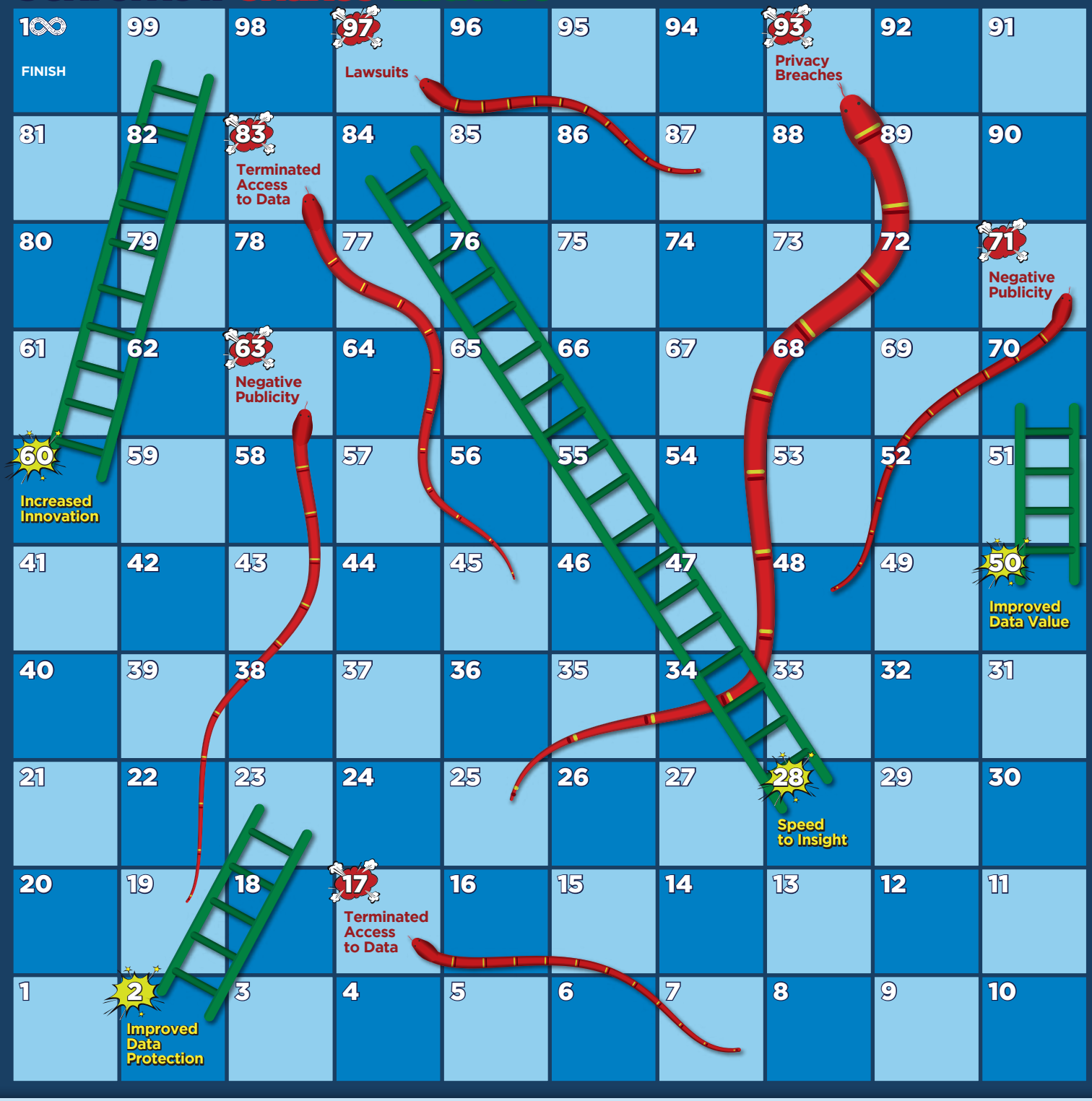
Schrems II Snakes&Ladders

ANONOS



Top 10 Immediate Requirements for Surviving and Thriving Under Schrems II

1. Updating SCCs without new technical controls is not enough. Protection for EU personal data **must travel with the data wherever it goes immediately**.
2. **Technical Supplementary Measures** are required to prevent the identification of data subjects directly or indirectly using other available data sources.
3. Encryption does **NOT** travel with the data **WHEN IN USE** because it must be decrypted to enable use.
4. Encryption is **not adequate** for data transferred to US importers subject to FISA.
5. Encryption must be **state-of-the-art and effective** against cryptanalysis capabilities of public authorities in the recipient country.
6. The EDPB recommends **GDPR-compliant Pseudonymisation** to protect data WHEN IN USE.
7. GDPR-compliant Pseudonymisation **enables greater lawful data use**.
8. Localisation of processing does not solve the issue. Schrems II controls are **required even if data is processed in the EEA or adequacy decision countries** to satisfy GDPR Article 25 Data Protection by Design and by Default and Article 32 Security requirements.
9. All parties in a data supply chain are **jointly and severally liable to data subjects**.
10. **Upstream data providers will discontinue data flow** rather than risking damage to their own business.

Contact us at **LearnMore@Anonos.com** to learn how to protect your data WHEN IN USE.