DPIA – Inter-Agency Misconduct Disclosure Scheme [TEMPLATE: UK- specific]

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
The Inter-Agency Misconduct Disclosure Scheme for the Sharing of Safeguarding-related Misconduct (the Scheme) aims to establish a minimum standard for participating humanitarian, development and other civil society organisations (Participating Organisations) to share upon request relevant information about people who have been found to have been involved in or committed Misconduct, during employment or in a governing role, for the primary purpose of making informed recruitment/appointment decisions. For the purposes of the Scheme, **Misconduct** covers sexual abuse, sexual exploitation and sexual harassment (as these terms are defined by the UN or the codes of conduct of Participating Organisations). Sexual harassment qualifies as Misconduct for purposes of the Scheme where it has resulted in dismissal/termination of office or otherwise indicates a serious safeguarding risk. The project complements the work that organisations are already doing as part of their recruitment processes and reflects a widely a recognised need in the sector to prevent those involved in Misconduct moving between organisations and repeating such misconduct. The Scheme and accompanying Explanatory Notes set out the aims of the project and the type of processing it will involve.

Step 2: Describe the processing

Describe the nature of the processing: *how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?*

Organisations participating in the Scheme (**Participating Organisations**) will share Misconduct History (see below) relating to data subjects who work, or have in the past worked, for the Participating Organisation as an employee, or in a governing position, with other Participating Organisations.

Participating Organisations will:

- only request the personal data as part of their recruitment processes (i.e. the process by which each Participating Organisation assesses the suitability of an individual for a position);
- use the form at Appendix 1 of the Scheme (the **Statement of Conduct**) to respond to a request for information;
- use information contained in Statement of Conduct to inform their decision as to whether to hire or appoint the data subject.

The Scheme requires each Participating Organisation to process personal data contained in a Statement of Conduct in accordance with applicable data protection policies, legislation and regulations. Accordingly, each Participating Organisation must put in place compliant measures for transferring, storing and deleting the personal data. Personal data shared under the scheme will be transferred via an email as an encrypted attachment with a password shared separately, or via another appropriately engineered solution designed with suitable guidance and support on security-by-design.

In line with the Article 29 Data Protection Working Party Guidelines on DPIAs, the processing has been identified as likely to result in a high risk to data subjects because:

- it could prevent a data subject from entering a contract with a Participating Organisation (because it could lead to an offer of employment being refused or revoked) or from continuing a contract with a Participating Organisation (because it could lead to a data subject's employment being terminated);
- if the data was shared insecurely, and disseminated more widely than its intended audience and purpose, it may have significant reputational consequences for the data subject(s) and impact on the data subject's personal and family life;
- it involves sensitive, confidential information (and may be considered to include higher-risk categories of data – see below) that can be considered as increasing the possible risk to the rights and freedoms of individuals; and
- it is shared between numerous Participating Organisations in a context of high media scrutiny of, and interest in, misconduct in the sector.

Nature:

The personal data shall include the following information relating to a candidate held by a Participating Organisation (the **Misconduct History**):

- whether the candidate was found to have committed Misconduct during the period of employment with the Responding Organisation;
- the nature of the Misconduct;
- the Disciplinary Measure imposed for the Misconduct; and
- the date of the Disciplinary Measure by a Participating Organisation.

For the purpose of the Scheme "Disciplinary Measure" means the sanction applied by the Participating Organisation in respect of an employee or person in a governing role found to have committed Misconduct either as a result of its investigation process or the sanction that would have applied where an investigation process concluded with a finding of Misconduct after the candidate has left the Participating Organisation.

Special Category:

This data may be considered to include 'Special Category' data and data related to potential criminal offences as designated in European Data Protection law[1] and may comprise sensitive personal data or other regulated forms of data under the laws of other jurisdictions.

Occasion of Use and Scope of DPIA:

Each Participating Organisation must request Misconduct History as a part of its recruitment process for any employee or governing position.

This DPIA covers the processing activities of ***sharing*** data in a 'Statement of Conduct' between Participating Organisations for the purposes of preventing re-employment of individuals who have been involved in specific types of misconduct within the aid sector.

This DPIA does not cover the processing activities which *produced* the Statement of Conduct, or its further use – e.g. any additional *checks* or *processes* carried out by Participating Organisations, its internal ***storage***, and ultimate ***retention or destruction*** within them, or any *additional information shared* as part of recruitment processes – although the compliance of Participating Organisations with relevant data protection laws on these matters is a requirement of the Scheme.

This DPIA considers that for the ***sharing*** of this data, the Participating Organisations are *Controllers in Common*, i.e. they process and control the use of the Personal Data within the Statement of Conduct which is on occasion shared between them but do so independently of each other. In this respect, Participating Organisations will comply with their own legal obligations around retention, storage, and destruction of the shared information.

The geographical area covered by the Scheme is dependent on the location of the Participating Organisations, however, the nature and purpose of the Scheme means that it is anticipated that Misconduct History will be shared internationally.

As above, each Participating Organisation shall be responsible for putting in place compliant measures for deleting the personal data in accordance with applicable data protection policies, legislation and regulations.

Describe the context of the processing: *what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved*

The relationship between the Participating Organisation and the data subject shall be that of:

- Employer and employee;
- Organisation and member of the organisation's governing body (for example, trustee or non-executive director); or
- Organisation and applicant for employment or office.

No children's data will be processed under the Scheme and it is not anticipated that personal data of other vulnerable groups will be processed.

The Scheme is a novel arrangement and is intended to be consistent with, and support implementation of, the Core Humanitarian Standards on Quality and Accountability (CHS). It is also designed to support international, national and local safeguarding measures and schemes.

Participating Organisations will inform data subjects about the Scheme. This will include providing clear privacy information at the outset of the recruitment process and providing similar information to existing employees and members of the governing body within a Participating Organisation. This DPIA (or each organisation's equivalent) will be made available to data subjects as part of these communications.

Participating Organisations' Privacy Statements will clearly state that the Scheme does not derogate from, or restrict, their rights under relevant data protection laws (and these rights, if not set out in existing Privacy Notices, should be detailed).

Depending on the jurisdiction, these may include rights of access to the disciplinary record that will form the basis of the Statement of Conduct, rights to rectification of inaccuracies, and, depending on the legal basis for processing, rights to object to processing.

[1] We do not believe that any data to be shared under the Scheme will comprise 'special category' or criminal offence data under European Data Protection law. In our view, a statement in relation to Sexual Misconduct under the Scheme does not represent processing of data relating to an individual's sex life or of any potential criminal conduct, as neither of those data attributes - although they may be disclosed incidentally and indirectly - represent, or are relevant to, the purpose of the processing. However, to ensure this assessment is comprehensive, we cover the possibility that data shared under the scheme may be considered by a regulator to fall within these categories.

The terms of the Scheme will be available via public website to permit easy access to, and to promote widespread understanding of, the Scheme.

We believe that the processing is of substantial public interest to respond to a recognised problem of repeat Misconduct in the aid sector and to protect the vulnerable individuals the sector serves. The processing represents a variation of existing referencing processes which are within data subject expectations and are widely accepted publicly as a legitimate means to protect organisations, their staff, and those they work for. We are not aware of any specific prior concerns around referencing processes and, indeed, data subject access rights in relation to confidential references for employment have been reduced in the UK under the GDPR which appears to reflect the significant societal and organisational benefits of candid disclosures between employers on material matters. In this respect, data subject transparency around Statements of Conduct under the Scheme exceeds regulatory requirements.

The security of data exchange is recognised as an important challenge in sharing data under the Scheme and is being addressed through agreed protocols/processes (above).

Describe the purposes of the processing: *what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?*

The Scheme has been designed to help mitigate the pressing safeguarding concerns within the humanitarian and development sector, which are currently of particular public concern, and to strengthen public trust in sector safeguarding and related procedures. Each Participating Organisation is committed to eradicating sexual exploitation and harassment in the sector.

The Scheme is intended to enable Participating Organisations to make informed recruitment decisions and to prevent individuals who have previously been found to have committed misconduct relating to sexual abuse, sexual exploitation and/or sexual harassment, from being employed in a sector where they are likely to have access to vulnerable individuals and communities and may have opportunities to exploit power imbalances vis a vis such individuals.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: *describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?*
Specialists in safeguarding, human resources, data protection and medical from Participating Organisations have been consulted to develop the Scheme and associated Explanatory Notes. Participating Organisations consider that it would be disproportionate to consult with all employees and office-holders in all Participating Organisations. However, some Participating Organisations may consult with Union and staff representatives where they consider this appropriate. The expectation is that the vast majority of data subjects who will be subject to the operation of the Scheme will benefit from the Scheme in terms of a safer working environment, and an enhanced reputation for the sector.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: *what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?*

Participating Organisations agree that personal data will be processed on legitimate interest grounds (Article 6(1)(f) of the GDPR). These legitimate interests include the legitimate interests of the organisations who disclose and receive the data, as well as the legitimate interests of the individuals and communities these organisations serve. Subject to the risk-mitigation measures outlined in this assessment, the Participating Organisations believe these interests are not overridden by the interests and rights of those whose data will be processed under the Scheme.

Participating Organisations believe that the processing set out in the Scheme will achieve the purpose set out in section 2 above and, at present, in the absence of equivalent sector regulation across the multiple jurisdictions in which they work, there is no other way to achieve the same outcomes. They also believe the processing is necessary to meet the public's concern.

Any special category data will be processed under the substantial public interest condition in Article 9(2)(g) of the GDPR as elaborated in particular, in the UK under:

(a) Section 12 part 2 schedule 1 of the Data Protection Act 2018 (DPA) ("regulatory requirements relating to unlawful acts and dishonesty" – where such regulatory requirement includes a requirement forming part of generally accepted principles of good practice relating to a type of body or an activity; and/ or

(b) Section 18, part 2, schedule 1 of the DPA ("safeguarding of children and of individuals at risk").

Any potential criminal offence data under Article 10 of the GDPR will be processed under the same conditions as above (per section 36, part 3, schedule 1 of the DPA).

Participating Organisations will:

- prevent function creep by complying with the limitations set out in the Scheme in relation to the Misconduct History;
- ensure data quality by requiring Participating Organisations to have in place robust, fair and reliable disciplinary procedures and to keep accurate records;
- ensure compliance with the principle of data minimisation by using the Statement of Conduct form to share information about Misconduct History

and by requesting the Statement of Conduct at the last stage of the recruitment process before making an offer of employment;
- ensure that data subjects are given information about the Scheme (where applicable, such information will include all privacy information required under Article 13 and 14 of the GDPR).

When personal data is transferred outside the EU, Participating Organisations will transfer under either (a) the derogation provided under the second limb of Article 49(1)(b)of the GDPR, being a transfer necessary for the implementation of pre-contractual measures at the data subject's request. In this respect, a data subject, requesting consideration of their application where the recruiting organisation participates in the Scheme and the data subject has been made aware of this) will be considered to found the relevant request or (b) the derogation provided under Article 49(1)(d) of the GDPR being a transfer necessary for important reason of public interest.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high
Risk 1 - Data subjects are prevented from working in the sector because of a prior finding of misconduct that is based on poor quality investigative processes, inaccurate information, or involves conduct that does not present a true safeguarding risk, such that an inability to work in the sector is disproportionate.	possible	significant	medium
Risk 2 – Statements of Conduct containing sensitive, confidential information are disclosed to unauthorised third parties.	possible	significant	medium
Risk 3 – Insufficient transparency for affected data subjects – i.e. data subjects do not understand how their data is used; with whom it will be shared; how decisions will be made based on the data; what rights they have in relation to the processing; and, in a complex controller arrangement) who is the duty bearer for these rights. The scheme could cause distress, or inappropriately deter applications for roles in the sector, if not adequately explained.	possible	significant	medium

Risk 4 - Too much data is shared by a responding Participating Organisation relative to the purposes of the Scheme.	probable	significant	medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk Eliminated reduced accepted	Residual risk Low medium high	Measure approved Yes/no
Risk 1 Data subjects are prevented from working in the sector because of a prior finding of misconduct that is based on poor quality or incomplete investigative processes, inaccurate information, or relates to conduct that does not present a true safeguarding risk, such that an inability to work in the sector is disproportionate.	The Scheme requires participants to identify their internal definitions of Misconduct for the purpose of the Disclosure Statement which will enable requesting organisations to critically assess the information provided. Disclosing Organisations are expected to apply a materiality threshold to disclosing any finding of sexual harassment to a Requesting Organisation. If such conduct is considered to be of a nature that does not indicate a real safeguarding risk, they retain discretion not to	Risk reduced	Medium/low	Yes. The risk to Data Subjects is similar to that which affects those who are subject to other fit and proper criteria and processes (such as those who work in the financial services sector in the UK) or other regulated criteria to work in particular sectors for the benefit of those the sectors' serve or the public more generally. The measure responds to a recognised

	disclose it, and to document this decision. Data Subjects are afforded a possibility to comment on the Statement of Conduct prepared by a Responding Organisation and to make representations to the Requesting Organisation on the Statement provided to them. Decisions made about - and on the basis of - Statements of Conduct are not automated and Participating Organisations are required to consider the representations of data subjects on the Disclosure Statement. (this is in addition to data subject's ordinary rights under relevant data protection rights, such as to access their misconduct record and require amendments to any inaccuracies in their data). Participating Organisations are required, under the Scheme, to have in place robust, fair and reliable disciplinary			need in the sector and represents a proportionate response to the harm that may arise in the absence of the Scheme.

	procedures and to use technical measures to keep complete, accurate and reliable HR records, and processes for updating and reviewing records, in particular when facts linked to elements of the case have changed or been reassessed. The Scheme is subject to ongoing review and assessment, including in relation to impacts on data privacy aspects. The Scheme and its DPIA will be reviewed by data protection specialists at the first-year anniversary of the rolling out of the Scheme.			
Risk 2 Statements of Conduct containing sensitive, confidential information are disclosed to unauthorised third parties.	Statements of Conduct are only created and shared by Authorised Personnel within a Participating Organisation. Misconduct Histories must only be shared with, and accessed by, Authorised Personnel within a Participating Organisation. An up-to-date list of Participant	Risk accepted	Low.	Yes. Residual risk proportionate to aims of the project.

	Organisations and Authorised Personnel within such organisations will be maintained. Personal data will be shared under the Scheme using agreed secure methods (see above). If third party processors are used for data sharing these will be subject to GDPR- compliant contractual obligations.			
Risk 3 Insufficient transparency for affected data subjects – i.e. data subjects do not understand how their data is used; with whom it will be shared; how decisions will be made based on the data; what rights they have in relation to the processing; and, in a complex controller arrangement) who is the duty bearer for these rights. The scheme could cause distress, or inappropriately deter applications for roles in the sector, if not	Clear information to be provided to affected or potentially affected data subjects through updates to privacy notices for (a) employees and (b) those in governance positions. Access to the terms of the scheme and copy of this DPIA to be made available. Clear Privacy Notices to be provided to all recruits (*with access to an explanation of the scheme and its terms of the scheme available through a public website*?) Internal communications to be made to socialise existence	Risk reduced	Low Scheme processing not conceptually very different to processing associated with existing referencing and vetting practices of employers and organisations appointing those to governance positions.	Residual risk accepted as proportionate to aims of the project.

adequately explained.	of scheme to affected data subjects and provide contact point for questions and concerns.			
Risk 4 Too much data is shared by a responding Participating Organisation.	The Statement of Conduct form will include only official conclusions of reports and disciplinary processes (unless there are exceptional circumstances duly documented and adopting a rights and principle based reasoning). The Scheme adopts a standardised Statement of Conduct form to facilitate data minimisation.	Risk reduced	Low.	Residual risk is proportionate to the project's aims.

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA