Data Protection
UNHCR’s Data Protection Policy

• In line with international data protection standards.
• There should be a legitimate basis and a specific purpose.
• Maintaining a high level of data security.
• Conducting Data Protection Impact Assessments.
• POCs must be informed about how their data will be used.
• UNHCR’s implementing partners should adhere the principles of the Policy.
• Data Sharing Agreement should be in place prior to transferring or sharing any personal data.
Data Sharing

- Purpose
- Necessity
- Consent
- Data sharing agreement
- Data protection impact assessment
- Data security
- Operational environment
- Data retention and deletion
Data Sharing

Encryption:
Each Iris Consumer has their own public key supplied by UNHCR, thus ensuring added security when multiple Iris Consumers are defined. The private and public key is based on RSA 2048 bits with an exponent of 65537 and is hashed with SHA-512 and encrypted using AES 256.

<table>
<thead>
<tr>
<th>Without EyeCloud</th>
<th>With EyeCloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive KYC data (full name, DoB, address and nationality)</td>
<td>proGres ID only</td>
</tr>
<tr>
<td>Complex data sharing agreement</td>
<td>Basice data sharing agreement or none at all (depending on whether values are shared back)</td>
</tr>
<tr>
<td>Parallel enrollment systems (by the bank, by WFP, by other partners) to manage their biometric ecosystem</td>
<td>No secondary / parallel enrollment by partners – authentication centralized through EyeCloud</td>
</tr>
</tbody>
</table>