DataXR Data Sharing - Code of Conduct

1. **Transparency:** Data sharing should be open and transparent. There should be clear communication regarding the data shared, its intended use, the involved parties, how it will be used and by whom. Data ownership should be acknowledged, and the roles and responsibilities of data owners, custodians, and users should be clearly defined.
2. **Single Source of Truth**: Every data element is mastered (or edited) in only one place. Each data element should have a clear and unique source and version. Copies can be made, but should be treated as read-only.
3. **Standardization & Metadata Description:** Data is shared, stored and analyzed according (international) standards. Comprehensive metadata descriptions, specifying data sources, formats, and update frequency, are provided.
4. **Data Privacy:** Maintain high data security and integrity standards, prioritizing the protection of both personal and confidential business information to preserve its commercial value, while strictly adhering to data protection guidelines.
5. **Data Security:** Each partner implements robust proportionate security measures to safeguard data during transmission and storage, including encryption, access controls, and authentication.
6. **Compliance:** Each partner adheres to relevant laws and regulations, including, but not limited to, governing data protection, data-privacy, data-security and AI and stays updated on changes in legislation.
7. **Data Integrity:** To uphold the integrity of shared data within the CropXR ecosystem. Ensure that shared data is accurate, up-to-date, and reliable. Maintain records of data sources and modifications and data is kept organized, clean and structured.
8. **Accountability and stewardship:** Establish clear lines of accountability for data sharing and stewardship within the organization for all data sharing, while creating strong reporting mechanisms for data issues and protecting whistleblowers from retaliation and enforce a framework with appropriate consequences for policy violations based on breach severity and impact.
9. **Data Retention:** Define data retention policies, specifying how long data can be stored and when it should be securely disposed of.
10. **Training and Awareness:** Provide data sharing training and raise awareness among employees and stakeholders regarding data sharing responsibilities and best practices.