BRIEFING NOTE

USAID OIG / A4ID WORKSHOP

INTRODUCTION

In common with many of our Institutional Donors, USAID – and their investigative body, the Office of the Inspector General (OIG) – exercise functions designed to detect and prevent fraud and various types of misconduct. These may include both monitoring and reporting functions (measuring partners' effectiveness as well as instances of misconduct), and detective and responsive functions (i.e. intervening where appropriate).

These functions manifest in requests and requirements to share information – both in the form of **'reporting' requirements** to inform USAID/OIG of various types of misconduct as well as **'continued cooperation' requirements** – i.e. participating in investigations carried out by OIG in response to instances of misconduct or fraud.

We have a common interest in preventing and responding to misconduct, abuse, and fraud; we also have a common interest in doing this as part of a broad ecosystem, which inspires trust and allows effective programming. However, there are challenges to sharing information – within Data Protection law – and in particular, across international borders.

These challenges begin in our understanding, and develop through various dimensions – including legal challenges deriving from Data Protection Law in the European Economic Area (EEA), as well as considerations of Survivor-Centrism, Whistleblower and Witness Protection, and risk to the individuals involved.

Many of us have not yet established a clear framework based on an adequate understanding of these dimensions and rooted in comprehension of relevant dataflows and their implications. We have not established consistency in our approaches multilaterally.

This has various harmful consequences – our approaches are inefficient and wasteful, they may introduce data protection risk through incoherent practice, they it may also prevent effective action (where taken in the public interest) to prevent various types of fraud and misconduct, and they may produce tension with donors and make trust challenging.

This briefing paper explores where some of the Data Protection challenges are and proposes how we might consider them and what type of solutions we might be able to consider.

THE DATA PROTECTION CHALLENGE

We propose that there are four key problem areas in Data Protection Law.

Resolving all four – and establishing proportionality and necessity more broadly – requires consensus regarding how data will be used – where it will go, what decisions it will inform, and what consequences will be produced for those to whom it relates.

ESTABLISHING A LEGAL BASIS FOR SHARING

Our best understanding of use cases proposed by OIG is that it is likely to be challenging to establish a legal basis rooted in a statutory provision or common law task – i.e. opening the "Public Task" basis – or one rooted in an obligation linked to employment (i.e. "Contract").

Public Task (or Legal obligation) would in many ways be the ideal choice. It could be a strong choice in the event of multinational agreement or consensus amongst international development agencies regarding the importance of protective functions and cooperation.

In the absence of this agreement Legitimate Interest (LI) might be applicable. Using LI, our challenge becomes one of passing the balancing test – i.e. concluding – based on an understanding of the proposed dataflows – how a compelling overriding interest (for instance, to prevent crime, misconduct, and fraud) consistently outweighs risks to the rights and freedoms of individuals.

Choosing the right legal basis requires in the first instance a clear understanding of how data will be used, and – particularly in the case of LI – a balancing assessment underpinned by understanding of the risks to individuals involved, which may vary between countries and contexts.

Establishing a Special Category Processing Condition

Given any large scale reporting of identifiable misconduct we are likely to need to share details of criminal activity, sexual life or orientation, and potentially data on race/ethnicity or religion, where allegations relate to Human Resources issues or are motivated by a victim or survivor's protected characteristic.

These categories of data are proscribed as Special Category under GDPR (or treated with heightened restrictions under national legislation) and require additional conditions to be fulfilled to make their use legal. We should therefore consider Condition to use.

The only Special Category Processing Condition which is likely to be a good fit for misconduct reporting is a Substantial Public Interest Condition – aligning with purposes such as prevention of unlawful acts, protection against misconduct, or necessity in preventing unlawful acts, dishonesty and malpractice – based on an understanding that the transfer to OIG is architected for these purposes.

Finding an appropriate safeguard or Derogation for Transfer outside the EEA

GDPR prohibits transfer outside the EEA in circumstances where a safeguard or derogation does not apply, preventing the export of data to jurisdictions with weaker legal protections. Many of the safeguards one might use as part of a commercial dataflow (e.g. a Contractual Framework or Privacy Shield registration) are clearly not appropriate when dealing with a Government Agency.

The best fit is likely to be *an "important reason of public interest"* – while noting that that the EUDPB/WP29 guidance is clear that *"it is not sufficient that the data transfer is requested (for example by a third country authority) for an investigation which serves a public interest of a third country which, in an abstract sense, also exists in EU or Member State law."*[1]

[1] Guidelines on Article 49 of Regulation 2016/679 – WP29/EUDPB

Our challenge, then, becomes establishing that the intended use of the data would serve a public interest as defined by the EU or member state law – such as a common law obligation or *"international agreement or convention which recognises a certain objective and provides for international cooperation to foster that objective"*.[2]

SUCCESSFULLY ACCOUNTING FOR THE RISK TO WHICH DATA SUBJECTS MAY BE EXPOSED

While broad requirements to balance need and risk exist throughout GDPR, we consider that an explicit and governed obligation exists where we are required to carry out a Privacy Impact Assessment (PIA) to account for them with a high level of diligence.

GDPR is clear that if we cannot account for this risk, prior regulatory consultation may be needed – we have discussed in the past as part of work with A4ID carrying out this consultation process collectively should risks be insurmountable.

We propose that various factors make a PIA unavoidable for most of us, including the cross-border transfer, scope and scale of transfer, vulnerability of data subjects, and heightened public awareness of uses of data of this type.

A PIA linked to a protocol and collective understanding is also likely to be helpful in cementing understanding, producing transparency and accountability, reducing cost, and ensuring that our actions robustly consider privacy by design in a demonstrable manner.

Viewed through this lens (and having established that a legal pathway exists to sharing information) the single remaining obligation of an assessment of the impact under GDPR then remains to establish the *"risk to the rights and freedoms of natural persons [..which..] may result from personal data processing"*.[3]

Doing this requires mapping the consequences – both intended (e.g. civil or criminal action targeting perpetrators; involvement in follow-up investigation for whistleblowers or witnesses) and unintended (e.g. inadvertent 'tipping off' of communities, retribution, re-traumatising survivors or bystanders, breaches of employment or other statute).

From an understanding of the consequences which are likely and intended – and which have a defence in public interest or based on their probability – we may be able to agree on mitigations which ideally are rooted in and documented as common practice with OIG as an alternative to consultation.

SURVIVOR CENTRISM AND WHISTLEBLOWER PROTECTION

Whistleblowing has "*a key role in exposing and preventing [threats or harm to the public interest] and in safeguarding the welfare of society*".[4]

Our sector is increasingly recognising that programming, misconduct disclosure and follow-up, and safeguarding approaches which consider **survivors' rights and needs**, treat survivors with dignity, and empower them to choose next steps which are right for them – sharing power and maintaining privacy and confidentiality – represent a minimum standard for respect and dignity.

The consequences of data sharing, and the risk associated with its processing, clearly have deep significance in the context of approaches which are survivor-centric and which protect whistleblowers. Data sharing which

[2] As above
[3] GDPR Recital 75
[4] DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

produces distress or discourages reporting – or which forms part of processes with prejudicial, disempowering, or unsafe will not be compatible with either approach.

Our solution must not only consider risk to data subjects as a dimension of respecting the right to privacy, but also consider risk and scope in the context of a rights-based survivor-centric approach, and encourage and facilitate open and forthright reporting of misconduct.

SOLUTIONS

While we may individually conclude solutions to many of these legal and risk challenges, a collective approach may open up better solutions – e.g. one aligned on a common protocol, code of conduct, or multinational agreement.

We propose that a solution needs to embrace several key steps:

1. **Understanding OIG's role, function, and use of data**
2. **Map dataflow**
3. **Concluding legal analysis,** which is harmonised and compatible if not identical
4. **Designing reporting, which is compatible with GDPR, survivor-centric and whistleblower-respectful considerations**
5. **Understanding what collaboration (e.g. investigation) may look like,** which meets the same considerations

Practical steps along this journey could include:

- **Agreeing a common PIA with risk mitigations,** which we can either **apply to our processes** or which represent **cross-cutting work** we may need to do together.
- **Considering what underpinning instrument might be useful or wise** – e.g. Code of Conduct, Protocol, MoU, standard.

The issues which we might choose to treat as part of a PIA or common protocol might include:

I. **Understanding when our investigations are of high quality** – i.e. an NGO "good investigations" standard. We propose that at this standard we might be well-placed to conclude or propose that little or no "use" of data which affected Subjects might be used by institutional donors by OIG beyond scrutinising *our* processes – i.e. in effect acting as a mitigation for *most* risks precipitated by consequential use of data about individuals through a form of 'self-regulation'.

II. **Understanding and mitigating further uses of data by institutional donors,** such as triangulation, or blacklisting. Mitigations for this may be as simple as understanding and communication – as agencies and to our communities. In the case of other institutional donors, they might include clearly agreed-upon red lines; easier where we have collective agreement.

III. **Mapping consequences for subjects of concern and mitigating pathways to harm particularly with a view to survivor-centrism and whistleblower protection** – acting as a mitigation for *most* risks precipitated by consequential use of data about individuals who are survivors or whistleblowers – i.e. the most vulnerable data subjects. These consequences and risks might include re-traumatisation, risk of harm or intimidation locally, or in the most serious cases honour killing or other revenge actions.

IV. **Understanding, where donors' use of data involves proactive activity such as audit or further investigation** – e.g. where condition 'I' is not met and therefore a donor "leans in" to carry out action themselves, what this process looks like and how we can understand that it is safe and low-risk – or what mitigations we may need to put in place.

V. **Developing approaches to support our legal analysis –** e.g. a firm ask for *agreement between* DFID / USAID / other institutional donors, which firmly establishes legal analysis, or for *information sharing through law enforcement* channels.