Data Handling and Safety – SentinelX / SentinelStack AB

# 1. Datainsamling

SentinelX samlar endast in data lokalt på användarens enhet. Ingen molnbaserad loggning eller överföring sker utan uttryckligt samtycke. Insamlad data inkluderar:  
- Händelselogg (t.ex. misstänkt aktivitet, skärmdump)  
- Telegramkommandon (loggade lokalt)  
- Appinteraktioner (GuardianAgent – lokalt)

# 2. Lagring och åtkomst

- Loggar lagras i krypterad lokal datamapp  
- Endast användaren (eller auktoriserad admin) har tillgång  
- Telegramdata är end-to-end krypterat och loggas inte i moln  
- Alla PDF-rapporter genereras lokalt utan molnuppladdning

# 3. Dataskydd och säkerhet

- Kryptering vid vila (lokala loggar och PDF:er)  
- Automatisk loggrensning efter X dagar (användarstyrt)  
- Möjlighet till manuell rensning via CLI-kommandon  
- Kodsignatur för att verifiera att mjukvaran är äkta

# 4. Dataexport och rapportering

- Export sker endast via användarens initiativ  
- PDF-rapporter innehåller händelser, metadata och signatur  
- Möjlighet att skicka PDF automatiskt till angiven e-post  
- Export kan automatiseras med kryptering

# 5. Dataförstöring

- CLI-kommando /wipe eller via lokal inställning  
- Automatisk radering av äldre loggar (>30 dagar) som standard  
- GuardianAgent har inbyggt nöd-stopp och datatömning

# 6. GDPR-efterlevnad

- Ingen persondata delas med tredje part  
- Användare informeras via onboarding-manual  
- Möjlighet att exportera och granska all lokal data  
- SentinelStack är 'privacy by default', byggd utan molnberoende