



Core principles of security in Open Data

Privacy by design

Do	Don't
• Build anonymisation, minimisation and aggregation into data lifecycle from start • Use privacy-preserving techniques to protect personally identifiable information	• Apply aggregation or de-identification only at the final stages before opening data • Assume removing IDs is sufficient to protect privacy

Context-aware disclosure

Do	Don't
• Assess the dataset in context and potential combinations with other datasets. • Assess the risk inference or re-identification before release	• Forget to consider external linkability of your data • Forget a real-world context analysis

Continuous risk assessment

Do	Don't
• Regularly audit datasets and security threats • Periodically update risk policies as technology and user behaviour evolves	• Assume a one-time risk assessment is sufficient • Ignore emerging vulnerabilities or rely on existing methods

Clear governance and accountability

Do	Don't
• Define roles for data stewardship, approval, and security oversight • Document decisions around data publishing	• Operate without transparency about roles and responsibilities, especially regarding approval and management of data releases

Community feedback and transparency in security practices

Do	Don't
• Enable channels for reporting misuse or identified risks • Publish methodologies used for data protection and anonymisation methods	• Obscure your data handling processes

