions most relevant for this advice are: [3]

    a. *Consent:* The data subject has given 'explicit consent' to the processing for one or more specified purposes: art 9(2)(a) GDPR.

    b. *Substantial public interest:* The processing is necessary for reasons of substantial public interest: art 9(2)(g) GDPR. As to what amounts to 'reasons of substantial public interest', the controller must be able to make specific arguments about the concrete wider benefits of their processing. Vague or generic public interest arguments will not suffice: Guide to the GDPR, p 89.

19. A reason of substantial public interest for the purposes of the GDPR includes:

    a. *Statutory and government purpose*: Where the processing (i) is necessary for the exercise of a

[3] The 'health and social care' condition is unlikely to be appropriate, as IAS Services are not themselves providing health or social care.

function conferred on a person by an enactment, and (ii) is necessary for reasons of substantial public interest: s 10(3) and Schedule 1 para 6 DPA 2018.

b. *Support for individuals with a particular disability or medical condition*: where the processing (i) is carried out by a not-for-profit body which provides support to individuals with a particular disability, (ii) relates to data concerning health of individuals with a disability, or their relatives or carers, (iii) is for the purpose of raising awareness of the disability or providing support to individuals with the disability or a relative or carer, (iv) can reasonably be carried out without the consent of the data subject[4], and (v) is necessary for reasons of substantial public interest.

c. *Safeguarding of children and individuals at risk:* Where (i) the processing is necessary for the purposes of protecting an individual from neglect or physical, mental or emotional harm, (ii) the individual is under 18, or over 18 and 'at risk'[5], (iii) the processing is carried out without consent because, in the circumstances, consent to the processing cannot be given by the data subject, the controller cannot reasonably be expected to obtain the consent of the data subject or obtaining consent would prejudice the provision of protection, and (iv) the processing is necessary for reasons of substantial public interest: s 10(3) and Schedule 1 para 18 DPA 2018.

d. *Safeguarding of economic well-being of certain individuals:* Where the processing (i) is necessary for the purposes of protecting the economic well-being of an 'individual at economic risk' who is aged 18 or over, (ii) is of data concerning health, (iii) is carried out without consent because, in the circumstances, consent to

[4] For these purposes, processing can be carried out without consent if the controller cannot reasonably be expected to obtain the consent of the data subject and the controller is not aware the data subject is withholding consent: s 10(3) and Schedule 1 para 16 DPA 2018.

[5] For these purposes, an individual is 'at risk' if the data controller has reasonable cause to suspect that individual has needs for care and support, is experiencing or is at risk of neglect, physical, mental or emotional harm, and, as a result of those needs, is unable to protect himself or herself against the neglect or harm: Schedule 1 para 18(3) DPA 2018.

the processing cannot be given by the data subject, the controller cannot reasonably be expected to obtain the consent of the data subject or obtaining consent would prejudice the provision of protection, and (iv) is necessary for reasons of substantial public interest: s 10(3) and Schedule 1 para 19 DPA 2018. For these purposes, an 'individual at economic risk' means an individual who is less able to protect his or her economic well-being by reason of physical or mental injury, illness or disability: Schedule 1 para 19(3) DPA 2018.

20. In relation to each of these 'substantial public interest' conditions for processing special data, it is necessary for the controller to have an 'appropriate policy document' in place: Schedule 1 para 5(1) DPA 2018. An 'appropriate policy document' must specify the condition or conditions you are relying on for processing special data, the controller's procedures for securing compliance with the GDPR, the controller's policies as regards the retention and erasure of personal data, and an indication of the retention period for the specific data: Schedule 1 para 39 DPA 2018.

<u>Special considerations when processing children's personal data</u>

21. Recital 38 of the GDPR provides:

> Children require 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…

22. If a controller regularly processes children's personal data, it is vital that they think about the need to provide specific protection from the outset and design their processing and systems with this in mind. Carrying out a Data Protection Impact Assessment ('DPIA') is good practice for anyone processing children's data: Children and the

GDPR, p 12. A DPIA is a process to help a controller identify and minimise the data protection risks of a project. A DPIA must:

a. describe the nature, scope, context and purposes of the processing;
b. assess necessity, proportionality and compliance measures,
c. identify and assess risks to individuals (including both the likelihood and severity of any harm being caused to individuals), and
d. identify any additional measures to mitigate those risks: Guide to the GDPR, p 197.

The ICO has produced a sample template DPIA, which I have attached.

23. It is also good practice for a controller to invite the views of children themselves when designing their data processing systems. This can assist in identifying risks, designing safeguards and assessing understanding. It may also be a good idea to consult child's right advocates: Children and the GDPR, p 13.

24. In relation to processing of children's data, where reliance is placed on consent, the controller must ensure that the imbalance of power between the child and the controller is not exploited: Children and the GDPR, p 1, 2. The concept of competence (the child's capacity to understand the implications of their decisions) is relevant. If a child is not competent to consent to processing themselves, then it will usually be in their best interests to allow an individual with parental responsibility to act on their behalf. If a child is competent, then the controller's overriding consideration should still be what is in their best interests, however, in most cases it should be appropriate to let the child act for themselves: Children and the GDPR, p 9. In some contexts, you may be able to make an individual assessment of the competence of a child. However, if this is not possible, you at least need to take

into account the age of the child and the complexity of what you are expecting them to understand: Children and the GDPR, p 16.[6]

25. Alternative bases for processing children's data include the 'public task' basis and 'legitimate interests' basis. In relying on these bases, it is important to recognise that what is 'necessary' in relation to the processing of children's personal data may be different to what is necessary in relation to processing adult's personal data. Further, the best interests of the child should prevail. A DPIA will assist in ensuring that a controller can demonstrate they have protected the rights and freedoms of children and have prioritised their interests over the controller's interests, when this is needed: Children and the GDPR, p 19-20.

Information that must be provided to the individual

26. The GDPR also places obligations on a person receiving personal data to provide certain information: see art 13 GDPR. A data controller, at the time they collect personal data from a data subject, must provide the data subject with the following information:

a. the identity and contact details of the controller,

b. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing,

c. where the lawful basis is 'legitimate interests', the relevant legitimate interests pursued by the controller or by a third party,

[6] The GDPR contains some specific provisions about children's consent in relation to 'information society services' ('ISS') offered directly to children online. These do not apply to IAS Services as the definition of 'ISS' is 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services': art 1(1)(b) Directive (EU) 2015/1535. IAS Services do not provide services that are 'normally provided for remuneration'.

d. the recipients or categories of recipients of the personal data, if any,

e. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period,

f. the existence of the right to request from the controller access to, rectification and erasure of personal data, or restriction of processing concerning the data subject, or to object to processing, and the right to data portability,[7]

g. where the processing is based on consent, the existence of the right to withdraw consent at any time, and

h. the right to lodge a complaint with a supervisory authority.

27. This information should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child: art 12(1) GDPR. The standard method by which privacy information is provided is by the use of a Privacy Notice, which sets out all the necessary content. Where children's data is processed, clear Privacy Notices for children should be used, so that they are able to understand what will happen to their personal data and what rights they have: Children and the GDPR, p 1.

SPECIFIC QUESTIONS

How should services gain consent to deliver their service?

28. The first question I am asked to advise on is how IAS Services should gain consent to deliver their service (a)

[7] If the basis for processing is 'public task', the right to erasure and data portability do not apply: Guide to the GDPR, p 77.

over the phone for short term work, (b) during events when delivering presentations or training on any subject, and (c) in other circumstances where gaining written consent is not possible, especially regarding working virtually or in other arm's-length ways.

29. This question assumes that consent is required in order for IAS Services to lawfully process data. However, in my view consent is not the best or even the appropriate lawful basis to rely on, at least in relation to the provision of advice and training over the phone and virtually. I will consider the delivery of presentations and training events separately.

Delivering services over the phone or virtually

30. As set out above, obtaining consent is one way of ensuring that the processing of personal data is lawful. However, it is not always the most appropriate legal basis to rely on. For the following reasons, reliance on consent by IAS Services is problematic:

a. Consent should not be relied upon as a lawful basis for processing if consent is a precondition of receiving a service. If IAS Services rely on consent, they will need to insist on those accessing its services providing consent prior to providing those services. This raises questions about whether the consent is truly 'freely given' so as to comply with the requirements of the GDPR.

b. Public authorities and other organisations in positions of power over individuals should avoid relying on consent, unless they can demonstrate it is freely given. Moreover, IAS Services will be providing services to children. The power imbalance between IAS Services and a person, particularly but not only a child, seeking to access advice and support may raise concerns as to whether the consent is freely given.

c. Where a child is interacting with IAS Services, there are extra difficulties that arise in terms of ensuring the child is competent to consent to data processing and, if not, in obtaining consent from a person with parental responsibility. Assessing the competence of a child may be difficult where services are accessed remotely, such as over the telephone or online. This may cast doubts on whether fully informed consent has been given by a child competent to do so.

31. Given this, it is my advice that the following lawful bases for processing should generally be relied upon by IAS Services, as an alternative to consent:

a. *Public task*: IAS Services provide the advice and information which local authorities are required to arrange under section 32 of the CFA 2014. That is, advice and information provided to children and young people, and those with parental responsibility, in relation to disabilities and special educational needs. Accordingly, any processing carried out by IAS Services that is necessary for them to provide this advice and information fall under the 'public task' lawful basis. This is because the provision of such advice and information is the performance of a specific task in the public interest, and this task has a clear basis in law, i.e. in s 32 CFA 2014. Therefore, in relation to all processing that falls within the scope of IAS Services' role in providing this advice and information, the 'public task' basis will be the appropriate lawful basis for processing, so long as that processing is 'necessary'. Processing will be necessary if it is a targeted and proportionate way of achieving the purpose in question. Essentially, in accordance with the data minimisation principle, this means that the personal data collected from people and any use of this data should be kept to the minimum required to enable IAS Services to carry out its public function in providing advice and information.

b. *Legitimate interests*: IAS Services may also carry out some functions that fall outside the scope of their public function in providing advice and information. To the extent that this is the case, the 'public task' basis cannot be relied upon in relation to these additional functions. Instead, the appropriate basis will be 'legitimate interests'. In relation to each function in question, it will be necessary for IAS Services to identify the legitimate interest being pursued in collecting and processing personal data, to consider whether this collection and processing is necessary to achieve the legitimate interest, and then to balance the rights of the data subjects in question against the controller's interests in processing the data. Extra care must be taken in this context when it comes to considering children's data. It is advisable in this regard that ISA Services carry out a DPIA, which will ensure they can demonstrate compliance with the GDPR. Alternatively, IAS Services may choose to limit their services strictly to those which fall within the remit of s 32 CFA 2014, so that they can rely exclusively on the 'public task' lawful basis.

32. Without further information on the additional functions which IAS Services carries out, it is not possible to give specific advice as to what processing may or may not be justified on the 'legitimate interests' basis. As a next step, if an IAS Service wishes to go beyond the tasks linked to s 32 CFA 2014, further analysis will required to determine whether the 'legitimate interests' basis will apply to those additional tasks. It is likely that this lawful basis for processing will be adequate to cover all of the processing that IAS Services carries out. However, if this is not the case, IAS Services may need, in some narrow circumstances, to fall back on the less-than-ideal basis of consent.

33. However, in relation to data processing by IAS Services, this is not the end of the inquiry. Given the nature of IAS Services' work, it is highly likely that personal data that is processed will include 'data concerning health', for instance in relation to an individual's disability. This is 'special category' data and, as such, an additional condition must be satisfied before this data can be lawfully processed. For the reasons given above, if possible, it is best for IAS Services to avoid reliance on explicit consent as a basis for processing data concerning health.

34. Instead I would advise that IAS Services rely, where possible, on the 'statutory and government purpose' additional condition. This provides that processing of special category data will be lawful where the processing is (i) necessary for the exercise of a function conferred on a person by an enactment and is (ii) necessary for reasons of substantial public interest. This will apply to processing of health data where this is necessary for the provision of advice and information, as required under s 32 CFA 2014. This is because the provision of advice and information to individuals in relation to disability and special educational needs is a 'substantial public interest'. Reliance on this condition for processing data concerning health is subject to the familiar limitation that the processing must be kept to the minimum necessary for IAS Services to carry out its public function.

35. There however a potential problem with 'Statutory and government purpose' where the IAS Service in a particular area is provided by an independent charity or other body, rather than the local authority itself. In that situation, the 'function' of providing advice and information is not, strictly speaking, conferred on that IAS Service by an enactment, as the duty applies to the relevant local authority. However in my view, considering the language of the legislation (which refers to functions conferred on 'a person'), it is likely to be sufficient that the function is conferred on the local authority (which is a legal 'person') and that processing by the

external IAS Service is necessary for the exercise of that function. However external IAS Services should seek specific advice on this question, and if they are not satisfied that this interpretation of the 'Statutory and government purpose' additional condition is correct, they will need to rely on one of the other additional conditions.

36. Where 'Statutory and government purpose' is not available, reliance might instead be placed on one of the following conditions, but each has its potential difficulties:

a. *Support for individuals with a particular disability or medical condition:* This condition potentially applies to IAS Services, because they are not-for-profit bodies providing support to individuals with a particular disability. The condition will apply to individuals who contact IAS Services who themselves have a disability, or who are a relative or carer of such an individual. However, for the condition to apply, further requirements must be met. The processing of health data must be necessary for the purposes of raising awareness of the disability or providing support to individuals with the disability or their relatives or carers. The individual whose data is being processed must be (or have been) a member of the not-for-profit body in question. Finally, it must be the case that the processing cannot reasonably be carried out without consent. Accordingly, there may be difficulties relying on this condition because (i) as I understand the position, IAS Services are not membership organisations such that the requirement the data subject be a member cannot be met[8]; and (ii) it is unlikely to be the case that IAS Services 'cannot reasonably be expected to obtain consent' in providing their services.

b. *Consent:* Given the difficulties with relying on the above condition, it is very likely that where 'Statutory or

[8] Although it may be that some people will have been members of a charity who provide a particular IAS Service, this will not be the case for everyone who needs to access the services.

government purpose' is not available then 'explicit consent' to processing will be required. Extreme care will need to be taken in obtaining consent from individuals, particularly children.

37. Accordingly, my preliminary advice in relation to gaining consent to deliver services over the phone or in other circumstances where gaining written consent is difficult, such as virtually, is that consent is unlikely to be necessary or appropriate. Instead, IAS Services should rely on the 'public task' and 'legitimate interests' bases for processing personal data, and the 'statutory and government purpose' condition for processing special category personal data, in particular health data. This means that it would not be necessary or appropriate for an IAS Service to require written (or any) consent to be provided before starting to work with a child, young person or parent.

38. There may, nevertheless, be instances where processing of special category personal data is necessary in order for IAS Services to carry out one of their functions, and this function is outside the scope of their public function under s 32 CFA 2014.[9] If this is the case, then further advice will be necessary on how consent should be obtained in these circumstances, which I would of course be happy to provide. I have not addressed the statutory provisions and guidance in relation to consent and explicit consent at this stage, to avoid lengthening this already lengthy advice still further.

Events where delivering presentations or training

39. The first question that is relevant when considering events is whether any 'personal data' is in fact being

[9] Or potentially because the IAS Service is provided by an external organisation, although for the reasons set out above I consider that the 'Statutory and government purpose' additional condition is likely to still be available to external IAS Services.

collected or processed by IAS Services. If IAS Services do not keep a record of who has attended an event, which identifies individuals, then the data protection regime does not apply at all. There will, thus, be no need to consider consent or any other basis for processing personal data.

40. If IAS Services do record the names of people who attend an event or, for example, further personal details such as their email address, then there will be 'personal data' that is collected and processed. As above, the most appropriate lawful basis for this processing is likely to be the 'public task' basis if the provision of training falls within the scope of IAS Services providing advice and information under s 32 CFA. If it does not, then the 'legitimate interests' basis may be available. It is unlikely that, in running an event, IAS Services will be collecting and processing data concerning health – indeed I would advise that such data should not be collected unless strictly necessary. Accordingly, there will be no need to satisfy an additional condition in order for data processing to be lawful.

41. Therefore, my advice is that it is not necessary to gain consent to deliver presentations or trainings, even if the personal data of attendees is collected and processed by IAS Services. However, if personal data is collected then a Privacy Notice should be brought to the attendees' attention.

How should services record consent?

42. For the reasons set out above, I advise that IAS Services avoid reliance on consent as a basis for processing personal data as far as this is possible. However, there are still documentation requirements for IAS Services relying on other lawful bases.

43. IAS Services should develop a Privacy Notice, which identifies the identity and contact details of IAS Services

(the data controller) and records the categories of data subjects and categories of data that they process. The Privacy Notice should identify the purposes for which the Service processes this data and the lawful bases for processing upon which it relies, including any additional condition relied upon for the processing of special category data such as that concerning health. It should also set out the details of anyone with whom data may be shared, IAS Services' data retention policy and the rights of data subjects (as set out above under 'Information that must be provided to the individual').

44. When interacting with a service-user, whether this be in person, over the phone or online, their attention should be drawn to this Privacy Notice. This can be done, for example, by providing a link to the Privacy Notice that is posted online by IAS Services, or by sending a follow-up email that sets out the Privacy Notice therein. A hard-copy of the Privacy Notice might also be provided. Where the service user is a child, a Privacy Notice that is accessible to them should be used.

How should services manage the need for volunteers to make records on case recording systems?

45. The GDPR sets out what can be referred to as the 'security principle'. This is that personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures: art 5(1)(f) GDPR.

46. Further, art 32(1) GDPR provides:

> Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate

technical and organisational measures to ensure a level of security appropriate to the risk.

47. The security principle goes beyond the way information is stored and transmitted. It includes the security measures in place to ensure that the data can be accessed, altered, disclosed or deleted only by those who have authorisation to do so, and that those people only act within the scope of the authority they have been given: Guide to the GDPR, p 228.

48. The GDPR requires a level of security that is 'appropriate' to the risks presented by the specific processing in question, while also taking into account the current state of technology and the costs of implementing measures: Guide to the GDPR, p 228. IAS Services will be dealing with personal data, including data concerning health, that is likely to be very sensitive. Security measures taken should, accordingly, reflect the sensitivity of this data.

49. Factors to consider include:

a. the quality of doors and locks and the protection of your premises,

b. how you control access to your premises and how visitors are supervised,

c. how you dispose of paper and electronic waste,

d. how you keep IT devices, including mobile devices, physically secure,

e. the security of your network and information systems,

f. the security of the data you hold within your system, e.g. ensuring appropriate access controls are in place and that data is held securely,

g. the security of your website or any other online service or application you use, and

h. device security, including policies on how those who bring their own devices to work access and manage data: Guide to the GDPR, p 230.

50. The GDPR requires you to ensure that anyone acting under your authority with access to personal data does not process the data unless you have instructed them to do so. It is therefore vital that your staff and volunteers understand the importance of protecting personal data, are familiar with your security policy and put its procedures into practice. You should provide appropriate initial and refresher training, including:

a. your responsibilities as a data controller under the GDPR,

b. staff responsibilities for protecting personal data, and

c. any restrictions you place on the personal use of your systems by staff: Guide to the GDPR, p 236.

51. Accordingly, while it is beyond my expertise to advise on particular technological solutions that might be deployed by IAS Services, I can advise the following:

a. IAS Services have clear policies in place in terms of how volunteers access IAS Services' physical workplaces and infrastructure. These policies take into account the need to protect against access by unauthorised persons or at times when a person is not permitted to be there.

b. If volunteers access any IAS Services' databases remotely, that consideration be given to the security arrangements surrounding this online platform.
c. That volunteers should be provided training which covers GDPR requirements and their obligations concerning personal data. It should be made clear what limits there are on the personal data they should collect and add to the database, and what information they can and cannot access on the database. Technological solutions might be explored, that could prevent access to certain data by people with a volunteer logon.
d. The volunteers should enter a contract with IAS Services which confirms they will comply with GDPR requirements (and/or any data protection policy developed by IAS Services), that they will only act in accordance with instructions in processing personal data, that they are bound by a duty of confidentiality in relation to the personal data they access at IAS Services, and they will not copy or remove any personal data from IAS Services.

When can confidentiality be breached with regards to safeguarding?

52. There are two distinct issues that arise in the safeguarding context. The first is whether a duty of confidentiality can be breached in order to share information. This is governed by the common law of breach of confidence and is unaffected by the GDPR and DPA 2018. The second is whether the processing of personal data involved in sharing information, for safeguarding purposes, is compliant with the data protection regime. My advice will focus on the latter, which I take to be the thrust of the question here.

53. The Department of Education has issued guidance entitled '*Information sharing: advice for practitioners providing safeguarding services*' (July 2018). Its content provides a useful

summary of relevant data protection considerations, which are equally applicable in IAS Services' context. It emphasises that the GDPR and DPA 2018 are not barriers to justified information sharing but provide a framework to ensure personal data is shared appropriately: Information Sharing, p 4.

54. The guidance suggests that, where possible, information sharing should occur with the consent of the data subject. However, it recognises that it may not be possible or appropriate to rely on consent in all circumstances, such as where the safety of an individual is at risk. In these circumstances, other lawful bases for data processing can apply: Information Sharing, p 4. Given my above advice as to the difficulties of IAS Services relying on consent, I will focus on other lawful bases on which information could be shared for safeguarding purposes. Nevertheless, I advise that IAS Services should include in their Privacy Notice details of when data may be shared and with whom, and that this Privacy Notice should be drawn to the attention of service users. IAS Services should also ensure they have in place clear processes and principles for sharing information internally and with other organisations as necessary.

55. The processing (including the sharing) of personal data must be on a lawful basis. As above, I advise that the most appropriate bases for IAS Services to rely upon are the 'public task' basis and (if 'public task' is unavailable) the 'legitimate interests' basis:

a. *Public task:* Where an IAS Service is provided by a local authority itself, it will be subject to the duty under section 11 of the Children Act 2004 ('CA 2004') to ensure its functions are discharged having regard to the need to safeguard and promote the welfare of children. Where the local authority arranges for someone else to provide the local IAS Service, the local authority must make arrangements to ensure that this service is provided having regard to the need to safeguard and promote the welfare of children: s 11(2)(b)

CA 2004. Accordingly, where it is necessary for an IAS Service to share information for safeguarding reasons, it is very likely to fall within the public task basis for processing. This is because the local authority, or the independent IAS Service, have a function set out in law (the provision of advice and information under s 32 CFA 2014) which must be discharged having regard to the need to safeguard children (s 11 CA 2004) and the safeguarding of children is in the public interest.

b. *Legitimate interests*: As above, to the extent that IAS Services carry out functions that fall outside the scope of the provision of advice and information in accordance with s 32 CFA 2014, then any data processing related to these functions, including data sharing for safeguarding purposes, should be carried out on the legitimate interests basis. Safeguarding is clearly a legitimate interest. It will be necessary, on a case-by-case basis, to determine whether the interest in safeguarding outweighs the data subject's interests, rights and freedoms. It is to be expected that in many cases safeguarding will outweigh the data subject's interests so that information can be lawfully shared.

56. Where the data to be shared for safeguarding purposes includes special category data, such as data concerning health, then an additional condition must be met for data sharing to be lawful. Where explicit consent can be obtained, this will suffice. Nevertheless, as above, there are potential difficulties with IAS Services relying on consent and, in the safeguarding context, this may be particularly problematic. Accordingly, it is most likely to be appropriate to rely on one of the following conditions for processing special category data:

a. *Statutory and government purpose:* Where the safeguarding issues arises in the context of IAS Services carrying out the public function of providing advice and information in accordance with s 32 CFA 2014, this condition can be relied

upon. This is clearly the case in my view for in-house services and is likely to be the case for external services, although as above external IAS Services may wish to seek specific advice on this point. The processing of data is necessary for the exercise of a function conferred on a person by an enactment and for reasons of substantial public interest, namely safeguarding. This will be the simplest condition to rely upon as it neither requires consent nor that consent cannot reasonably be obtained. Accordingly, I advise it should be relied upon wherever possible.

b. *Safeguarding of children and individuals at risk:* As set out above, this condition applies where (i) the processing is necessary for the purposes of protecting an individual from neglect or physical, mental or emotional harm, (ii) the individual is under 18, or over 18 and 'at risk', (iii) the processing is carried out without consent because, in the circumstances, consent to the processing cannot be given by the data subject, the controller cannot reasonably be expected to obtain the consent of the data subject, or obtaining consent would prejudice the provision of protection, and (iv) the processing is necessary for reasons of substantial public interest.

c. *Safeguarding of economic well-being of certain individuals:* This condition applies where the processing (i) is necessary for the purposes of protecting the economic well-being of an 'individual at economic risk' who is aged 18 or over, (ii) is carried out without consent because, in the circumstances, consent to the processing cannot be given by the data subject, the controller cannot reasonably be expected to obtain the consent of the data subject, or obtaining consent would prejudice the provision of protection, and (iii) is necessary for reasons of substantial public interest. For these purposes, an 'individual at economic risk' means an individual who is less able to protect his or her economic well-being by reason of physical or mental injury, illness or disability. However although this condition is available, the previous

condition is more likely to be applicable to information sharing in the safeguarding context by IAS Services.

57. Regardless of the basis for sharing information that is relied upon, the sharing should be necessary, proportionate, relevant, adequate, accurate, timely and secure. That is, the data controller must ensure the information shared is necessary for the purpose for which it is shared, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion and is shared securely. Further, the data controller should keep a record of their decision to share data (or not to share data) and their reasons for it, including the legal basis and conditions upon which they rely: Information Sharing, p 4. It is particularly important that the data sharing is proportionate to the safeguarding concerns, given that sharing personal data in the safeguarding context is very likely to interfere with the individual's rights under Article 8(1) ECHR, and so must be proportionate in order to be justified under Article 8(2). In the final analysis, this means that the decision must strike a 'fair balance' between the individual's rights and the wider public interest in ensuring effective safeguarding of children and vulnerable adults.

How long should services keep files/records for?

58. The GDPR provides that personal data should be kept for no longer than is necessary for the purposes for which the data is processed. It does not stipulate particular timeframes for retention. A number of factors will be relevant to determining the appropriate period of retention, including:

a. The normal frequency with which those accessing advice and information contact IAS Services again, such that keeping a record of prior contact is necessary to provide a good service.

b. Any potential legal liability of IAS Services. It may be necessary to keep records as to advice given until the limitation period for any potential claim has passed.

c. Any need to retain data, whether identifiable personal data or anonymised, for statistical or internal audit purposes.

d. Any other reasons why IAS Services might wish to store the personal data of those who access their services.

59. Having regard to (i) the need or IAS Services to retain information to support any safeguarding enquiries, and (ii) the general limitation period for legal claims which may be brought against IAS Services, it seems to me that in very broad terms retaining information for six years would be compliant with the GDPR. However this can only be very general yardstick, and consideration should be given to whether a longer or shorter retention period is appropriate for any particular data or categories of data. Furthermore if information is received in (for example) 2020 which gives rise to a degree of concern as to the child's welfare, and then further information is received in 2024 which adds to the concern, it may be necessary to retain the original 2020 information beyond 20026, so that it is available if more serious safeguarding concerns arise in (again for example 2028).

60. IAS Services should also have regard to the data retention policies of their wider local authority or host organisation, albeit that it is important that data retention is justified by reference to the specific data in question, not generalised approaches.

CONCLUSION

61. I therefore advise in response to the specific questions posed by IASSN that:

a. Consent should not be relied upon by IAS Services as the lawful basis on which they process personal data, unless this is strictly necessary. As such generally IAS Services should not seek written (or any) consent before starting to work with families. There are other lawful bases that IAS Services can rely upon which will ensure that they are compliant with data protection law. Accordingly, IAS Services should adopt a data protection policy and formulate a Privacy Notice that sets out their reliance on the 'public task' and 'legitimate interests' bases for processing, as explained above. Where health data is processed, then this should be relying on the 'statutory and government purpose' condition wherever possible, as explained above. Service users should be directed to the Privacy Notice when their data is collected.

b. In a narrow set of circumstances, it may be necessary for IAS Services to rely on consent in order to process data. However, I would need further information in order to advise whether this will be necessary and, if so, the process that should be followed.

c. IAS Services should manage the need for volunteers to make records on case recording systems by ensuring that volunteers are provided data protection training and sign contracts which confirm they will comply with IAS Services' data protection policy, that they will only act in accordance with instructions in processing personal data, that they are bound by a duty of confidentiality in relation to the personal data they access at IAS Services and they will not copy or remove any personal data from IAS Services. Volunteers should be given clear instructions about the data they can and cannot access on databases.

d. Sharing of personal data for the purposes of safeguarding can be carried out in accordance with the data protection regime where this is on the ‘public task’ or ‘legitimate interests’ basis, as explained above. Further, health data can be shared for safeguarding purposes where this is within the ‘statutory and government purpose’ condition, the ‘safeguarding of children and of individuals at risk’ condition or the ‘safeguarding of economic well-being of certain individuals’ condition, as explained above. Whenever the sharing of information for safeguarding purposes is considered, IAS Services should document the decision made and the reasons for this, including the legal bases / condition relied upon.

e. As a very broad guide, it seems to me reasonable for IAS Services to retain data for six years, subject in particular to whether any safeguarding concerns have arisen in that period which would justify retention for a longer period. The relevant factors to consider in determining the appropriate period for data to be retained are set out below.

This advice is emailed to the IASSN to allow for immediate action. If I can provide any further assistance, including in developing a data protection policy or Privacy Notice for IAS Services, please contact me at Steve.Broach@39essex.com.

Dated 10 July 2020

STEPHEN BROACH
39 Essex Chambers