Theme 1 Supervisory Authority

No response

Theme 2 Sanctions

Article 36, 5. (See also Article 58 3, c.)

It may be helpful if UK law requires data controllers, including those in the voluntary sector providing social protection services in the public interest, to consult with and obtain prior authorisation from the ICO when a privacy impact assessment for an intended new processing operation meets the threshold in paragraph 1. Such a consultation would enable the data controller to be confident that its risk mitigation measures were fair and appropriate.

Background: The NSPCC currently processes personal data and special categories of personal data for purposes in the public interest. These include providing a helpline to which members of the public can report concerns that a child may be at risk of harm, and to which professionals may report concerns ('whistle-blowing'). The NSPCC is designated as a prescribed person under the Public Interest Disclosure Act. From time to time, the NSPCC has provided a dedicated helpline service on behalf of another data controller, for example the Home Office's Modern Slavery Helpline or the IICSA witness helpline. Such partnerships might well in future be subject to the requirements of Articles 35 and 36.

Article 83 and Article 84

In relation to the general conditions for imposing administrative fines, Article 83, 7, allows a member state to lay down rules for administrative fines on public authorities and bodies. However, there is no provision for rules relating to fines for voluntary sector data controllers such as the NSPCC other than Article 83 paragraphs 4 and 5 where annual turnover is used to set fines. We ask that the rules the UK will set as allowed by paragraph 7 include voluntary sector data controllers such as the NSPCC who are processing personal data for public interest purposes.

Theme 3 Demonstrating Compliance

No response.

Theme 4 Data Protection Officers

No response.

Theme 5 Archiving and Research

Article 89

Paragraph 2: We ask that the UK Regulations provide for derogations from the rights referred to in Articles 15, 16, 18, and 21. The derogations should be similar to those in s33 of the Data Protection Act 1998.

Paragraph 3: We welcome the provision for derogations in relation to archiving purposes which are in the public interest. We ask that the UK Regulations provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21.

/ continued -

Background: The NSPCC processes personal data and special categories of personal data in order to evaluate the effectiveness of its services in protecting children from harm. We also conduct research in order to establish policy and campaigning objectives, for example our research into the prevalence of sexual abuse of children. These research objectives are in the substantial public interest. Where practicable and fair, we obtain the consent of data subjects but there are circumstances where we rely upon the provisions of s33 of the Data Protection Act and safeguards such as our research approval process. The NSPCC processes personal data and special categories of personal data for archiving purposes in the public interest. This includes our case work with children and families and data relating to cases where the NSPCC used its statutory powers in the Children Act to apply to the Court to have a child taken into care. We have a records retention policy for such archived data and access is controlled.

Theme 6 Third Country Transfers

Article 49

1, d, 4 and 5: We ask that transfers to third countries for reasons of protecting any child from the risk of harm are recognised as being necessary for important reasons of public interest. We ask that the UK Regulations should make that clear.

Theme 7 Sensitive personal data and exceptions

Article 9

Condition g: We ask that the UK Regulations provide for the processing of special categories of personal data in line with the existing provisions in SI 2000 No. 417, section 4.
Background: The NSPCC provides confidential advice, counselling, and support services as part of our face to face social work, our child protection Helpline (includes whistle-blowing by professionals, and ChildLine. These services are in the substantial public interest. It is often not possible to obtain the explicit consent of all the data in the context of these services and indeed asking for such consent would make the provision of such services impossible.

Condition h: We ask that the UK Regulations provide for the processing of special categories of personal data in line with the existing provisions in Data Protection Act, Schedule 3, condition 8 in respect of health data, and SI 2000 No. 417, section 4 in relation to social care purposes.
Background: The NSPCC delivers services which are in the substantial public interest in partnership with health professionals. For example, we work in multi-disciplinary teams and may hold health information about parents and children where it is necessary for our services. While in most cases we have the explicit consent of data subjects (or parents on behalf of children) to process the data, consent is not always obtainable and would in any case prejudice the delivery of the service.

Condition j: We ask that the UK Regulations provide for the processing of special categories of personal data in line with the existing provisions in SI 2000 No. 417, section 9.
Background: See our response to Article 89. The NSPCC processes personal data and special categories of personal data in order to evaluate the effectiveness of its services in protecting children from harm. We also conduct research in order to establish policy and campaigning objectives, for example our research into the prevalence of sexual abuse of children. These research objectives are in the substantial public interest. Where practicable and fair, we obtain the consent of data subjects but there are circumstances where we rely upon the provisions of s33 of the Data Protection Act and safeguards such as our research approval process. The NSPCC processes personal data and special categories of personal data for archiving purposes in the public interest. This includes our case work

with children and families and data relating to cases where the NSPCC used its statutory powers in the Children Act to apply to the Court to have a child taken into care. We have a records retention policy for such archived data and access is controlled.

Theme 8 Criminal Convictions

Article 10

We ask that the UK Regulations provide for cases where the processing of personal data relating to criminal convictions and offences is authorised in UK law. In particular, we ask for provisions equivalent to s29 (1) and (3) of the Data Protection Act, and SI 2000 No. 417, sections 1, 2 and 9. *Background: the NSPCC's child protection Helpline receives allegations about criminal offences. This data is passed to social services and the police for investigation. The NSPCC does not itself investigate alleged offences but may receive feedback from social services and police as to the outcome of their investigations. The NSPCC is sometimes required to disclose personal data relating to criminal offences for the purpose of evidence in criminal proceedings. We also process data about criminal offences allegations in the course of providing our Childline confidential counselling service and our social work with children and families.*

Theme 9 Rights and Remedies

Article 17 Right to erasure ('right to be forgotten')

The NSPCC are pleased to see that 'the right to erasure' has been incorporated into the GDPR and that recital 65 makes reference to the specific needs of children who may not be 'fully aware of the risks involved by the processing, and later want to remove such personal data'. Children and young people must be given the space to explore their identities and experiment, without content that they produce or share following them into adulthood.

However, the GDPR contains no definition of what a child is, and we would like clarification around this point. The United Nations Convention on the Rights of the Child (UNCRC) defines a child as someone who is younger than the age of 18, and such treaties are recognised to take primacy. The NSPCC would like to see the Information Commissioner's Office (ICO) as the UK's Data Protection Authority and other authorities across the EU expressly confirm an agreed age, for the purpose of the GDPR, that will be used to define a child.

Theme 10 Processing of Children's Personal Data by Online Services

The first clause of Article 8 states the need for parental consent in relation to the processing of data by information society services when the child is under the required age (13-16 depending on the derogation adopted by the UK). We would similarly like clarification on how this consent will be obtained, and consideration of what the impact will be for young people if methods to gain this consent vary between countries.

It remains unclear what the age of consent for accessing information society services will be in the UK. The NSPCC are highly concerned that young people have not been consulted in this decision, contravening Article 12 of the UN Convention on the Rights of the Child. It is essential that an

independent evaluation or impact assessment is carried out. Young people's understanding of personal data must be explored, as well as the impact that social networking sites have upon young people at different stages of their development must similarly be consulted.

Once an age has been established, it is critical that social networking sites implement appropriate age verification processes. We know that underage children are accessing social networking sites before they reach the required age:

- From a survey of nearly 1700 young people, the NSPCC found that 66% had accessed the most popular social networking sites, apps, and games with an age rating of 13+, before they had reached that required age[1].

There should be an obligation applied to social networking sites to demonstrate that they are not acting negligently and allowing underage children to access their services. Even when services are not directly targeted at young people, proper age verification processes must be in place, to prevent them from accessing age inappropriate material. Article 8 refers to the requirement to make reasonable efforts to obtain parental consent regarding data use. We would like the standard of 'reasonable efforts' to be set high, and explicitly stated. If age 16 is adopted by the UK without proper age verification procedures, the NSPCC are concerned that offenders engaging in sexual activity with children on the site will be able to justify their actions on the basis that they could reasonably assume all users were above the age of consent.

We are pleased to note that Childline and other online counselling services are considered a service of the type referred to in Recital 38, and that any requirement for parental consent at any age would prejudice the provision of that service and be contrary to the public interest.

Article 40: Codes of conduct and certification

We are pleased to see that Article 40 encourages in paragraph 2, g the establishment of codes of conduct regarding 'the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained'. We welcome the powers given to ICO as the competent supervisory authority to enforce providers of information services to comply with such codes. The NSPCC believes that the websites and apps that children access should be built with their safety in mind, with minimum standards and measures in place to ensure children and young people can safely and appropriately inhabit online spaces.

Theme 11 Freedom of Expression in the Media

Article 85

We ask for derogations as permitted in paragraph 2 which in line with those in s32 of the Data Protection Act. We support responsible journalism where publication is in the public interest.

[1] NSPCC research on file with the NSPCC.

Theme 12 Processing of Data

Article 6, 2 c and e, and 3 (Lawfulness of processing)

- **and Article 18, 2, and Article 88 (processing in the context of employment).**

We ask that the legal bases for processing (fair processing conditions) as expressed currently in Schedules 2 and 3 of the Data Protection Act, and SI 2000 No.417 are incorporated in the UK Regulations as permitted by Article 6. This is particularly important for us where we are carrying out processing in the public interest of protecting children from harm.

Article 88, 1 We ask that the UK Regulations provide rules for not only employees but for other types of worker and for volunteers who work to help deliver our services.

Theme 13 Restrictions

Article 23

We ask that the UK Regulations incorporate the provisions in SI 2000 No. 415, section 5. The right of access by the data subject as set out in Article 15, (social work contexts) needs to be qualified where it is likely that disclosure of personal data would cause serious harm to the data subject or any other person's physical or mental health.

We also ask that the UK Regulations impose restrictions as set out in Article 23, 1, a to j inclusive. These are likely to reflect the provisions already in the Data Protection Act. We see 1, i, as being particularly important in relation to Article 15, the right of access by the data subject.

Background: We understand the restrictions must be on a case by case basis and must be applied fairly. Our social work records often contain information which is confidential to other persons so we need the Regulation to allow for the rights and freedoms of those other persons. In some cases, for example ChildLine counselling records where a young person has expressed suicidal feelings, the young person might self-harm if they were to be provided with all their personal data.

Theme 14 Rules surrounding Churches and Religious Associations

No response.