IRARA's Data Protection Policy:

IRARA takes data protection extremely seriously and we understand that we are handling sensitive data that must be protected and treated in accordance with GDPR. IRARA has clear Data Protection Guidelines in place for all regions of our operations which guarantee the safe handling and protection of the personal data of all returning individuals. We are committed to processing data in accordance with our responsibilities under the GDPR, namely that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date;
e. 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;
f. processed in a manner that ensures appropriate security of the personal data,

IRARA's in-house cloud-based returnee database is called the Integrated Returnee Toolkit (IRT) and this along with the RIAT (Reintegration Assistance Tool) system, are the only repository of returnee data. These systems are well documented, and staff are trained on their operation and the data held within them using various training materials, face to face and online training sessions.

All staff have undertaken Data Protection training, delivered online and refreshed annually as part of each staff member's annual Personal Development Plan (PDP), specific attention is given to:

- Duty of confidentiality
- Safeguarding personal data about returnees
- The need to only retain relevant information that is directly related to the process of return to a person's 3rd country
- The reason that IRARA stores data regarding returnees
- Ensuring that personal data is not printed or photographed

As well as this IRARA staff have been made aware of the following regarding the rights of individuals to access their data:

- The right to be informed – being told what data we hold about them and what we do with it.
- The right of access – individuals can request a copy of their data.
- The right to rectification – being able to have inaccurate data corrected.
- The right to erasure – being able to ask to delete / destroy their data.
- The right to restrict processing – being able to limit the amount or type of data used.
- The right to data portability – requesting to move their data electronically to another business.
- The right to object – being able to request us to stop using their data.