# How Ready Are We to Share? A CARICOM–GDPR Legislative Heatmap on Data Sharing Features

Version 1.0 (28-June-2025)

| LEGISLATION FEATURE | INTERNATIONAL STANDARD (GDPR) | Antigua and Barbuda | The Bahamas | Barbados | Belize | Dominica | Grenada | Guyana | Jamaica | Haiti | Montserrat | St Kitts and Nevis | St Lucia | St Vincent and the Grenadines | Suriname † | Trinidad and Tobago | Summary Score | Rank |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Is there a clear legal reason to share data? | | Lawful bases like consent, legal duty, public interest clearly stated (Section 5). | Allows sharing based on legal duty, public interest, and consent. | Sharing allowed for legal obligations, public interest, contracts, or consent | Act lists legal bases incl. consent, contracts, vital/public interest (s.7). | No clear lawful bases (e.g. consent, public interest) for data sharing found in Constitution. | Multiple lawful bases (contract, legal obligation, public duty) are defined for processing, covering sharing implicitly. | Lists lawful bases (consent, public task, etc) but not all GDPR bases. | Act defines lawful bases incl. consent, legal duty & public interest, similar to GDPR. | No legal basis or framework identified that justifies data sharing. | No law clarifies lawful processing purposes. | Act outlines consent, legal duty, justice, and public interest as lawful bases. | Law outlines clear legal grounds: consent, legal obligation, public interest (s.34). | Some lawful bases are mentioned, like legal requirements and public interest, but not comprehensively. | Article 6 provides clear legal bases like consent, legal duty, public interest. | Law lists several valid reasons incl. consent, public interest, legal obligation (Sec 6 & 42). | 52 | 3rd (joint) |
| Does the law say who is responsible when data is shared? | | Terms like "data user" and "data processor" used, but role clarity is weaker than GDPR. | Defines roles of data controller and processor clearly. | Law clearly states who is responsible when sharing and sets out contractual terms | Roles of controllers / processors clearly defined (s.2, s.4–5, s.54-56). | Roles like data controller or processor are not defined. | Data users and processors are clearly defined; responsibilities are assigned and enforced. | Roles of controllers/processors defined, but joint responsibility not clear. | Roles of controller, processor, & DPO are defined, like GDPR Articles 4, 24-30. | No roles or responsibilities for data sharing defined by law. | No statutory rights to access, correction, or erasure. | Roles of data user and processor defined; users must ensure legal processing. | Roles of data controllers defined, but processors not clearly distinguished (s.2, s.46). | Act does not define roles like controllers or processors clearly. | Clear roles for controller and processor are defined (Art. 1, 14-16). | Roles of public/private bodies outlined, but joint responsibilities not clearly defined (Sec 6, 56). | 50 | 4th (joint) |
| Are the rules for getting consent clear and practical? | | Consent must be informed and explicit, esp. for sensitive data (Sections 5 & 18). | Consent must be written, but lacks full GDPR clarity on consent conditions. | Consent must be clear and can be withdrawn anytime | Consent must be freely given, informed, unambiguous, and withdrawable (s.8). | No guidance on consent for data use or sharing. | Consent must be informed and written for sensitive data; clear when consent is required and when not. | Defines consent as informed and voluntary; less detailed than GDPR. | Consent must be informed, specific, freely given & can be withdrawn. | No legal rules or guidance on valid consent found. | No rules defining obligations for data roles. | Freely given consent required; clear on when it's needed and exceptions. | Consent is defined and alternatives allowed, but lacks practical detail (s.34). | Consent is required for disclosure, but conditions for valid consent are not detailed. | Consent must be informed, specific, and freely given (Art. 6(2), 6(3), 7). | Consent required and mentioned, but conditions for valid consent less clear than GDPR (Sec 6, 31, 40). | 50 | 4th (joint) |
| Are people's rights protected when data is shared? | | Strong access, correction, and rectification rights (Sections 12–16). | Allows access, correction, erasure, and marketing objection. | Strong rights including access, correction, deletion, and portability | Strong rights incl. access, correction, erasure, portability (s.11-22). | Some rights like privacy and protection from inhuman treatment are in the Constitution. | Data subjects have rights to access, correct, and request deletion of data; refusal reasons must be provided. | Rights listed (access, correct, erase, object), generally consistent with GDPR. | Access, rectification, deletion, objection & data portability all included. | No laws in place to protect individual rights in data sharing. | No formal principles like purpose limitation or minimisation. | Access, correction, and complaint rights protected; includes timeframes. | Access, rectification, deletion rights exist, aligned with GDPR (s.52–56). | People can request corrections and the Act protects against misuse or unauthorized access. | Broad rights to access, correction, erasure, objection are listed (Art. 11). | Right to access, correct, request erasure is covered; some limits exist (Sec 6, 52-57). | 57 | 2nd |
| Can data be shared safely if personal details are removed? | | No mention of anonymisation or pseudonymisation as legal grounds for safe sharing. | Mentions statistical/research data but lacks anonymization detail. | Pseudonymisation is defined but not emphasized as a routine practice or safeguard | Act supports de-identification but lacks specific detail on anonymization (s.36). | No mention of anonymization or pseudonymization. | No explicit reference to anonymisation; some indirect support via 'data minimisation' and masking principles. | Mentions anonymization and pseudonymization but lacks technical detail. | De-identification supported, but lacks explicit GDPR-style anonymisation rules. | No mention of anonymisation or pseudonymisation in current legal framework. | No regime for international data transfer. | No mention of anonymization or pseudonymization in sharing context. | Anonymization is implied but not clearly supported in law (s.33, s.42). | Act does not mention anonymization or pseudonymization. | Law allows pseudonymization and requires safeguards (Art. 1(i), 5(f), 17). | Anonymization/pseudonymization not strongly supported or defined (few refs only). | 35 | 9th |
| Can data be shared with people or organizations in other countries? | | No provisions on cross-border data sharing or adequacy mechanisms found. | Allows international transfer with equivalent protection. | Transfer rules mirror GDPR with adequacy, safeguards, and public interest options | Detailed rules for cross-border transfer incl. adequacy & safeguards (s.23-27). | Constitution mentions international agreements but no framework for data sharing. | No clear provisions for international transfers or safeguards similar to GDPR's adequacy decisions. | Says rules apply to cross-border sharing but lacks adequacy safeguards. | Transfers require 'adequate protection' & include a list of safeguards. | No legal structure or safeguards for international data transfers. | No requirements to secure data or notify breaches. | Mentions extraterritorial scope but lacks GDPR-like safeguards for cross-border transfers. | International transfer allowed with conditions, but lacks detail (s.45). | No provisions found on international data sharing. | International transfers allowed if safeguards exist, but lacks detail (Art. 22). | Some safeguards required for foreign transfers (Sec 28, 46), but lacks adequacy test detail. | 42 | 7th (joint) |
| Is there a public body that oversees data sharing and helps resolve problems? | | Role assigned to the Information Commissioner (Section 21), with oversight powers. | Independent Commissioner with enforcement and complaint powers. | Dedicated Data Protection Commissioner with legal powers and duties | Independent Commissioner with strong powers (s.68-69). | No independent supervisory authority for data protection was found. | Independent Information Commission is established with investigative and enforcement powers. | Provides for Data Protection Commissioner with oversight powers. | Independent Information Commissioner with powers to investigate & enforce. | No independent supervisory authority established. | No authority exists to enforce or oversee. | Independent Information Commissioner with clear powers and duties. | Independent Data Commissioner with clear oversight powers (s.5–12). | A dedicated Privacy Commissioner exists with investigative powers. | An independent Commissioner with strong powers is established (Art. 23-32). | Info Commissioner role well-established with powers and independence (Sec 7–10, 22–28). | 61 | 1st |
| Do data producers have to keep records and be open about sharing? | | Limited mention of transparency in disclosures, but no strong documentation duties. | Requires registration and some disclosure but not GDPR-level detail. | Transparent rules and duties to inform users, though record-keeping could be clearer | Record-keeping and breach notification required (s.58, s.61-62). | No duties to document or report data sharing activities. | Acts encourage procedural documentation and access logs, but no mandatory sharing registers or Article 30-equivalents. | Requires records and transparency, but no duty to notify data subjects. | Registration & documentation of sharing duties are included. | No obligation to record or report data sharing activities found. | No requirement for DPIAs or record-keeping. | Requires transparency but lacks detailed record-keeping duties. | Some duties to notify and record but limited public transparency (s.46-54). | No legal duty to keep sharing records or notify subjects. | Record-keeping and notification required (Art. 10, 15(5), 18). | Requires privacy impact assessments and some record keeping (Sec 47-48, 56). | 42 | 7th (joint) |
| Does the law support data sharing for research and the public good? | | Exemptions support research use, but limited proactive facilitation or safeguards (Section 19). | Mentions research/statistics but with limited facilitation. | Exemptions for research and statistics if protections are maintained | Data sharing for research/statistics allowed with conditions (s.36). | No explicit support for research-related sharing. | Sharing for statistics and research is allowed with conditions, and exemptions apply with safeguards. | Allows use for research/public interest with safeguards. | Research is a listed exemption with safeguards; public interest i s a basis. | No legal support for sharing data for research or public interest. | No enforcement regime or fines exist. | Allows data use for research with exemptions, but safeguards less clear. | Research use permitted under conditions, notably for public health (s.38). | Allows use of data for statistics or public interest but without strong research-specific rules. | Research/data reuse permitted with safeguards (Art. 5(c), 8(2)(h), 43). | Allows sharing for research/public health with safeguards (Sec 43). | 48 | 6th |
| | Summary Score | 28 | 32 | 37 | 41 | 14 | 38 | 31 | 38 | 9 | 9 | 32 | 34 | 25 | 38 | 31 | | |
| | Rank (out of 15) | 11th | 7th (joint) | 5th | 1st | 13th | 2nd (joint) | 9th (joint) | 2nd (joint) | 14th (joint) | 14th (joint) | 7th (joint) | 6th | 12th | 2nd (joint) | 9th (joint) | | |

† The Suriname Privacy and Personal Data Protection Law (2020) has been drafted, and is not yet active