First Year Plan

30 Days:

- Assemble privacy team
- Data inventory (What are we collecting now?)
- Business need evaluation (Do we need everything we are collecting?)
- Existing privacy policy review
- Data usage policy review
- Legal evaluation (Are we compliant?)

60 Days:

- Data flow mapping (collection, storage, transmission, usage), Tinkerbell
- Vulnerability assessment, Tinkerbell
- Risk assessment, Tinkerbell
- Classify collected data, Tinkerbell
- Retention policy review, Tinkerbell
- Restrict retention of video data
- Review social media policy
- Cybersecurity evaluation (website, mobile, drones)
- Governance review

6 Months:

- Data flow mapping (collection, storage, transmission, usage), Arachnid
- Vulnerability assessment, Arachnid
- Risk assessment, Arachnid
- Classify collected data, Arachnid
- Retention policy review, Arachnid
- Update global privacy policy
- Update privacy notices for both companies
- Design and implement privacy controls and monitoring
- Redesign and implement employee privacy training
- Cybersecurity evaluation (Arachnid)
- Create incident response team
- Develop and implement incident response plan

1 Year:

- Incident response preparedness evaluation
- Update IT structure to support governance and control changes
- Create and implement plan to achieve FedRAMP compliance for Arachnid
- Privacy audit
- Evaluate effectiveness