RCNI submission on the General Scheme on the Data Protection Bill 2017

June 20th 2017

- **Introduction**
- **Three priority areas**
  - **Statutory Exemption from Fines**
  - **Consolidated legislation**
  - **Digital Age of Consent**

Introduction:

Rape Crisis Network Ireland (RCNI) is a national level specialist NGO on the issue of sexual violence, representing survivors of sexual violence and owned and governed by Rape Crisis Centres who deliver a range of services to survivors of sexual violence.

This submission is informed by our pioneering expertise in data collection in the NGO sector, our partnership and collaboration with IT, legal, regulatory and academic expertise and our ongoing challenges and problem solving around what and how we collect and how we protect and serve our clients, survivors of sexual violence. That said we are by no means GDPR experts, we have a lot more questions than answers and a lot more to learn. We represent only RCNI and have no authority or mandate to represent other charities but where we know our experience and analysis is pertinent to the wider charity sector we have noted same below.

Background: Rape Crisis Centres in the course of their service delivery are recipient of highly sensitive personal data. RCNI has, over the past decade, built a data collection best practice system to standardize, collect and quality control data collection across the sector. EIGE[1] have recognized the RCNI system as a best practice model in Europe http://eige.europa.eu/gender-mainstreaming/good-practices/ireland/rape-crisis-network.

We recognize that data protection is a core competency of any data collection activity we undertake and have supported and certified data collection officers (DCO) in each participating centre. In the past three years we have been engaged in negotiations with the statutory funder regarding data sharing and data protection. These negotiations are set against a background of uneven data protection knowledge and remain incomplete.

All data RCNI collects from survivors is sensitive data. Bearing in mind the continued endemic and systemic levels of sexual violence and the failure to prosecute and the stigma attached to sexual violence, the majority of victims of these crimes choose to maintain privacy from their family, friends, work colleagues and/or others and from statutory agencies such as social services or the police force. For Rape Crisis Centres, 65% of clients choose not to be known to the formal state authorities which raises particular considerations regarding consent, and data sharing demands by statutory funders.

Upholding privacy is critical for RCNI and RCCs. At stake is the fundamental Rape Crisis model which commits to providing survivors with a safe place. For the majority of survivors this means confidential and non-statutory. If we fail, survivor trust and access to our services will be jeopardised.

Context: While not a matter for the Joint Oireachtas Committee on Justice and Equality the context under which we comply with GDPR and this proposed legislation might be noted.

RCNI data protection or collection capacity is not funded by the state and RCNI are by no means unusual in this. The NGO sector in Ireland employs approximately 133,000 staff, with almost 19,500 organizations registered, 5,500 of those in health, social services, development and housing, spending €4.6bn of the total NGO spend of €19.5bn.[2]

In order to ensure the rights of the people charities serve, we urgently need to understand NGOs' data engagement, to develop an appropriate support structure for the NGO sector's

[1] EU Commission agency European Institute of Gender Equality
[2] https://benefacts.ie/Explore

compliance with GDPR including a budget, and possibly to legislate to protect our independent data protection capacity in particular vis a vis state agencies that fund us.[3]

The principal obstacle to compliance we would see for ourselves and indeed many organizations across the NGO sector, is

- The absence of data protection resources from statutory sources who fund our service provision to meet statutory duties.
- Terms and practice with regards contractual relationships between the State and NGOs in the delivery of public duty services, with regards data protection, giving wide scope for demanding data sharing not matched with resourcing the data controller NGOs with data protection capacity[4].
- An increasing emphasis by public bodies on seeking to have charity partners fully indemnify the public body.

The provision that NGOs are bound by law in data protection matters and that ignorance is no defense does not in itself overcome said ignorance based on insufficient capacity and support and reinforced in potentially compromising and highly unequal funding arrangements.

Priority 1

Head 16 Statutory exemption from Fines *(Relevant Heads, Articles, etc listed at end of submission for your information).*

For an NGO such as ourselves the duty we have to individuals, our data subjects, is often in the context of relationships with state agencies. The principal of checks and balances on the state in the protection of the individual is well established. Exemption for the public sector to the fullest range of sanctions would seem to go against this principal and furthermore may have the impact of placing an intolerable burden on non-state organisations such as Charities who continue to carry full responsibility for data protection in any relationship with statutory agencies.

The State's apparent exemption from paying fines, unless acting as an "undertaking" within the meaning of Section 3 of the Competition Act 2002, is not readily justifiable in

[3] An example in comparison is the Health Research Board Data Project which published a discussion document in 2016 following four years of scoping, consultation and research into infrastucture needs. They are currently preparing a white paper for government on these outcomes.

[4] Currently service level agreements with Rape Crisis Centres (RCCs) and the Irish statutory funders require RCCs to ensure consent from third parties - eg clients and service users for the purposes of complying with contractual obligations to share data the contracts purport 'belong' to the funder. Funding can be withdrawn from RCCs who do not ensure such consent and on that ground refuse to share client data. The EU GDPR is a very welcome regulation given this reality.

circumstances where private companies will themselves be liable for fines for data protection breaches.[5]

This exemption will mean that there will be only limited financial sanctions for statutory breaches of data protection law which could be very wide-ranging and could have serious consequences for many individuals, given the size and complexity of many data sets controlled and accessed by Government agencies.

It seems clear that it is not the intention of the General Data Protection Regulation to tip the scales of justice in favour of very large State agencies and against the individual, but rather to ensure that each member State has a wide discretion in deciding where and to what extent, to impose financial sanctions against State agencies themselves.

While a regime providing for very limited financial sanctions against State agencies is clearly possible under the GDPR, it does not do anything either to encourage compliance by those agencies, or to maintain the balance of rights between the State and the individual as far as data protection is concerned.

It should be borne in mind that the NGO sector is a significant repository of sensitive personal data, much of which is collected by NGOs in the context of the delivery of publicly funded services. This funding relationship is increasingly characterised by charities being asked to fully indemnify state bodies.

Cases for damages and other sanctions, should the statutory agents behaviour result in breach, will likely first and foremost punish the charity. Therefore, should there be insufficiently high data protection standards and behaviours in statutory agencies, charity partners may be left carrying the intolerable burden of being liable to fines, damages and sanctions should we fail to hold the State to standards it may not choose to hold itself to.

In effect the public sector, in relation to some of the most vulnerable subjects, may be protected from lability by the Charity sector over whom it wields considerable control. The capacity of the charity sector to robustly and independently carry out our GDPR duties with regards our data subjects vis a vis the state in particular must be considered.

Again it might be pertinent to note that currently charities cannot avail of, that we are aware of, a government funding stream to aid compliance or employ the obligatory GDPR data protection officers. Should such a funding stream come online to support NGO GDPR compliance, the independence of that arrangement would need to be addressed, perhaps through legislation.

[5] **Section 3, Competition Act 2002 – definition of "undertaking":** "undertaking" means a person being an individual, a body corporate or an unincorporated body of persons engaged for gain in the production, supply or distribution of goods or the provision of a service.

We do not believe the particular relationship of the Charity sector to the State has been considered in this section of the general scheme which currently concerns itself with the competitive relationship of public and private undertakings.

Recommendation 1: Accordingly RCNI recommends that the apparent exemption from liability to financial sanctions for data breaches, is removed from State agencies, whether or not they are acting as "undertakings".

Recommendation 2: Further, we recommend that consideration should be given to any legislative measures needed to ensure the highest standards in public commissioning and contracting of services through NGOs such that NGOs are inoculated from coercion or pressure into risky and illegal practices of data sharing.

Recommendation 3. We recommend that consideration should be given to possible legislative measures that would support the independence of publicly funded NGO DPOs from NGO public funding bodies.

Recommendation 4: We would suggest directing fines that public sector bodies are subject to towards the NGO sector specifically to enhance our data protection capacity. There are practical precedents for same, for example the vast majority of prosecutions for electronic marketing offences result not in a financial penalty paid to the State but in an agreed resolution where a donation is made to a Charity. This has the benefit of negating the undesirable circular movement of funding in the public exchequer and of simultaneously enhancing civil society's capacity to independently and robustly advocate for the data protection and privacy rights of individual vis-a-vis public bodies.

Priority 2 Consolidated legislation

The intention of GDPR is to empower data subjects though accessible instruments and clarity under the law. It cannot achieve this if the legislation lacks transparency and is overly complex. Therefore, RCNI recommends that this Data Protection Bill should be a consolidating statute, replacing all existing Data Protection legislation, repealing, amending, and/or adding to it as necessary.

If all statute law is contained in one document, it becomes much more accessible to those it seeks to protect. If on the other hand, it becomes necessary to consult several statutes and work out how they interact with each other, it becomes difficult to access and is likely to be consulted and used less often. Such difficulties will not help to empower data subjects whose rights are supposed to be enhanced by this legislation. Ease of reference is in the interests of fairness and transparency and should be one of the guiding principles in drafting this (or any) legislation.

3. Digital Age of Consent to online services (GDPR Article 8)

While older children should be afforded appropriate and progressive autonomy the possibility of parental control remains important, particularly when we know the digital world to represent opportunity for exploitation and harm. On the other hand the provision of digital support information and services to this, sometimes hard to reach cohort, for example in mental health outreach, should be enabled as far as possible. We look forward to reading the result of the government consultation on the matter and commenting further at that point.

Address: RCNI, Carmichael Centre, North Brunswick St., Dublin 7.
Email: Director@rcni.ie
Phone: 01 8656955 or Clíona Saidléar on 087 2196447

Appendix: General Data Protection Regulation Articles and Heads of General Scheme of the Data Protection Bill cited above

1. Exemption of Fines - Enforcement powers of supervisory body

GDPR Article 83 Powers of supervisory body to impose fines

General conditions for imposing administrative fines 1.Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive. 2.Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; (b) the intentional or negligent character of the infringement; (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects; (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32; (e) any relevant previous infringements by the controller or processor; (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; (g) the categories of personal data affected by the infringement; (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement. 3.If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement. 4.Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; (b) the obligations of the certification body pursuant to Articles 42 and 43; (c) the obligations of the monitoring body pursuant to Article 41(4). 4.5.2016 L 119/82 Official Journal of the European Union EN 5.Infringements of the following provisions shall, in

accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1). 6.Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. 7.Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State. 8.The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process. 9.Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

GDPR Article 58(2)

2. Each supervisory authority shall have all of the following corrective powers: (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation; (b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; (c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation; 4.5.2016 L 119/69 Official Journal of the European Union EN (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; (e) to order the controller to communicate a personal data breach to the data subject; (f) to impose a temporary or definitive limitation including a ban on processing; (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19; (h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met; (i) to impose an administrative fine pursuant to

Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case; (j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

GSDPB Head 23:
Imposition of administrative fines on public authorities and bodies (Article 83.7)
Provide that:
1. Pursuant to Article 83.7, an administrative fine may be imposed on a public authority or body in respect of an infringement of the Regulation arising from its activity as an undertaking.
2. In this Head, "undertaking" has the meaning given to it in section 3 of the Competition Act 2002.

Explanatory notes
Article 83 of the General Data Protection Regulation provides for the imposition of substantial fines on data controllers or data processors for infringements of its provisions. However, paragraph 7 provides as follows:

- *7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.*

A decision not to impose such fines on public authorities and bodies could possibly create competition distortions in areas in which public and private bodies operate in the same space (e.g. public and private hospitals; public and private refuse services).

A possible solution would be to keep the possibility of fines open where public and private bodies provide goods or services in the same market; this would require a distinction to be drawn between categories of public bodies.

A focus on the concept of "undertaking" in competition law is a possible way forward. Irish case law suggests that it is necessary to analyse each activity of a public body separately and consider the circumstances in which it is performed.

The High Court has, for example, ruled that the HSE is an undertaking when providing ambulance services to private patients – Medicall Ambulance Service Ltd v HSE [2011] IEHC 76 – but not when providing the same service to public patients – Lifeline Ambulance Services Ltd v HSE [2012] 432. In Medicall, the Court noted that the HSE was involved in economic activity (as opposed to a regulatory or administrative function) because it provided the service for gain and was in competition with private operators, whereas in Lifeline the Court appeared satisfied that the service for public patients was provided in the public interest and not for gain.

3. Digital Age of Consent

GDPR Article 8

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

EU Directive 2015/1535 *"information society service" means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council**1**;*
1 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

GSDPB Head 16

GSDPB Head 16: Child's consent in relation to information society services [Article 8]
Provide that
For the purpose of Article 8 of the Regulation, [ ] years shall be the age below which data processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Explanatory notes
A separate Government decision will be sought on "the digital age of consent" for the purposes of this Head.
Article 8 of the Regulation (below) permits Member States to specify an age which is lower than 16 years:

1. *Where point (a) of Article 6(1) applies [i.e. processing based on data subject consent], in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.*
Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.
2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.
3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.