Data Protection Impact Assessment (DPIA) – Shopping List App

Project Name: Shopping List App

Date: 01 October 2025

Project Owner: Sinenhlanhla Magubane

Purpose: This DPIA assesses the collection, storage, and processing of personal data in the Shopping List App built using ReactTS, Redux, and JSON Server.

1. Purpose of Data Processing

The Shopping List App collects personal data to enable user registration, authentication, profile management, and interaction with shopping lists. Data is collected only to provide the app’s core functionality and improve user experience.

2. Lawful Basis for Processing

- User consent: Users voluntarily provide data when registering or submitting profile updates.
- Contractual necessity: User data is required to create an account and manage shopping lists.

3. Types of Personal Data Collected

- First Name
- Last Name
- Email Address
- Account Password (encrypted)
- Shopping list details (name, quantity, notes, category, images)

4. Data Protection Principles

- Lawfulness, fairness, and transparency: Data is collected only for the app’s functional purposes. Users are informed via this DPIA and app documentation.
- Purpose limitation: Data is used solely to manage user accounts and shopping lists.
- Data minimization: Only essential personal data is collected.
- Accuracy: Users can update their profile data to maintain accuracy.
- Storage limitation: Personal data is retained for a maximum of 2 years unless the user consents to extended retention.
- Integrity and confidentiality: User credentials are encrypted. Access to data is restricted to authenticated users.
- Accountability: Development follows GDPR-compliant practices, with regular review and testing.

5. Users’ Rights

Users have the following rights:

- Access their personal data
- Rectify or update their data
- Erase their data by unsubscribing or requesting deletion
- Restrict or object to processing (if applicable)

6. Data Retention

- Personal data will be retained for up to 2 years.
- Users may request extended retention via the home Portfolio webpage.
- Data is removed permanently from the JSON server upon account deletion.

7. Data Storage & Security Measures

- JSON Server stores all app data.
- Redux manages state securely on the client side.
- Password encryption: Credentials are encrypted on sign-up and decrypted on login.
- Protected routes: Only authorized users can access restricted pages (e.g., Home, Profile).
- Regular backups: JSON server data is backed up to prevent loss.

8. Risk Assessment

Risk	*Likelihood*	*Impact*	*Mitigation*
Unauthorized access to user accounts	Medium	High	Encrypted passwords, protected routes, authentication
Accidental data deletion	Low	Medium	Regular backups
Exposure of personal data via shared lists	Low	Medium	User-controlled sharing settings
URL manipulation (sorting/filtering) leaking data	Low	Low	Validation of URL parameters and sanitized outputs

9. Data Sharing

- No personal data is shared with third parties outside the app.
- Users can share shopping lists, but only the list content is shared, not personal account data.

10. DPIA Conclusion

The Shopping List App collects minimal personal data necessary for its functionality. With encryption, protected routes, user rights management, and data retention policies, risks are minimized. The app is compliant with GDPR principles and ensures user data is processed lawfully, transparently, and securely.