

LINDDUN Privacy Threat Analysis Table

(Based on Level 1 DFD: Registration, Login, Recovery, Security Management)

Using LINDDUN, I identified privacy risks across registration, login, recovery, and session management. A key finding is that unawareness and detectability risks are amplified for users with MS due to cognitive fatigue, which informed my focus on clear privacy feedback, minimal data collection, and accessible recovery pathways.

P1 - Registration

LINDDUN Category	Privacy Threat	MS-Specific Impact	Mitigation Strategy
L - Linkability	Registration data can be linked across services (e.g. same email reused)	Users with MS may reuse identifiers to reduce cognitive load.	Support passkeys, minimise identifiers, avoid cross-service tracking.
I - Identifiability	Registration uniquely identifies user across systems	Increased risk if user relies on third-party assistance	Collect minimal personal data; pseudonymous identifiers where possible
N - Non-repudiation	Logs permanently tie user to actions they may not recall	Memory impairment may lead to disputes or distress	Allow user-visible activity history with clear timestamps and explanations
D - Detectability	Account existence detectable during registration	Enables targeted phishing campaigns	Uniform responses regardless of account existence
U - Unawareness	User unaware how data will be used or stored	Cognitive fog may reduce comprehension of privacy notices	Short, plain-language explanations; layered privacy notices
N - Non-compliance	Registration flow fails WCAG privacy requirements	Disproportionately affects MS users with cognitive impairments	Align with WCAG 2.2 accessible authentication criteria

P2 - Login / Authentication

LINDDUN Category	Privacy Threat	MS-Specific Impact	Mitigation Strategy
L - Linkability	Login metadata links sessions over time.	Predictable patterns increase profiling risk	Limit session correlation; rotate identifiers
I - Identifiability	Authentication data reveals user identity	Increases risk if devices are shared or assisted	Device-bound credentials; minimal visible identifiers
N - Non-repudiation	Login logs used to assert actions user may not recall	Cognitive fog may impair recall of sessions	Provide accessible session summaries and logout history
D - Detectability	Error messages reveal valid usernames	Supports phishing and account enumeration	Generic login errors; no confirmation of account existence
U - Unawareness	User unaware of tracking or session persistence	Fatigue may limit understanding of session scope	Clear session indicators; explicit logout confirmation
N - Non-compliance	Authentication requires memory or transcription	Violates WCAG 2.2 for cognitive disabilities	Avoid memory-based challenges; support passkeys

P3 - Account Recovery

LINDDUN Category	Privacy Threat	MS-Specific Impact	Mitigation Strategy
L - Linkability	Recovery requests link user across channels (email/SMS)	Increases exposure during recovery stress	Limit metadata sharing; avoid persistent recovery identifiers
I - Identifiability	Recovery process confirms identity externally	Heightened vulnerability during cognitive fatigue	Use generic recovery messaging; avoid explicit identity confirmation
N - Non-repudiation	Recovery actions permanently logged	User may not remember initiating recovery	Provide clear recovery summaries and confirmation steps
D - Detectability	Recovery flow reveals account existence	Enables targeted attacks	Uniform recovery responses regardless of account status
U - Unawareness	User unaware of how recovery data is stored or reused	Complex flows increase confusion	Step-by-step guidance; plain language explanations
N - Non-compliance	Recovery relies on timed codes or memory	Disproportionately excludes users with MS	Offer multiple accessible recovery pathways

P4 - Security & Session Management

LINDDUN Category	Privacy Threat	MS-Specific Impact	Mitigation Strategy
L - Linkability	Audit logs correlate activity over long periods	Long-term profiling risk	Retention limits; aggregate where possible
I - Identifiability	Security alerts reveal sensitive activity details	May require external help to interpret alerts	Minimal, privacy-preserving alerts
N - Non-repudiation	Logs used to assert responsibility for actions	Memory impairment may cause distress	User-accessible explanations; dispute mechanisms
D - Detectability	Lockouts or alerts reveal user presence	Enables social engineering	Generic notifications without confirmation of identity
U - Unawareness	User unaware of ongoing monitoring	Cognitive load reduces awareness	Clear explanations of security monitoring
N - Non-compliance	Privacy controls inaccessible	Violates inclusive design principles	Ensure WCAG-compliant privacy interactions