

Law 25 checklist

Groupe Conseil GRD. Source: Commission d'accès à l'information (CAI), <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/principaux-changements-loi-25> (S1), CAI incidents (S2) <https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privées/incidents-confidentialite-mesures-securite-entreprises> (CAI pages are in French.)

- ☐ Person in charge designated (by default, the person with the highest authority; may be delegated in writing); title and contact information published on the website [S1]
- ☐ Governance policies (retention, destruction, roles, complaints) adopted and published [S1]
- ☐ Privacy policy in clear and simple terms (collection by technological means) [S1]
- ☐ Privacy settings set to the highest level by default [S1]
- ☐ Privacy impact assessment (PIA) for any information system project and before any communication outside Québec [S1]
- ☐ Transparency information provided at the time of collection [S1]
- ☐ Incident register, kept for at least 5 years [S2]
- ☐ Ability to respond to data portability requests (since September 22, 2024) [S1] Technical side: see the "NIST CSF 2.0 summary" guide and the article "14 Microsoft 365 and Azure security settings to check".