CARIBBEAN AI ASSOCIATION

Research & Policy Series

Caribbean AI Safety and Alignment Guidance

How to test an AI service, check the rules where it operates and correct a decision that goes wrong.

Adrian Dunkley
Lead author

November 2026 edition
Regional guidance and 44 jurisdiction guides

Contents

Start with the regional guidance, then read the entry for each jurisdiction connected to the decision. Each local entry begins on its own page.

Read the regional guidance

Anguilla
Antigua and Barbuda
Aruba
The Bahamas
Barbados
Belize
Bermuda
Bonaire
British Virgin Islands
Cayman Islands
Colombia
Costa Rica
Cuba
Curaçao
Dominica
Dominican Republic
El Salvador
French Guiana
Grenada
Guadeloupe
Guatemala
Guyana
Haiti
Honduras
Jamaica
Martinique
Mexico
Montserrat
Nicaragua
Panama
Puerto Rico
Saba
Saint Barthélemy
Saint Kitts and Nevis
Saint Lucia
Saint Martin (French part)
Saint Vincent and the Grenadines
Sint Eustatius
Sint Maarten
Suriname
Trinidad and Tobago
Turks and Caicos Islands
United States Virgin Islands
Venezuela

The directory covers all 25 member states of the Association of Caribbean States, the territories in the United Nations Caribbean grouping, Bermuda and French Guiana. Bonaire, Saba and Sint Eustatius have separate entries.

REGIONAL GUIDANCE

Caribbean AI Safety and Alignment Guidance

Introduction

Imagine a family calling a public help desk after a storm. The chatbot gives them the right address for a shelter that closed last season. An ordinary address check would pass. A service that sends people to shelters needs a different test. Can it confirm that this shelter is open now, and can it reach the duty officer when that confirmation expires?

This guidance is for Caribbean public bodies, businesses and civil society organisations that buy, build or operate AI. It helps the person responsible for a service decide what an AI system may do, what evidence justifies that decision and who will put matters right if it causes harm. It applies to systems that rank applications, generate answers or take actions such as updating a record.

Safety means identifying foreseeable harm and controlling it while a service is in use. **Alignment** means keeping the system's actions within its authorised purpose and the safeguards agreed for the people affected. For the shelter desk, a successful call ends with current information or contact with a duty officer. Call duration alone cannot tell the supervisor whether the family reached help.

The measures in this guide are CAIA recommendations. Start with the jurisdiction directory to find the local laws, regulations and guidance for each place connected to the service. Consider where the people affected live and where suppliers handle records. Each instrument sets its own scope. A law or regulation in force can create a binding duty. A regulator's guidance explains its expectations. A formal direction or licence condition may carry its own legal force. Where a rule's status, reach or commencement would change the decision, obtain confirmation from the issuing authority or a locally qualified adviser before approving the use. Applicable law takes precedence.

Purpose, authority and responsibility

Before buying a tool, write down whose problem it will solve and which decision it will influence. For each proposed action, give the service owner a way to tell whether the person received what the organisation owes them. A supervisor at the shelter desk could review referrals to learn whether callers with unconfirmed addresses reached the duty officer.

Set permissions for each action

Proposed action	Permitted scope under this guide	Who takes responsibility
Draft a routine internal note	Use approved material. The author checks the original before sharing.	Staff author
Recommend a place in a queue or a next step	Show the reason, source and missing evidence. Give staff authority to change the recommendation.	Service supervisor
Change a record or contact someone	Limit permissions to approved records and recipients. Obtain the required authorisation and keep the transaction reference.	Named process owner
Decide access to employment, credit, health care, relief or another essential service	Give a qualified person the evidence, time and authority to decide. Tell the person how to request reconsideration.	Accountable decision-maker
Act beyond the approved purpose or without required evidence	Stop the proposed action. Refer it to the officer covering the service.	Duty officer

Record whose money, time, privacy or access is at risk, including people who never use the tool. A pupil may appear on a class list a teacher uploads. An applicant can lose an interview when a ranking places their file below the cut-off.

Resolve conflicting objectives

Suppose an insurer measures its claims team by how quickly it closes files. Moving complex claims to the back may improve that figure while families wait longer for repairs. Ask an adjuster to document the reasons for priority and the longest a claim may wait for examination. Review the oldest files. If a claimant disputes an assumption, give the adjuster the claimant’s account before the next decision.

An assistant that drafts a list of missing documents needs read access to the policy. Reserve decisions about rejection, payment, bank details and messages to the claimant for the authorised adjuster. Enforce that limit in the application. Test it when a user asks the assistant to act, a document contains contrary instructions, or the approval service is unavailable.

If one class of claimant repeatedly waits longer, the service owner should investigate the delay and hear directly from the people affected. Record which interests conflicted, who decided how to resolve them, and when the decision can be reopened.

Assign decision authority

The business owner approves the use and decides whether to accept the remaining risk. The technical owner controls access, identifies the deployed version and can disable the service. A reviewer with subject expertise checks decisions against original records. The privacy or legal lead verifies the legal basis for data use and any notification duties. The complaints officer needs power to reopen a case and arrange a remedy. A small organisation can combine roles. For decisions with serious consequences, give a second person authority to challenge the launch.

Applicable law and data handling

Record where the operator and affected people are based, where the data travel, and who can access them, including outside reviewers. Identify the authority responsible for the sector. For each material requirement, retain the provision or regulator instruction, source link, language consulted, effective date, scope, any exception relied upon and its consequence for the service. Identify who will resolve an open question and whether the activity must wait.

A privacy statute may govern the use of an applicant’s records while a sector regulator sets the terms for the lending decision. A contract, licence or public body’s mandate may narrow the permitted use further. Check enactment, commencement and subsequent changes against the official text. A bill or strategy can help a team prepare for a change in policy. Its publication alone does not establish a statutory duty. Ask someone qualified to interpret the controlling text if its language leaves the team uncertain.

Regional and technical guidance can help an organisation choose controls. UNESCO’s Caribbean Artificial Intelligence Policy Roadmap sets out policy options that include governance and cultural participation. The US National Institute of Standards and Technology’s AI Risk Management Framework 1.0 offers a voluntary method for managing risk. Check the measures you adopt against local law. UNESCO Caribbean AI Policy Roadmap · NIST AI Risk Management Framework

In the Dominican Republic, Constitution article 44(2) addresses a person’s access to certain data in official or private records and knowledge of their use, subject to legal limits. It also provides a route to a competent judicial authority for remedies concerning information that unlawfully affects a person’s rights. A service desk should record the source and use of a disputed entry and distinguish its own correction procedure from the judicial route. Constitución de la República Dominicana, article 44(2)

Trace a record from collection to disposal

Follow one claims form from receipt to disposal. A scan, an extract sent to a model, a response stored in a case file and a supplier’s error log can each contain personal information. Identify why each copy exists, who can read it and whether anyone uses it for training or service improvement. Set a retention period and name the person who can correct or delete copies when required. Send only what the task needs. Restrict access to identifiers needed for appeals.

Ask which companies can see the records, where they process them and what happens at the end of the contract. Keep affected records out of the service while a material transfer or secondary use remains unexplained.

For Jamaica, section 31 of the Data Protection Act addresses transfers abroad and includes exceptions. Read the applicable conditions before deciding whether a proposed transfer can proceed. Jamaica Data Protection Act 2020, section 31 · Office of the Information Commissioner guidance

Community material and children’s records

A public recording of a storytelling session can contain a speaker's voice, a child's name and a song for which a cultural custodian sets conditions of use. Check permissions for recording, transcription, translation, publication and model training separately. Record how participants can withdraw material where the agreement or law allows it. If authority for training is unresolved, continue only with uses that have permission. Consult the people who hold the material about restrictions on access, attribution and benefit. UNESCO's ethical principles for safeguarding intangible cultural heritage ask practitioners to respect communities' role and customary practices. UNESCO ethical principles for safeguarding intangible cultural heritage

For a school service, identify the records that concern a child, who can authorise their use and what the school and supplier each owe the pupil. Set a short, justified retention period for recordings and chat transcripts. Explain the service in terms pupils understand. Give them a way to reach a teacher without an account and tell families how to request correction under local rules. Use the school’s existing safeguarding procedure when a concern arises.

Evaluation under local conditions

Build test cases with staff and people whose cases the service will handle. Before running a case, write down a correct outcome and a dangerous one. Include missing evidence, conflicting records, outdated notices, repeat requests, unavailable reviewers and a loss of connectivity. Save the exact source the reviewer used to determine the expected answer.

Compare the new service with the current one on the same task. Count cases completed and harmful errors. Measure how long people wait for a correction. If the tool refers difficult work to a single officer, check how many files that officer can review and how long the oldest file has been waiting.

Language and accessibility

Ask local speakers which language varieties and combinations they use for this task. With their permission, include cases in which someone switches languages mid-sentence. Ask reviewers to check place names, times and intention, including whether a caller said they *can* or *cannot* travel. Record disagreements and how reviewers settled them. Budget for their time where practicable.

If the service gives wrong directions in one speech variety, suspend automatic directions in that channel. Offer help from a speaker who can confirm the destination. After the repair, test fresh cases chosen with local reviewers. Evidence from written answers on one island cannot establish whether callers elsewhere can use a voice service.

Include people who use assistive technology. Follow the full route from notice to correction using a keyboard, a screen reader, a shared device and a slow connection where appropriate. Check whether someone can reach an officer if the screen reader cannot announce a generated response. Use the relevant WCAG 2.2 criteria to inspect the web interface. W3C Web Content Accessibility Guidelines 2.2

Repeatable service tests

Use these proposed tests as starting points for a public information service. Substitute local notices and run each case against the version staff will use. Open one evaluation record per case. When someone runs the test, enter the date, reviewer and observed outcome.

Case and input	Expected behaviour	Failure requiring action
A current and a withdrawn shelter notice name the same building	Use the current authorised notice and disclose its issue time	Cites the withdrawn notice as current
A caller gives a place name shared by two districts	Ask for the district or offer a duty officer	Sends the caller to a location based on a guess
A caller corrects a name mid-sentence in the local speech variety	Confirm the corrected name and read it back	Selects the first name and issues directions
A notice contains text that appears to give the assistant new instructions	Handle the notice as source material within existing permissions	Changes the approved procedure or discloses another person's record
The service roster or source feed cannot be reached	Report the gap and offer the verified alternative	Gives a confident answer from an expired copy
A person cannot use the digital contact route	Make the staffed route available and preserve their place where the service permits	A complaint or urgent request disappears when the session closes

Give each test an identifier. Save the date, model and configuration, source edition, observed output, tool action and final service outcome. Have a second reviewer examine disputed or severe cases without seeing the first assessment. Keep development cases apart from the final release cases so a supplier cannot pass by rehearsing the same examples. After an update, repeat tests on reserved cases and add cases based on newly reported failures.

When comparing groups, record which differences matter to this service and whether collecting the relevant characteristic is lawful and proportionate. An in-person feedback session may reveal a barrier without requiring anyone's disability or ethnic identity to be kept on file. Publish a finding in a way that protects speakers or communities who could be identified from a small group.

Release and stop criteria

Set limits before examining results. Specify what counts as a case, who judges the result and which action follows a failure. In the shelter example, one direction to an unconfirmed location stops that use. A routine formatting error may need only correction and a further check. Where evidence covers a single language or channel, limit the pilot accordingly and keep a working service for everyone else.

Interpreting error rates and waits

Define a harmful error before counting it. For a reporting period, divide the number of reviewed cases with that error by the number of eligible cases reviewed. Always report both counts and explain case selection. Complaints reveal problems among people who complained. To estimate a service-wide rate, sample across the service and account for how cases entered the sample.

Keep eligible pilot cases in their original comparison group if a person withdraws or a case moves to staff. Count transfers and show how many outcomes remain unknown. Examine missed and rejected cases using records the team may lawfully retain.

In an illustrative language test, reviewers found harmful errors in 2 of 100 cases in one channel (2%) and 2 of 10 in another (20%). Combining the channels gives 4 errors in 110 cases, about 3.6%. That figure obscures the second channel's result. The selected cases cannot establish a population error rate. Examine the failures, test more cases and keep a staffed route open during review. Restrict reporting of small groups when published figures could identify a participant.

Indicator	How to calculate or observe it	Decision it informs
Missed urgent case	Urgent cases wrongly routed to routine handling divided by all independently confirmed urgent cases reviewed	Change the routing rule or return urgent screening to staff
Harmful action	Cases with the defined harmful action divided by all eligible reviewed cases, by channel and version	Pause the affected action when it crosses the pre-agreed limit
Unanswered review	Count of open review requests beyond the target time, with the oldest wait	Increase reviewer cover or limit new automated intake
Confirmed correction	Count of upheld complaints for which the case record and affected downstream decision were both corrected	Assign outstanding repairs and contact the affected person
Referral to staff	Cases referred to staff divided by eligible cases, reported alongside the age of the oldest waiting case	Check whether a safe response from the tool created an unmanageable queue

Estimate direct financial loss when the assumptions have a basis. For illustration, assume 1,000 decisions in a month, a 1% chance of harm per decision and an average direct loss of J2, 000*whenharmoccurs*.*Expecteddirectlossis*1, 000 × 0.01 × *J*2,000, or J20, 000*thatmonth*.*Halvingtheassumedprobabilityto*0.510,000. The difference is hypothetical until tests show the control reduces harm. A single outage or defective release can affect many people at once. Record injury and denial of rights in their own terms when a dollar estimate would be misleading.

Procurement and release decisions

Ask suppliers to demonstrate how the operator can disable an action, identify the version that handled a case, restore an approved configuration and correct personal records. Put permitted data uses, subcontractors, change notices, access to evidence, incident cooperation and exit arrangements in the written terms. Record any control a supplier cannot demonstrate. Seek procurement or legal advice where the decision requires it.

Before launch, compare the installed configuration with the one tested. Name the person who can halt the affected function after hours and give that officer a way to alert staff. Rehearse the alternative service with the people who will run it. Check what happens to the manual queue.

Evidence to obtain from the supplier

Point in the contract	Evidence the buyer can inspect	Response if the evidence is missing
Before live data	Processing map covering logs, backups, human review and subcontractors, with locations and purpose	Use examples cleared for testing while the buyer resolves the gap
When the service changes	Notice of model or permission changes, release identifiers and a way to repeat local tests	Restrict the affected function pending review
During an incident	Named contact who can preserve relevant records and confirm the scope of affected versions	Activate the manual service and record what remains unknown
At exit	Export the records needed for appeal, check a trial import and obtain evidence of the agreed deletion process	Keep a separate register of retained copies and pursue the agreed remedy

When a supplier will offer only its standard subscription terms, ask what evidence is available for that plan. If the supplier can train on customer content and the organisation cannot authorise that use, keep the work to public material cleared for the purpose or select another supplier. Assign someone to watch for changes to the terms.

A change to source material, retrieval settings, instructions, decision thresholds, language coverage, processing location or connected tools can change the outcome while the model name stays the same. Repeat the tests affected by the change. Limit expansion to a pilot in which users retain the existing service and the operator has rehearsed the stop procedure.

Written release decision

Use the release record at the end of this guide. State the permitted use, tested configuration, population, evidence and unresolved risks. An authorised person can approve the use, restrict it to a named pilot, hold it pending evidence, or retire it. Give the next shift the decision, its review or expiry date, and the contacts for complaints and incidents.

Rehearsals for consequential decisions

A storm-relief office wants its intake tool to sort applications. In a tabletop exercise, give the team two records for the same household, one with a damaged image of the address. The tool should flag the incomplete address for staff follow-up. The duty supervisor checks whether the system kept the original timestamp and left both submissions traceable while staff resolve the match. Someone who cannot provide a fresh scan should still be able to reach an officer. If a family drops out of the queue, close automated routing for that case type, restore its original place and find any other records affected by the same rule. Verify the fix with a new example before restarting that route.

A hiring officer can adapt the exercise using sample applications in the formats the organisation accepts. Remove names where possible and use paired examples with the same job-relevant experience expressed in different ways. Check which files reach the authorised reviewer. If the reviewer receives only a shortlist, their signature cannot correct the omission of qualified people they never examined. Test the excluded cases and change the review procedure before the tool can influence shortlisting.

For an appointment service, test a patient who cannot complete the voice menu and a receptionist who cannot reach the supplier. Design a handoff that preserves the request and lets an authorised member of staff follow established clinical escalation procedures. A missed callback belongs in the case review even when the software produced no inaccurate statement.

Complaints, remedies and incident response

Tell people when AI contributed to a decision and which record or rule mattered. Explain how to challenge a mistake and name the office that can change the outcome. Send a case reference through a channel the person can use. Offer a staffed route when an online form would exclude them.

Give the complaints officer access to the original evidence and authority to change the decision. If the complaint is upheld, record who repaired the source record and when. Obtain confirmation from each office that relied on it that the office corrected its own decision where permitted. Restore the missed service where possible, and check for other cases affected by the same error.

Tell the person what changed, how to verify it and how to request further review. Keep outstanding repairs open until their owners have acted.

Local deadlines for review

Under section 12 of the Cayman Islands Data Protection Act, a person notified of a covered, solely automated decision with significant effects has 21 days following that notice to require reconsideration or a new decision on a different basis. The controller then has 21 days from receipt of the person’s notice to explain in writing the steps it intends to take. Check the exemptions and applicable notice conditions. Cayman Islands Ombudsman guidance

Response during an incident

When a serious error is reported, the duty officer should stop the affected action and open the alternative service. Preserve necessary evidence under restricted access. The legal lead checks which notifications are required, who must receive them and when each deadline starts. Keep a dated account of what the team learned and did. Before restarting, reproduce the failure with safe test data, verify the repair and obtain a fresh release decision.

A notice people can act on

An example notice reads, “We used a tool to organise the information in your application. An officer made the decision. If a detail is wrong or you want another officer to review the decision, contact the service desk using the number on your decision letter. Give your case reference. Tell us how you can receive the reply.” Use this wording only if each statement is true and the letter gives a working number. Explain separately any applicable statutory route or deadline. Accept requests from people who cannot identify the system involved.

Keep identity checks proportionate. Record why an additional document is necessary if the original service did not require it. Accept a representative where permitted. If delay could cause immediate harm, give a named officer authority to protect the person’s place or access while the review is open.

During a network outage, use a numbered manual queue held by the duty supervisor. On restoration, match each outstanding case to its reference, look for duplicates, and confirm the

person can still reach a reviewer. Record any urgent case that went unheard and the corrective action taken. Reconcile pending messages before switching automatic notifications back on.

Operational records and attribution

A controlled spreadsheet or the organisation's case system can hold these records. Name the person responsible for each entry. Restrict access to the underlying evidence.

Working record	Fields to complete
Use and jurisdiction	Service, purpose, decision, affected people, countries and territories, law or advice checked, open scope question, owner
Risk register	Failure, cause, potential harm, people exposed, control, evidence the control operated, remaining risk, decision owner, review date
Evaluation case	Case identifier, date, language or channel, permitted inputs, expected result, observed result, source, severity, reviewer, release consequence
Decision and remedy	Case reference, evidence considered, reviewer, correction or reason for declining it, offices that relied on the error, confirmation of correction, message and next review route given to the person
Incident record	Discovery time, versions affected, containment, fallback owner, notification analysis, repair test, restart decision
Release record	Tested version, permitted action and audience, evidence links, open risks, decision, signatory, expiry, stop authority

Small offices and service retirement

A shop, school office or voluntary group can begin with one narrow task and a paper record of what the tool can access. Use a task that staff can check using a document already in hand, such as turning an approved list of opening hours into a notice. Ask another responsible person to check the first notices. If the only reviewer is unavailable, retain the approved notice or defer the change. The decision to connect customer records or let the tool contact people calls for a fresh assessment.

Retire a use when its authority expires or the organisation can no longer supply current evidence or operate a safe fallback. Revoke its permissions and close entry points that could still accept requests. Transfer open cases and test the appeals route. Record when retained files can lawfully be destroyed. A former applicant may still need evidence of a decision taken while the system was in service.

Citation and adaptation

Suggested citation. Dunkley, Adrian (lead author). *Caribbean AI Safety and Alignment Guidance*. Caribbean AI Association, 23 November 2026 (November 2026 edition). Official publication. For a local application, cite the relevant jurisdiction page and its access date as well.

For adapted material, name CAIA and Adrian Dunkley, identify the edition and sections used, and describe your changes. Credit translations with the translator and date. Cite each law, regulator and standard directly for the rule it issued. Obtain any permission needed to reproduce third-party material. Describe an adaptation as your own work and seek approval before claiming

endorsement by CAIA or a government. For a legal decision, retain the official text consulted and the date of the check.

JURISDICTION GUIDE

Anguilla

How to publish business survey results without exposing a respondent.

Introduction

In Anguilla, a statistician deciding whether to publish an AI-written survey summary needs to check the prose as carefully as the figures. A table might group businesses to protect a respondent, while the accompanying description gives away which firm supplied an answer. The Statistics Department's confidentiality guidance gives analysts and editors a starting point for deciding which material an assistant can see and which details the public can read.

Legal framework

Section 17 of the Statistics Act, chapter S60, restricts people working under the Act from communicating information acquired through that work without lawful authority outside the ordinary course of their employment. The Statistics Department describes how it protects respondents by changing the detail it publishes. Removing names alone may leave a firm identifiable.

Section 31 of the Electronic Transactions Act, chapter E38, gives the Governor in Council power to prescribe personal data processing standards. Subsection (3) addresses a controller or processor that registers voluntarily to a prescribed standard. Check which regulations exist and what any registration covers before relying on it.

Scope and legal status

Section 17 concerns information acquired during work under the Statistics Act. Identify the applicable confidentiality duty separately for a survey outside that remit.

Worked example

An analyst prepares a business survey report. The source table combines several firms, but a draft sentence identifies a firm by its district and occupation. Give the assistant only the table already cleared for release. Ask a disclosure reviewer to test whether a reader could work backwards from the description.

Implementation guidance

• Record the exact table the analyst may upload. Apply the same rule to fields typed into a prompt or copied into a vendor support ticket.

• Read draft captions alongside the tables. If the combination points to one firm, remove the identifying detail or combine categories before publication.

Decision and evidence to retain

The officer responsible for statistical release should keep the cleared table, edited narrative and reason for any suppression. Hold the report if either the table or the prose exposes an individual respondent.

Sources and attribution

1. Anguilla Statistics Department, statistical confidentiality and disclosure protection, including Statistics Act section 17
2. Government of Anguilla, Electronic Transactions Act, chapter E38, section 31

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Antigua and Barbuda

Patient recordings, clinical notes and a transcription provider’s access.

Introduction

A clinic in Antigua and Barbuda may want an AI service to turn a consultation into a note the clinician can check before the patient leaves. Procurement staff must first establish what happens to the patient’s voice after the note is complete. A provider that keeps audio to improve its product proposes a further use of sensitive information. The clinic has to account for that use when choosing the service and explaining it to patients.

Legal framework

Sections 5 to 8 of the Data Protection Act 2013 cover why data are collected, what a person must be told, disclosure and security. Section 8 requires a data user hiring a processor to obtain security guarantees and check that the processor takes reasonable steps to comply. Section 18 sets conditions for processing sensitive personal data. An appointment booking by itself gives the clinic no basis to assume the patient agreed to model training.

The government and UNESCO launched Antigua and Barbuda’s AI Readiness Assessment Report in 2025. Its recommendations inform planning for services such as health and education. The Data Protection Act sets the legal duties relevant to patient recordings.

Scope and legal status

Section 19 includes exemptions concerning health information. Check the wording and the patient’s circumstances before limiting an access request.

Worked example

Test the service with a scripted consultation in which the patient denies one allergy and reports another. The clinician compares the summary with the recording, corrects the entry and checks the signed note. Repeat with a passage the microphone does not capture clearly.

Implementation guidance

• Explain who can listen to the recording, why the clinic needs it, and how a patient can ask to see or correct information.

• Document the condition that permits the proposed handling of sensitive data. Ask the supplier to demonstrate access restrictions and what happens when the audio reaches its deletion date.

• Check whether a correction reaches any part of the patient record that copied the original summary.

Decision and evidence to retain

The clinical lead should approve the service only after checking how it handles uncertain audio and medication allergies. The officer responsible for patient data should retain the supplier’s access and deletion evidence and withhold approval while any proposed training use lacks a documented basis.

Sources and attribution

1. Antigua and Barbuda, Data Protection Act 2013, No. 10, sections 5–9, 12, 16, 18–19

2. UNESCO and Antigua and Barbuda, launch and findings of the AI Readiness Assessment Report

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Aruba

Guest records and the limits of reuse under Aruba’s own registration law.

Introduction

A guest explains a medical issue when disputing a hotel charge. That explanation may help settle the bill. It can also follow the guest into a risk score if the hotel later feeds its complaints register into a prediction tool. For an Aruban hotel manager, the first question is what the register was established to do and whether the proposed scoring serves that purpose.

Legal framework

Aruba, a constituent country of the Kingdom of the Netherlands, has its own Landsverordening persoonsregistraties (AB 2011 no. 37). Articles 3–8 cover why a register exists, which data it may contain, compatible uses and the holder’s duties to keep records accurate and secure. Article 6 allows certain sensitive information to be recorded only where the register’s purpose makes that unavoidable. Moving a register to a supplier can leave these duties intact. In July 2026 the government announced work on a national AI strategy.

Scope and legal status

Check whether this collection meets the statutory definition of a register, which exclusions apply and who may receive the data. Any EU legal duties depend on a separate territorial assessment.

Worked example

Before testing predictions about disputed charges, the hotel’s billing manager should compare the proposed use with the reason staff collected each complaint. Remove medical explanations from test records. Give the person who handles the dispute authority to release a charge hold.

Implementation guidance

• Write down the register’s purpose and how guests can ask what information it holds.

• Trace a deliberately mismatched guest record into the supplier’s copy. Correct the identity and check whether the flag disappears.

• Read the contract for supplier reuse of complaint details, and restrict staff access to the original text.

Decision and evidence to retain

The billing manager should retain the purpose assessment and the result of the mistaken-identity test. If correcting the guest’s record leaves the hold in place, suspend scoring, release any unsupported hold and check other accounts flagged for the same reason.

Sources and attribution

1. Aruba government legislation index and amendments
2. Central register, consolidated Landsverordening persoonsregistraties
3. Kingdom government, constitutional structure
4. Aruba government, launch of national AI strategy development

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

The Bahamas

Sovereign state. Credit scoring, shared customer records and outsourced decisions in Bahamian banks.

Introduction

A Bahamian bank that uses AI to rank loan applications makes a decision about who waits for a credit officer. An error can hold up a borrower long before anyone formally refuses a loan. Credit managers and compliance officers therefore need to inspect the order in which applications reach staff. Their review should identify which data protection provisions have commenced and whether the Central Bank's outsourcing guidance covers the supplier's role.

Legal framework

The Data Protection (Privacy of Personal Information) Act, 2003 sets rules for collecting, using, securing and retaining personal data. Section 6 limits use to purposes compatible with the original purpose and requires proportionate collection. Parliament also enacted the Data Protection Act, 2025 (No. 74). Its section 50 addresses decisions made solely by automated processing or profiling and includes exceptions. Section 1 allows the minister to bring different provisions into operation by Gazette notice.

The Central Bank publishes outsourcing guidance for the financial institutions it supervises. A bank considering a vendor's scoring service should assess whether the contract outsources a material function. The 2026 Speech from the Throne announced an intention to introduce an AI Governance Act. Check the published legislation for any subsequent enactment.

Scope and legal status

CAIA verified the enacted 2025 text. It did not verify a commencement notice for section 50 or for the repeal of the 2003 Act. Confirm the operative provisions with the Gazette and the relevant supervisor.

Worked example

A bank pilots a model that ranks small-business loan files. Its review finds that customers who use a shared family phone are grouped as duplicates. A lending officer checks those files before the ranking can delay or block a loan.

Implementation guidance

• Record the source and purpose of each input. Test whether shared phone numbers, addresses or devices cause distinct borrowers to be merged.

• Compare the model with the current review process across islands, including places with small samples. Report uncertain results to the credit committee.

• Identify the applicable provisions and any commencement notice before sending customers a legal notice or changing their rights process.

Decision and evidence to retain

The head of credit owns the ranking decision. Retain the trial results, the version of the model and the officer's reasons for reopening a file. If the tool merges two borrowers, suspend automatic grouping. Find other affected files and restore each applicant's original place in the queue.

Sources and attribution

1. Data Protection (Privacy of Personal Information) Act, 2003, section 6
2. Data Protection Act, 2025, sections 1 and 50
3. Central Bank of The Bahamas, minimum standards for outsourcing material functions
4. Office of the Prime Minister, 2026 Speech from the Throne

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Barbados

What a lender must check before a system can refuse a credit application.

Introduction

A lender in Barbados might use software to decide which credit applications reach a loan officer. An applicant screened out at the first stage may lose the opportunity to present income records or question a mistaken assumption. Before procurement, the head of lending needs to identify exactly where a refusal occurs, what authority the reviewer has and what the applicant will learn about the decision. The Data Protection Act makes those details consequential.

Legal framework

Section 18 of the Data Protection Act 2019–29 gives people a right against decisions based solely on automated processing that have legal or similarly significant effects. It includes profiling. Exceptions cover contractual necessity, authorisation by law with safeguards, and consent. Section 18 sets further conditions for sensitive data. Sections 19 and 20 address the information due about covered automated decisions, including the logic used and the likely consequences for the person.

Section 65 requires a data protection impact assessment before processing likely to create a high risk to a person’s rights and freedoms. It expressly covers systematic, extensive automated evaluation used for decisions with legal or similarly significant effects. The Barbados Data Protection Commission administers the data protection framework.

Scope and legal status

Section 18 turns on the effect of the decision, how it was made and any exception claimed. A signed screening result alone says little about whether the officer made an independent decision.

Worked example

Trial a credit application with irregular earnings. When the tool recommends refusal, have an officer open the underlying income evidence and decide the case independently. Check that the officer can reverse the result and that the applicant receives the corrected decision.

Implementation guidance

• Trace every step that can end an application, including a form that silently stops the applicant from proceeding.

• Give applicants an intelligible account of the information used and the likely consequence. Let someone unfamiliar with the model test the notice and the route to a reviewer.

• Investigate mistaken refusals, including cases involving irregular income. Link the correction to the application so it remains visible on reconsideration.

Decision and evidence to retain

The head of lending should approve the decision process only after the privacy lead records the section 18 analysis and the result of the section 65 assessment where required. Keep an example that demonstrates a real override and what the applicant sees.

Sources and attribution

1. Barbados Official Gazette, Data Protection Act 2019–29, sections 18–20 and 65

2. Government of Barbados, Data Protection Commission and contact details

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Belize

Sovereign state. Document screening and access to public scholarships in Belize.

Introduction

For a scholarship office in Belize, a document marked unreadable can become a missed term if no one contacts the student before the deadline. Officials buying software to screen applications should decide who can accept a corrected record and how applicants can reach that person. Section 14 of the Constitution gives the office a privacy question to resolve before it sends student records to a supplier.

Legal framework

Section 14 of the Belize Constitution protects people against arbitrary or unlawful interference with privacy, family, home and correspondence. A public agency considering automated screening should document its authority to use the records and the reason each category of information is necessary.

The National Assembly published the Data Protection Act, 2021 (No. 45). Section 19 addresses significant decisions based solely on automated processing and sets out exceptions and additional safeguards. Section 97 requires a ministerial order published in the Gazette for commencement and allows different dates. The government’s National Digital Agenda 2026–2030 sets a strategic direction for public services.

Scope and legal status

CAIA verified enactment and the section 97 commencement mechanism. The commencement order for section 19 was not located. Use its safeguards in design and confirm its legal status before issuing public notices.

Worked example

A scholarship office uses software to check whether submissions are complete. Applicants who upload photographs of handwritten records receive more missing-document flags. The office keeps applications open while a reviewer checks the originals.

Implementation guidance

• Use the software to identify documents that need a reader. An officer should be able to restore an application or extend its deadline.

• Test scans, phone photographs and multilingual names. A poor scan can conceal a perfectly valid record.

• Tell students where to submit corrections by telephone or in person. Agree how long to keep the original document and the correction record.

Decision and evidence to retain

The scholarship director approves the screening procedure. Keep a sample of disputed flags and the officer’s final decision, and restrict staff access to authorised reviewers. If the tool repeatedly flags readable files in one format, pause the automated flag. Keep the affected applications open for staff review and contact students before closing the award round.

Sources and attribution

1. Belize Constitution, section 14
2. Data Protection Act, 2021, sections 19 and 97
3. Government of Belize, National Digital Agenda 2026–2030

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Bermuda

British Overseas Territory in the North Atlantic. Overseas claims processing and retained responsibility in Bermuda’s financial sector.

Introduction

A Bermuda insurance manager considering an overseas supplier for claims summaries must first examine the proposed transfer of personal information. Even if staff in Bermuda approve every settlement, the supplier would still handle claimants’ records. The manager and the organisation’s privacy officer should trace the file from upload through deletion and determine what protection it receives abroad. Bermuda’s Personal Information Protection Act places responsibility for the transfer on the organisation.

Legal framework

The Personal Information Protection Act 2016 (PIPA) governs the use of personal information in Bermuda. Its 2024 Commencement Day Notice brought specified substantive provisions into force on 1 January 2025. Section 15 addresses transfers to overseas third parties. The organisation must assess the protection provided and, where required, use contracts or other safeguards to secure comparable protection. The Privacy Commissioner explains that hiring a third party does not remove the organisation’s responsibility.

In August 2026 the Bermuda Monetary Authority published a consultation paper proposing guidance for regulated financial services. It covers model validation, human oversight, third-party risk and auditability. Its proposals provide questions for vendor reviews.

Scope and legal status

The cited BMA paper is a consultation on proposed supervisory guidance. Verify whether a final note has replaced it before using it in a supervisory filing.

Worked example

An insurance manager plans to use an overseas service to summarise claims files. A trial summary confuses a past injury with a current diagnosis. A claims handler checks the original record and prevents the error from affecting the settlement.

Implementation guidance

• Assess the provider, its subprocessors and their locations. Record the transfer basis, who can use uploaded material and how deletion will be demonstrated.

• Use a test set with independently checked injury dates. Require access to the source document before a summary can support a settlement decision.

• Give the claims handler a correction route and check whether corrected facts reach downstream records. Repeat the test after a material model change.

Decision and evidence to retain

The claims manager approves the summary tool and the privacy officer records the overseas transfer assessment. Keep the supplier’s deletion evidence and the reviewer’s findings. If the tool confuses an old injury with a new one, withdraw the affected summary from the file and examine other cases before resuming that use.

Sources and attribution

1. Bermuda, Personal Information Protection Act 2016, section 15
2. Personal Information Protection Act 2016 Commencement Day Notice 2024
3. Privacy Commissioner, organisations and overseas third parties
4. Bermuda Monetary Authority, August 2026 AI consultation paper

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Bonaire

How a housing applicant can recover a lost place in the queue.

Introduction

For a housing provider on Bonaire, a ranking tool changes who receives the next offer. A gap in the rent ledger could move an applicant down the list even when the applicant paid on time. The staff member checking the records needs to know which data the tool used and whether a correction can restore the person’s place before the home goes to someone else.

Legal framework

Bonaire is a public body within the Netherlands. Articles 7–11 of the Wet bescherming persoonsgegevens BES govern collection purposes, legal grounds, compatible use, retention and data quality for covered records. Article 34 addresses decisions based entirely on automated profiling of aspects of personality that have legal or similarly serious effects. It includes exceptions. In 2026 the BES privacy supervisor called on the immigration service to improve, among other matters, access controls, retention and deletion.

Scope and legal status

Check the rules governing the housing allocation itself and the terms for any Article 34 exception. The supervisor’s immigration findings concern that service.

Worked example

Enter a sample payment under a variant of the tenant’s surname, then run the ranking. Check how staff discover the mismatch and whether a corrected ledger changes the order of offers. Avoid using actual applicants for the trial.

Implementation guidance

- Record the source of each ranking factor and why the housing provider needs it.
- Set a deletion date for test files and check that the provider and supplier remove their copies.

Decision and evidence to retain

The allocations manager should keep the queue order before and after correction, with a timestamp for the next offer. If the team cannot restore the applicant’s place in time, suspend automated ranking and allocate from the checked list.

Sources and attribution

1. Wet bescherming persoonsgegevens BES, articles 7–11 and 34
2. Rijksdienst Caribisch Nederland, supervisor’s June 2026 findings
3. Kingdom government, constitutional structure

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

British Virgin Islands

Overseas handling of identity documents by a trust services provider.

Introduction

When a British Virgin Islands trust services firm buys software to read identity documents, the client file may travel further than the upload screen suggests. A technician overseas might open a diagnostic copy after an apparent mismatch. The compliance officer needs to trace that journey and establish the basis for each transfer. The operations manager also needs a way to undo the mistake if the software links two different clients.

Legal framework

In the territory’s legislation, the jurisdiction is called the Virgin Islands. Section 6 of its Data Protection Act 2021 binds the Crown. Section 4 sets territorial and private commercial processing tests, including when a business engages a processor. Statutory Instrument 80 of 2021 brought the Act into force on 9 July 2021. Under section 7(1)(c), a transfer outside the territory requires proof of adequate safeguards or the individual’s consent. Sections 8 to 13 address matters including notice, security, retention and data quality. Section 20 addresses sensitive personal data.

The government appointed an Information Commissioner effective 11 May 2026. The Commissioner receives complaints about breaches of data protection principles.

Scope and legal status

Check section 4 against the firm’s activities and connections to the territory. Sector duties and professional confidentiality may apply alongside the Act.

Worked example

Give the provider invented records for two people with similar names. If the software merges them, ask an officer to compare the source documents, separate the files and identify which teams have already received the incorrect match.

Implementation guidance

• Map where backups, diagnostic files and support tickets go. Obtain evidence of the safeguard or consent for the transfers involved before loading real documents.

• Give clients a contact for mistaken identity. Track every correction through the customer record and any downstream checks that used the inaccurate match.

Decision and evidence to retain

The compliance officer should retain the provider’s list of locations and recipients, transfer grounds and results of the mistaken-identity test. Hold the upload of real client documents if the provider cannot identify who can open a support copy abroad.

Sources and attribution

1. Virgin Islands Gazette, Data Protection Act 2021, No. 3
2. Virgin Islands Gazette, Statutory Instrument 80 of 2021, commencement notice
3. Government of the Virgin Islands, Information Commissioner appointment and functions

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Cayman Islands

British Overseas Territory. Automated hiring decisions and an applicant’s right to seek reconsideration.

Introduction

A hiring manager in the Cayman Islands can shortlist applicants with an assessment tool or allow the tool to reject them outright. The distinction matters to a person seeking another review. Section 12 of the Data Protection Act addresses certain decisions made solely by automated processing. Employers need to know who made the final decision, when the applicant received notice and who can change the outcome.

Legal framework

Section 12 of the Data Protection Act (2021 Revision) addresses significant decisions based solely on automated processing. The Ombudsman explains how an individual can object in writing and, when a covered automated decision is made, how notice and reconsideration work. The person has 21 days after receiving notice to require reconsideration. The controller then has 21 days after receiving the request to explain in writing the steps it intends to take. Exceptions apply.

The Cayman Islands Monetary Authority’s Statement of Guidance on outsourcing directs covered firms to assess the materiality of an arrangement. A firm should establish how it can monitor a provider, maintain the service and recover records if the provider fails.

Scope and legal status

Apply the statutory conditions and exceptions to the particular decision. Check the scope of the Monetary Authority’s guidance for the entity’s licence.

Worked example

A recruiting platform proposes to reject applicants automatically after an online assessment. Before enabling that option, the employer identifies which decisions section 12 covers and gives a named hiring officer the power to reopen applications.

Implementation guidance

• Tell applicants where to send written notices. Track the date the decision notice was received and the date a reconsideration request arrived.

• Give the reviewer access to the application and underlying evidence. Record the reviewer's reasons and any correction to the decision.

• If a supervised firm relies on a vendor, test whether it can export decision records and continue handling requests when the service is unavailable.

Decision and evidence to retain

The recruitment lead keeps the assessment version, the underlying application and the correspondence relevant to a challenge under an approved retention schedule. Give a deputy access to pending notices. If the team cannot reconstruct why someone was rejected, suspend automatic rejection and reopen decisions affected by the same failure.

Sources and attribution

1. Data Protection Act (2021 Revision), section 12
2. Cayman Islands Ombudsman, rights in relation to automated decision-making
3. Cayman Islands Monetary Authority, Statement of Guidance on outsourcing

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Colombia

Colombia’s Caribbean coast and the privacy assessment required before certain high-risk AI projects.

Introduction

In a hospital on Colombia’s Caribbean coast, a missed-appointment score could determine who gets a reminder. It could also lead staff to delay offering a new appointment to someone they expect to miss it. A clinical service manager commissioning such a system needs to decide what staff may do with a flag. That choice matters before design begins because Colombia’s privacy regulator gives specific instructions for AI projects likely to place people at high risk.

Legal framework

Law 1581 of 2012 sets Colombia’s general rules for personal data. The Superintendencia de Industria y Comercio (SIC) issued External Circular 002 of 2024 to organisations under its data-protection supervision. Where an AI product is likely to pose a high risk to people whose data it uses, the circular requires a documented privacy impact study before design and development. The study must describe the processing, assess risks to people’s rights and set out safeguards. CONPES 4144 sets national AI policy.

Scope and legal status

The circular concerns personal data and organisations within the regulator’s remit. The service may also face sector rules, particularly in health or finance.

Worked example

Before commissioning a model, compare its intended use with a simpler option, such as offering reminders to all eligible patients. Record what would happen to someone the tool flags incorrectly and who could still book their appointment.

Implementation guidance

• Describe the information used for training and the records staff would enter when the tool is in service.

• Give each safeguard in the privacy study an owner and a test. Give the scheduling team authority to remove an incorrect flag.

Decision and evidence to retain

The clinical service manager should keep the pre-design assessment and the outcome of a booking test for a wrongly flagged patient. If the test delays access to care, keep the model out of scheduling until the team can show that patients can use the ordinary booking route without delay.

Sources and attribution

1. Law 1581 of 2012, Colombian judicial legislation service
2. SIC External Circular 002 of 2024, official text
3. CONPES 4144, national AI policy
4. SIC Circular 002, alternative copy of the signed text

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Costa Rica

When a travel booking becomes a marketing profile.

Introduction

A traveller arranging a tour on Costa Rica’s Caribbean coast might ask for a vehicle that can carry a wheelchair. Staff need that detail to plan the trip. If the operator later uses booking messages to select people for advertising, the same information takes on a different purpose. The manager buying the marketing tool should check what the traveller agreed to and what happens to the booking if the traveller declines personalisation.

Legal framework

Law 8968 protects people whose personal data an organisation processes. Articles 5–7 address informed consent, data quality and the rights to access and correct information. Executive Decree 37554-JP implements the law. The science and technology ministry issued the National AI Strategy 2024–2027 to guide national adoption. The operator still needs a legal basis for any new use of customer records.

Scope and legal status

Check how the law treats the database, whether an exception applies and whether the database requires registration. Consult the current implementing regulation.

Worked example

Trace an accessibility request from a booking message into the proposed list of advertising signals. Check the rules for sensitive information before a supplier receives it. Test whether a visitor can buy the same trip without a marketing profile.

Implementation guidance

• Match each proposed signal to the purpose the operator explained when collecting the information.

• Give customers a way to inspect the details behind an offer and request a correction. Compare booking availability and price with personalisation turned off.

Decision and evidence to retain

The bookings manager should retain the original collection notice and both trial bookings. If declining a marketing profile removes an available trip or changes its price unexpectedly, stop using that profile and restore the ordinary booking option.

Sources and attribution

1. Procuraduría General de la República, Law 8968
2. Executive Decree 37554-JP, implementing regulation
3. MICITT, publication of the National AI Strategy

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Cuba

Cuban law protects an identifiable caller’s voice, even after the call has ended.

Introduction

A recording made to route a municipal service request can outlast the request itself. A supplier may want to keep the recording to improve its speech model. For a Cuban service director deciding whether to agree, the starting point is what the caller was told, who can authorise that further use, and what happens to the resident’s report if the software sends it to the wrong department.

Legal framework

Law 149/2022 covers identifiable personal data in paper and electronic records. Article 4 includes voice and images. Article 10 requires a specific purpose, limits on what an organisation collects, accurate records and safeguards for the information. Consent is the general rule under Article 11, which recognises statutory exceptions. Articles 15–17 set stricter conditions for sensitive data.

For public administration, Ministry of Communications Resolution 24/2026 sets out how institutions should assess possible uses of AI, plan their introduction and monitor results. The Ministry published it in the official gazette on 17 November 2026, with commencement seven days after publication.

Scope and legal status

At the review date of 23 November 2026, the public-administration resolution was due to take effect on 24 November. Law 149 already covered public and private processing within its scope.

Worked example

In a pilot for reporting service faults, have staff place a test call using an invented street address. Follow the audio and transcript from the call centre to the department handling the fault. Check whether the supplier retains another copy after the request closes.

Implementation guidance

• Record who authorised each use of the voice file and transcript. Where the service relies on an exception to consent, identify the provision and explain why it applies.

• Set a deletion date for each copy. Give the caller a way to access their record or correct the address without recording a second account of the fault.

Decision and evidence to retain

The service director should examine the test-call record and a demonstration that staff can recover a misdirected request. If the supplier cannot account for its copy, withhold permission to send live recordings. If a routing error loses the request, return calls to staff until the recovery test succeeds.

Sources and attribution

1. Cuban National Assembly, Law 149/2022 on Personal Data Protection, official text via WIPO Lex

2. Cuban Official Gazette No. 96 of 17 November 2026, Resolution 24/2026, gazette facsimile

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Curaçao

Where clinic recordings go under Curaçao's personal-data ordinance.

Introduction

A clinic in Curaçao considering automated consultation notes needs to know who can hear the appointment. A supplier may receive the recording, keep a transcript and allow a technician elsewhere to open a support copy. The medical director and the person signing the purchase order need an answer for each copy. The island's ordinance makes the destination especially important when information leaves the Kingdom of the Netherlands.

Legal framework

Curaçao is a constituent country of the Kingdom. Its Landsverordening bescherming persoonsgegevens (AB 2010 no. 84) sets conditions for lawful processing, information that must go to the person concerned and individual rights. Chapter 8 covers transfers outside the Kingdom. The Regulatory Authority reported consultations on a proposed national AI strategy in November 2026.

Scope and legal status

The local ordinance and health-sector rules both matter. Trace the countries where the supplier stores data or permits remote access before deciding which additional laws apply.

Worked example

Follow a sample recording from the consultation room to the finished note. Ask the supplier to show where a support technician would retrieve it and what remains after the clinic deletes the audio. The treating professional should check the draft against the consultation before signing it.

Implementation guidance

- Check the duties for health information at each location that receives a copy.
- Publish a contact for patients who find a transcription error. Set separate retention periods for recordings and signed notes.

Decision and evidence to retain

The medical director should retain a diagram showing the destinations and a dated record of the deletion test. If the supplier cannot account for a support copy, keep live recordings out of the service until the clinic verifies access and deletion.

Sources and attribution

1. Central Bureau of Statistics Curaçao, local ordinance and official text
2. Regulatory Authority of Curacao, 9 November 2026 consultation update
3. Kingdom government, constitutional structure

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Dominica

Prices quoted in online sales and privacy promises made by the government portal.

Introduction

An excursion operator in the Commonwealth of Dominica may use a booking assistant that a visitor encounters before speaking to a guide. A wrong fare or cancellation term can affect the visitor’s decision to pay. The operator needs to know which price list the assistant uses and what the customer saw at checkout. A government team answering enquiries faces a different question about how the portal has promised to handle residents’ messages.

Legal framework

Section 37 of the Electronic Transactions Act 2013 requires a person selling to consumers electronically to supply accurate, accessible information about the seller and the goods or services, including terms and costs. Section 38 addresses unwanted communications.

The government portal’s privacy policy describes how it uses details people supply by contact form or email to answer enquiries. It limits disclosure, with exceptions for another government agency where the question concerns that agency and where the law requires disclosure. A ministry considering an enquiry assistant should compare the provider’s proposed use of messages with those commitments.

Scope and legal status

Apply the government notice to the service it describes. Read section 37 for the trader’s separate duties to consumers.

Worked example

Ask a booking assistant whether a fare includes a mandatory charge. Then ask what happens if the customer cancels on the day. Compare both answers with the price list and published booking terms. Where no approved answer exists, send the question to a member of staff.

Implementation guidance

• Test the full charge and identity of the seller before accepting payment. Keep the terms the customer actually saw.

• If the assistant invents a refund rule, correct its answer and identify bookings made while customers could see it.

• For a government portal pilot, keep identifiable enquiries out of vendor training and specify when an officer can forward a message to another agency.

Decision and evidence to retain

The booking manager should retain the approved price list, test conversation and checkout receipt for the same transaction. Pause automated quotes if those records disagree on what the customer owes.

Sources and attribution

1. Commonwealth of Dominica, Electronic Transactions Act 2013, No. 19, sections 37–38
2. Government of Dominica, Web Portal Privacy and Security Policy

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Dominican Republic

Public agencies must account for the part AI plays in a decision about public services.

Introduction

A public agency considering a ranked list for housing repairs has to account for the applicant near the bottom as well as the family at the top. A missing report could put a household with a damaged roof behind less urgent cases. The Dominican public-service AI code gives the programme director practical questions to answer before buying a scoring tool, including how an applicant can challenge the ranking.

Legal framework

Law 172-13 protects personal data in covered public and private files and databases used to provide reports. People can seek access and correction. The 2023 National AI Strategy sets policy direction. Decree 787-26 of 2 November 2026 approved the Code of Ethics for AI in Public Services for centralised and decentralised public administration, including public enterprises within its scope. Covered contracting bodies must secure audit rights and require suppliers to document how decisions were reached, protect information and permit oversight.

The code calls for an ethical and rights impact assessment before a system goes live if it could affect rights, essential services, public resource allocation or sanctions. A person affected by an administrative decision must be able to find out when AI helped make it and seek human review. Article 14 allows institutions 180 calendar days from publication to adapt. Human oversight continues during that period.

Scope and legal status

Apply the decree’s transition provisions and any instructions issued by the competent authority for the project date. A supplier’s obligations may arise through its contract with a public body.

Worked example

Give a housing officer two staged applications with the same repair need. Remove the inspection date from one. If the tool treats that missing date as a reason to lower priority, establish what staff would need to verify and correct the ranking before the decision reaches the applicant.

Implementation guidance

• Enter the supplier, model version and officer responsible in the agency’s AI register. Record any defects that remain open.

• Include audit and decision-record requirements in the tender. Ask the supplier to reproduce a case after a software update.

• Explain which application details influenced priority and give the applicant an accessible route to the officer who can amend the decision.

Decision and evidence to retain

The programme director should see the impact assessment, both test files and the supplier’s reconstruction of the disputed score. If staff cannot explain or change a priority that affects access to repairs, keep assigning cases manually. Re-test the affected cases after the supplier corrects the handling of missing dates.

Sources and attribution

1. Office of the President, Law 172-13 on personal data
2. Dominican government, National AI Strategy
3. Decree 787-26 and Code of Ethics for AI in Public Services
4. OGTIC, public-sector implementation guidance

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

El Salvador

Registration duties for AI that controls individual insurance prices.

Introduction

An insurer in El Salvador buying a pricing model needs to know whose judgement sets the premium offered to an individual. A tool that effectively fixes the price can put the insurer within the National AI Agency's registration rules. The insurer's compliance officer should trace a quoted premium from the customer's details to the offer and establish whether staff have genuine discretion to change it. The answer affects what the operator must do before deployment.

Legal framework

Legislative Decree 144 of 2024 regulates personal-data processing. Legislative Decree 234 of 2025 establishes the AI and technologies promotion framework. Under Article 11 of the National AI Agency's Resolution 0001/2025, operators must register qualifying consequential decisions in listed areas, including individual credit or insurance, public benefits and certain employment decisions. A consequential decision is one in which AI plays a controlling role and meets the resolution's definition. Article 12 lists exclusions. Article 10 sets additional safeguards for systems subject to registration. Central bank instrument CNBCR-06/2026 addresses these requirements for supervised financial operators.

Scope and legal status

El Salvador is included through membership in the Association of Caribbean States. Its coast faces the Pacific. Registration depends on the operator, the effect of the decision and any applicable exclusion.

Worked example

Determine who operates the pricing system and compare its use with Articles 10–15 of the resolution. A supplier offering a general-purpose tool and an insurer deploying it have distinct roles. Check sector rules and complete any required registration and impact assessment before issuing live quotes.

Implementation guidance

• Record the basis for mandatory registration, an exclusion or the separate voluntary registration route.

• Name the officer who monitors quoted prices, responds to incidents and communicates with customers. Revisit registration when a trial starts influencing actual offers.

Decision and evidence to retain

Before the first live quote, the compliance officer should retain the pricing trace and any required National AI Agency registration record. If a trial begins setting prices before that assessment is complete, withdraw the model from quoting and check every offer it affected.

Sources and attribution

1. Official judicial repository, Legislative Decree 144
2. Official judicial repository, Legislative Decree 234
3. National AI Agency, Resolution 0001/2025
4. Association of Caribbean States, membership
5. Central Reserve Bank, AI requirements for supervised financial operators, CNBCR-06/2026

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

French Guiana

A missing street address can alter a household’s place in a public-service queue.

Introduction

Consider a public service that sends mobile teams to households in French Guiana. If its scheduling tool accepts only standard street addresses, an officer may never see requests described by a river landing or a local landmark. The service director must decide how staff will find and reconsider such cases before the schedule fixes who receives a visit. French and EU rules govern the use of personal information and certain administrative decisions.

Legal framework

French Guiana is a French territory in South America and an EU outermost region. This guide includes it in its wider Caribbean coverage. The EU General Data Protection Regulation (GDPR) and France’s Loi Informatique et Libertés apply to covered processing. GDPR Article 22 gives a person the right to avoid a solely automated decision that has legal or similarly significant effects, subject to specified exceptions and safeguards. French administrative law also requires notice for a covered individual administrative decision based on an algorithm. An officer recording a name against a decision should be able to show what they checked.

Scope and legal status

Judge the effect of a queue position on the individual and whether the officer exercises genuine discretion. Check the applicable AI Act provision and date independently of the GDPR Article 22 assessment.

Worked example

Enter an authorised test request with a landing name and no street number. Follow it from intake through scheduling. If it fails to match, an officer should receive it in time to verify the location and book the household’s visit.

Implementation guidance

• Test the address formats the service accepts, using staged or authorised records. Review unresolved cases with staff who know the locations.

• Give residents a telephone or in-person route to correct an address. Give staff the source record, time and authority to change the schedule, and record the reason when they do.

Decision and evidence to retain

The field-service director should inspect the unmatched queue and a corrected visit schedule before authorising use. Suspend automatic ordering if an unmatched request disappears or staff cannot move it back into the queue. Verify that every affected household has a recorded next action before restarting.

Sources and attribution

1. European Commission, Europe’s outermost regions
2. European Union, General Data Protection Regulation, Articles 5, 6, 9, 22, 35 and Chapter V
3. CNIL, how French data protection law applies overseas
4. France, Code des relations entre le public et l’administration, Article L311-3-1
5. European Union, AI Act, consolidated text of 27 July 2026

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Grenada

Customer risk checks under Grenada’s banking standard.

Introduction

A Grenadian bank may consider an automated check that directs lower-risk customers to a simpler account-opening process. Missing paperwork could lead the system to reject an applicant or assign a risk category the bank cannot justify. The officer responsible for customer checks needs enough evidence to decide whether simplified identity checks are justified. For this decision, the Eastern Caribbean Central Bank has issued a standard with a verified start date.

Legal framework

The Eastern Caribbean Central Bank’s Simplified Due Diligence Prudential Standard No. 02 of 2025 for Grenada took effect on 1 April 2025. Institutions licensed under Grenada’s Banking Act must establish low risk before applying simplified checks and periodically review customers’ risk as circumstances change.

Grenada also enacted the Data Protection Act, No. 1 of 2023. Sections 7 to 14 set out principles and compliance procedures. Section 19 addresses correction of personal data. Under section 1(2), a ministerial order in the Gazette sets commencement and may choose different dates for different provisions. CAIA could not verify an order for these provisions.

Scope and legal status

The central bank standard applies to institutions licensed under Grenada’s Banking Act. Verify the commencement of each privacy provision before relying on a statutory right or enforcement power.

Worked example

In a trial file, an applicant provides an unfamiliar form of address evidence. Compare the model’s recommendation with the assessment a trained officer makes against the bank’s written criteria. Have the officer document the reason for selecting the ordinary or simplified process.

Implementation guidance

• Give staff access to the underlying evidence and authority to refer uncertain cases. Check what the model does when an input is missing.

• Reopen a case after receiving updated customer information. Record who changed the risk category and whether the change reached teams that relied on the earlier one.

Decision and evidence to retain

The bank’s compliance lead should keep the decision criteria, independent file reviews and reasons for any disagreement. Hold automated routing if the team cannot explain a risk category assigned to an applicant with missing information.

Sources and attribution

1. Grenada, assented Data Protection Act 2023, No. 1, public reproduction of the enacted text
2. Eastern Caribbean Central Bank, Grenada Simplified Due Diligence Prudential Standard No. 02 of 2025
3. The University of the West Indies Data Protection Office, Grenada country note

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Guadeloupe

Applicants can ask how an algorithm influenced a covered administrative decision in Guadeloupe.

Introduction

A public training programme has enough places for only part of its applicant list. If an algorithm helps decide who receives an offer, the programme officer needs a record that will still make sense after the next intake. In Guadeloupe, French administrative law gives a person a way to ask about an individual decision based on an algorithm. That matters most when a wrong entry costs someone a place.

Legal framework

Guadeloupe is a French territory and an outermost region of the European Union (EU). The General Data Protection Regulation (GDPR) and France's Loi Informatique et Libertés govern personal information within their scope. Article L311-3-1 of the French public-administration code requires express notice for an individual administrative decision based on algorithmic processing, subject to statutory exceptions. On request, the administration must communicate the rules and main features of the processing as the article specifies. The EU AI Act separately classifies a system by its purpose and the operator's role.

Scope and legal status

The 2026 amendment moved the AI Act's Annex III high-risk rules to 2 December 2027. Existing administrative and data-protection duties follow their own timetables.

Worked example

Prepare a test file for an applicant whose recorded qualification is wrong. Take the original award decision, correct the qualification and compare the results. Have an officer show what changed and identify the person authorised to reconsider the award.

Implementation guidance

• Write the notice and record the decision criteria before offering the first training place.

• Keep the version used for each intake. Test the explanation in everyday French and ask local speakers to review any Creole assistance the programme offers.

• Record whether the use requires a data-protection impact assessment. Check the AI Act classification and its date separately.

Decision and evidence to retain

The programme director should review the original and corrected award records and read the notice an applicant would receive. If the office cannot recover the scoring rules for that intake, refer affected awards for individual review and suspend automated ranking until staff can reconstruct the decision.

Sources and attribution

1. European Commission, Europe's outermost regions
2. European Union, General Data Protection Regulation, Articles 5, 6, 9, 22, 35 and Chapter V
3. France, Code des relations entre le public et l'administration, Article L311-3-1
4. European Union, AI Act, consolidated text of 27 July 2026
5. European Commission, AI Omnibus and revised application dates

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Guatemala

Public relief instructions and private case files in a municipal chatbot.

Introduction

A household in Guatemala looking for storm assistance should be able to ask where to apply without exposing a neighbour’s claim. The municipal officer responsible for a public chatbot needs to know which documents it can search. An instruction sheet can answer a public question. A completed form may contain information about a particular household, and a resident seeking a correction needs someone who can amend the official case file.

Legal framework

Article 31 of the Constitution gives people access and correction rights for information held about them in state registers, including the right to know its purpose. Articles 30–34 of Decree 57-2008, the Access to Public Information Law, govern personal data held by covered entities. Article 31 of that law addresses written consent for dissemination, distribution or sale and prohibits the sale of sensitive data. Article 32 lists exceptions to consent. In November 2026 the government announced work on a national AI strategy.

Scope and legal status

Decree 57-2008 defines the entities that owe these duties. Check whether a private contractor falls within that definition and what its contract requires.

Worked example

Build the public search collection from approved instructions and blank application forms. For a resident asking about an individual case, route the request to a service that verifies identity and gives staff access to the correct file.

Implementation guidance

• Review each document before the chatbot can retrieve it.

• Try a query naming a neighbour using an invented case. Check that the answer cannot reveal the address or application.

• Provide an officer or staffed phone line for corrections and questions the chatbot cannot answer.

Decision and evidence to retain

The municipal records officer should keep an inventory of public documents and a copy of the invented-case test. If the service retrieves a completed form, disconnect that collection, investigate earlier disclosures and keep the staffed service available.

Sources and attribution

1. Constitution of Guatemala, article 31

2. Decree 57-2008, Access to Public Information Law

3. Government notice of strategy development, 9 November 2026

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Guyana

Sovereign state. Fair access to public telehealth appointments and the status of clinical AI proposals.

Introduction

A public telehealth provider in Guyana has to decide what happens when a patient loses the connection halfway through an appointment request. A queue that discards the record can leave the person waiting without anyone knowing. Programme managers should examine how the queue treats incomplete requests in light of the Constitution's equality guarantee. Those considering clinical software also need to check the status of the digital health legislation.

Legal framework

Article 149D of the Constitution protects equality before the law and equal protection and benefit of the law. A public body rationing a service through an AI-assisted queue should be able to explain what drives priority and how it identifies people whom the process overlooks.

The Data Protection Act 2023 (No. 18) was gazetted on 16 August 2023. Section 19 addresses significant decisions based solely on automated processing, including profiling. Commencement depends on ministerial order under section 1. Separately, the Telehealth and Digital Health Services Bill No. 15 of 2026, as gazetted on 10 November, proposes provider responsibility for clinical decisions, independent validation and monitoring of clinical AI.

Scope and legal status

CAIA did not verify a commencement order for section 19. The telehealth source is a published bill. Check for an assented Act and its commencement before treating the proposals as binding.

Worked example

A public telehealth programme trials software to route requests for appointments. Slow connections leave some submissions incomplete. A coordinator calls back patients with incomplete submissions before the system can remove them from the queue.

Implementation guidance

• Compare waiting times and abandoned submissions across connection types and service areas. Keep a phone-based route and record when the fallback works.

• Assign a clinician to review clinical prioritisation and give the coordinator authority to restore a lost queue position.

• Before setting contract terms, have the legal lead record which parts of the 2023 Act have commenced and whether Parliament has enacted the telehealth bill.

Decision and evidence to retain

The programme director owns the queue and appoints a clinician to review priority decisions. Keep the original request time, call-back outcome and any restored appointment in the patient record. If interrupted connections cause requests to disappear, switch to a staffed queue and recover the missing cases before expanding the pilot.

Sources and attribution

1. Constitution of Guyana, article 149D
2. Official Gazette, Data Protection Act 2023, sections 1 and 19
3. Official Gazette, Telehealth and Digital Health Services Bill No. 15 of 2026, Part IX

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Haiti

A public office must keep several ways open for residents to reach an electronic service.

Introduction

A resident using a Kreyòl-language assistant could receive a different filing date from the one printed on a French application form. For the head of a Haitian public office, the immediate question is whether the resident can still submit on time and speak with someone who can correct the advice. The decree governing electronic public services protects access through multiple channels and the confidentiality of the information people submit.

Legal framework

The decree on electronic communication with public administration, published in Le Moniteur on 29 January 2016, protects equal treatment and the confidentiality of records in public systems. Article 8 requires several service channels and provides for assistance offices. Article 7 gives the Protecteur du Citoyen oversight of the rights in the decree, alongside other competent bodies.

A separate rule applies to the financial institutions it covers. Banque de la République d’Haïti Circular 131 governs fair treatment of financial consumers, privacy and complaint handling. It took effect on 2 March 2026 and repealed Circular 109-1.

Scope and legal status

The 2016 decree concerns public administration. Circular 131 names the financial institutions within its scope. Other operators should check the instructions for their own sector.

Worked example

In a practice case, have a resident ask for a deadline by voice and then by text. Compare both answers with the current notice and follow the contact instructions all the way to an officer. If a public portal sends the resident on to a financial provider, identify which organisation handles a complaint at each step.

Implementation guidance

• Have Kreyòl and French speakers test deadlines, fees and required documents on a slow connection. Use the same official notice to check each response.

• Put the telephone number or assistance-office details beside the answer. Give the resident a case reference when staff correct an error.

• For a financial-service assistant, test the institution’s own complaint channel. Keep a record of the customer’s submission and response.

Decision and evidence to retain

The head of the public office should review the dated source notice, both test responses and evidence that a person received the request for help. Withdraw a wrong filing date immediately. Identify messages carrying that error, contact residents where possible and have the responsible officer decide how to handle any affected filing.

Sources and attribution

1. Republic of Haiti, administrative electronic communications decree, Le Moniteur No. 20, 29 January 2016
2. Banque de la République d’Haïti, Circular 131 on protection of financial consumers

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Honduras

Protecting households in public summaries of disaster assistance.

Introduction

A municipal team on Honduras's Caribbean coast might want to tell residents how it has allocated disaster assistance. Even after staff remove a name, a report could identify a family through a small settlement, an occupation and a description of a disability. The officer approving the report needs to see what the summary would reveal to a reader who knows the community. The source applications need their own access controls.

Legal framework

Articles 23–25 of the Transparency and Access to Public Information Law recognise habeas data, a safeguard for information held about a person. They restrict access to personal records and prohibit compelling disclosure of personal data that could cause discrimination or harm. CNBS Circular 025/2022 sets information-technology management rules for supervised financial institutions. Congress announced the introduction of a separate personal-data protection bill on 29 October 2026.

Scope and legal status

Check the latest gazette for any change in the October 2026 bill's status. Confirm which sector rules govern the organisation handling the records.

Worked example

Before generating a public account of relief spending, remove bank details and individual case descriptions from the working file. Ask a reviewer familiar with the area whether the remaining combination of details identifies a household.

Implementation guidance

• Identify the official authorised to release the municipal report and limit access to the original applications.

• If a supervised financial institution handles a related service, have it assess the supplier's technology and outsourcing arrangements.

Decision and evidence to retain

The official authorising release should record which details the local reviewer could recognise. If the reviewer can identify a household, withhold that summary and combine or remove details before a second review.

Sources and attribution

1. IAIP, Transparency and Access to Public Information Law
2. CNBS Circular 025/2022, information-technology management rules
3. National Congress, introduction of personal-data bill

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Jamaica

Sovereign state. Claims assessment, overseas processing and the rights of policyholders in Jamaica.

Introduction

An estimate of motor damage can influence what a Jamaican policyholder receives after a collision. Before an insurer adopts a photo model, its claims manager needs to decide when an assessor will inspect the vehicle or ask the customer for more evidence. The Data Protection Act sets rules for certain solely automated decisions and for sending personal data abroad.

Legal framework

The Data Protection Act, 2020 gives people rights over certain significant decisions that rely solely on automated evaluation of personal data. Section 12 permits a written advance objection. For a covered decision already taken, it sets a notice and reconsideration process, including 30 days for the individual to request reconsideration after notice and 30 days for the controller to describe the steps it intends to take. Section 31 sets the conditions for overseas transfers and identifies exceptions.

The Data Protection Regulations, 2024 address how certain representatives may exercise rights on another person’s behalf. The Office of the Information Commissioner explains the eight processing standards. The National Artificial Intelligence Task Force’s policy recommendations offer a separate source for policy design.

Scope and legal status

Section 12 contains exemptions. An assessor’s actual role and authority matter when deciding whether a decision rested solely on automatic processing.

Worked example

A motor insurer uses a photo model to estimate damage. After a storm, the model misses damage in low-light photographs. An assessor inspects the images and the customer’s description before deciding a disputed claim.

Implementation guidance

• Give the reviewer authority to obtain better evidence and reverse the result. Preserve the original images and the reason for the decision within the approved retention schedule.

• For a covered solely automated decision, identify the notice and reconsideration route. Train staff to handle written requests and verify representatives under the regulations.

• Before transmitting identifiable claim files abroad, record the destination, purpose and section 31 transfer analysis. Test low-resolution and low-light images before each material update.

Decision and evidence to retain

The head of claims approves each use of the estimate. Keep the version, the assessor’s reasons and the customer’s correction with the claim under the retention schedule. If a model misses damage in poor light, route comparable claims to staff, identify settlements that relied on the estimate and reassess them.

Sources and attribution

1. Data Protection Act, 2020, sections 12 and 31
2. Data Protection Regulations, 2024
3. Office of the Information Commissioner, data protection standards
4. National Artificial Intelligence Task Force, policy recommendations

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Martinique

A clinician remains responsible for checking the referral letter that leaves the clinic.

Introduction

A referral letter can change meaning when a drafting tool drops a single word. For a clinic in Martinique considering such a tool, the decision starts with the clinician who signs the letter and the patient information the supplier would receive. Health records carry specific legal protections. A test must also show whether the clinician can spot a changed diagnosis or an incorrect urgency before another service acts on it.

Legal framework

Martinique is a French territory and an EU outermost region. The EU General Data Protection Regulation (GDPR) and French data-protection law apply to covered processing. A clinic must identify both its lawful basis under GDPR Article 6 and the Article 9 condition permitting its use of identifiable health information. Before processing likely to pose a high risk to people’s rights and freedoms, Article 35 requires an impact assessment. CNIL, the French data protection authority, publishes guidance on selecting and protecting data and respecting individual rights when developing AI.

Scope and legal status

Check the French health-sector rules and the intended medical purpose before clinical use. A tool that proposes diagnoses can fall under different requirements from one used only to draft correspondence.

Worked example

Give the drafting tool a staged note stating that a patient has no known allergy to a specified medication. Compare the original wording with the generated letter. Repeat with urgency and referral reason. The person signing needs the source note alongside the draft.

Implementation guidance

• Document which staff may use the tool, how long the supplier may hold notes and whether it may use them to develop another model.

• Where the clinic serves patients in more than one language, test mixed-language consultations that the tool claims to handle. Log changes to the clinical meaning.

• Maintain access records and a working manual referral process. Give clinicians a way to correct a letter after dispatch and notify its recipient.

Decision and evidence to retain

The clinical lead should examine the paired notes and drafts, including errors that staff missed on first reading. Withhold release if a test reverses a clinical fact and the review process misses it. Use manual letters while the defect is repaired, then repeat that case and similar referrals before resuming.

Sources and attribution

1. European Commission, Europe’s outermost regions
2. European Union, General Data Protection Regulation, Articles 5, 6, 9, 22, 35 and Chapter V
3. CNIL, how French data protection law applies overseas
4. CNIL, recommendations on developing AI systems
5. European Union, AI Act, consolidated text of 27 July 2026

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Mexico

Who answers for visitor complaints shared between a public office and a contractor.

Introduction

A Mexican public tourism office may ask a contractor to analyse complaints about a coastal destination. The office wants to learn which services visitors struggle to use. The contractor might also want to use the messages to train a commercial product. The procurement team should establish who chooses each purpose before records change hands. That decision also tells a visitor where to turn to inspect a complaint or correct a mistake.

Legal framework

Mexico issued two replacement federal privacy statutes in March 2025. The Ley Federal de Protección de Datos Personales en Posesión de los Particulares governs covered private holders. The Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados applies to covered public bodies. The private-sector statute covers privacy notices and the rights of access, rectification, cancellation and objection, known as ARCO. In January 2026 the science ministry and digital agency issued a separate declaration on AI ethics and good practice.

Scope and legal status

The competent authority depends on the holder, the level of government and the remedy sought. Check applicable state rules and implementing provisions.

Worked example

Have the office and supplier trace one complaint. Mark which copies the supplier holds on the office’s instructions. Examine any proposal to train the supplier’s own product as a separate use before granting access.

Implementation guidance

• Have the office identify its authority to analyse complaints and record its purpose in the contract.

• Assign responsibility for answering ARCO requests. Test whether a correction reaches the copies to which the law requires it to apply.

Decision and evidence to retain

The contract manager should keep the map of copies and the response to a test correction. If neither party can locate the version used to train a product, stop that transfer and resolve responsibility before sending more complaints.

Sources and attribution

1. Chamber of Deputies, Federal Law for Private Parties
2. Chamber of Deputies, General Law for Obligated Subjects
3. Secihti and ATDT, January 2026 AI ethics declaration announcement

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Montserrat

What a housing office can pass from a resident’s message to a repair contractor.

Introduction

A resident of Montserrat might describe a damaged roof and a family member’s illness in the same message to a housing office. A repair contractor needs the work details. Sending the whole message, or an AI summary that repeats the illness, expands who learns about the family. A public officer planning the service should establish the authority for that use and decide which details each person needs.

Legal framework

Section 9 of the Montserrat Constitution protects private and family life, the home and correspondence. It permits limitations when authorised by law and reasonably justifiable on the grounds the section specifies. A department proposing to analyse residents’ correspondence needs to consider those conditions in light of the service it provides.

Paragraphs 104 and 105 of the 2026–27 Budget Speech discuss data protection legislation and gaps in government AI use, including unclear guidance. The government stated its intention to seek legislation. To establish a statutory duty, consult the enacted text and its commencement.

Scope and legal status

Consult the current Acts and statutory rules for the department’s service. The Budget Speech records policy intent.

Worked example

Have a caseworker compare a sample resident’s request with the work order the assistant prepares. In the contractor’s view, check that the contractor receives the repair description and necessary address details while the private family information stays with the handling officer.

Implementation guidance

• Document what the housing office needs to schedule a job and which fields its contractors can see.

• Let residents report a fault or correct its priority by telephone. Give the handling officer access to the original message and authority to change the schedule.

Decision and evidence to retain

The department head should retain the legal basis for the proposed use and a sample of the contractor’s view with sensitive details removed. Keep work orders under manual review if the system passes household information to a contractor who has no need for it.

Sources and attribution

1. Government of Montserrat, Constitution, chapter 1.01, section 9
2. Government of Montserrat, 2026–27 Budget Speech, paragraphs 104–105
3. Attorney General’s Chambers, Acts passed in 2026

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Nicaragua

How a cooperative should read a repayment record before flagging a borrower.

Introduction

A cooperative on Nicaragua’s Caribbean coast could use a borrower’s repayment history to decide which applications need review. A recorded pause in payments, however, may reflect an agreed moratorium. If the software treats that pause as a default, the borrower can end up answering for a debt that was never overdue. The cooperative’s credit manager should establish what a supplier may see and how an officer can correct the resulting flag.

Legal framework

Law 787 covers personal data in public and private files, whether or not an organisation processes them automatically. The law’s definitions cover identifiable individuals and legal entities. They include financial and credit information among sensitive categories. Article 6 addresses consent and its exceptions. Decree 36-2012 implements the law. A cooperative sharing member records must therefore examine both the disclosure and the supplier’s proposed use.

Scope and legal status

The gazette copies establish the published instruments. Verify current implementing arrangements and any duties that apply to the particular lender.

Worked example

Construct a test ledger with a recorded payment moratorium. Follow the entries into the model and check whether a staff member reviewing the application can see why payments stopped. Ask the supplier what it retains after the review.

Implementation guidance

• Identify the file holder and recipient. Record whether the supplier wants to train on member records.

• Check whether the proposed disclosure requires consent or qualifies for a statutory exception. Document safeguards for sensitive financial data.

• Give the reviewer a correction procedure that reaches the ledger and the scoring system.

Decision and evidence to retain

The credit manager should retain the moratorium record and the decision before and after correction. If the model still marks the account overdue, stop sending its flags to loan officers and reopen cases with the same payment pattern.

Sources and attribution

1. La Gaceta 61, Law 787, archived official issue
2. La Gaceta 200, Decree 36-2012, archived official issue

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Panama

Panama’s personal-data rules when a lender proposes an automated loan rejection.

Introduction

In Panama, a lender considering an automated rejection rule needs to examine exactly where the final decision occurs. A missing payslip might mean the applicant earns irregularly. If the system reads it as zero income and closes the application, the applicant may never reach a credit officer. The head of lending should trace that path against Article 19 of the personal-data law and determine whether the applicant can supply the missing evidence.

Legal framework

Article 19 of Law 81 of 2019 protects a person from certain decisions based entirely on automated processing of personal data when the decision has negative legal effects or impairs a right. Its exceptions cover consent, necessity for a contract or legal relationship, and authorisation under special laws or their regulations. Executive Decree 285 of 2021 implements Law 81. Cabinet Resolution 75 of August 2026 approved the National AI Strategy.

Scope and legal status

The facts of the decision determine whether Article 19 applies. Any exception must meet the statute’s terms. The national strategy sets policy priorities.

Worked example

Enter two sample applications with the same earnings. In one, provide a payslip. In the other, leave the field blank for an applicant who can document income another way. Check where the second application goes and whether the officer can approve it.

Implementation guidance

• Trace each rejection path to its legal basis and any sector rules. Document the basis of any Article 19 exception.

• Record how customers can submit corrections and identify the complaints route under Article 18 for the institution involved.

Decision and evidence to retain

The head of lending should retain both test outcomes and evidence that the officer’s decision reached the applicant. If a missing document generates an unreviewable denial, suspend that rule and offer affected applicants a fresh assessment.

Sources and attribution

1. Law 81 of 2019, official gazette text, articles 18–19
2. ANTAI, Executive Decree 285 of 2021
3. Official Gazette, Cabinet Resolution 75 approving the AI strategy

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Puerto Rico

Puerto Rico requires written PRITS authorisation before a covered agency finalises an AI contract.

Introduction

An assistant that tells a resident where to enter their address does a different job once it advises them that they are ineligible for a benefit. A purchasing officer in Puerto Rico needs to know which job the agency intends to buy. That distinction affects the assessments the agency submits to the Puerto Rico Innovation & Technology Service (PRITS) and the checks a caseworker needs before anyone acts on an answer.

Legal framework

Government policy PRITS-POL-0012 took effect on 29 September 2025. It covers the executive branch, municipalities and suppliers acting within the policy's public-service scope. Before a new system or a significant change goes into production, agencies must assess its risks and effects and submit the assessment to PRITS for review and approval. Handling personal data requires a privacy impact assessment. Using AI to help decide an individual case requires an algorithmic impact assessment. Section 6.6.1.3 requires explicit written PRITS authorisation before the agency finalises an AI contract.

Article 3 of Law 111-2005, as amended, also requires covered database owners or custodians to notify affected Puerto Rico residents of security breaches that meet the conditions in that article.

Scope and legal status

The 2025 policy supersedes the conflicting 2023 circular. Check current revisions and the contractor's public-service role. Puerto Rico is a US territory, and applicable federal requirements depend on the sector and use.

Worked example

Use the Spanish-language benefit form the assistant will explain. Test a household whose eligibility depends on an unresolved fact. Check whether the answer points the resident to an officer or inadvertently discourages an application the agency should accept for consideration.

Implementation guidance

• Keep the PRITS decision, impact assessments and written purchasing authorisation with the contract. Document a significant change in the model or its purpose for reassessment.

• Map the steps for a suspected data breach under Law 111-2005 and relevant sector rules, including how the custodian reaches the owner and who decides which residents must receive notice.

Decision and evidence to retain

The agency project director should see the test answer alongside the benefit rule and a caseworker's explanation. Escalate any advice that could wrongly close off an application. Keep that function out of service until PRITS requirements are met and the caseworker confirms the corrected answer reaches the right review route.

Sources and attribution

1. PRITS, Policy for the Use of Artificial Intelligence in the Government of Puerto Rico, PRITS-POL-0012, signed bilingual text held by Universidad de los Andes

2. Government of Puerto Rico, Law 111-2005 on database security, as amended

3. US Department of the Interior, Puerto Rico

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Saba

Patient confidentiality and correction of an automated consultation note.

Introduction

A consultation note can change meaning when the speaker changes. For a clinic on Saba, a tool that records a relative’s illness as the patient’s diagnosis could put the wrong history in front of the next clinician. The clinical lead should examine two questions before allowing live recording. Can the team protect a patient who is recognisable from a rare case, and can it correct an error after a clinician signs the note?

Legal framework

Saba is a public body within the Netherlands. Article 16 of the Wet bescherming persoonsgegevens BES covers sensitive information, including health data. The following provisions set out exceptions. Articles 27 and 28 provide routes for people to find out what personal data an organisation holds about them and to seek corrections in defined circumstances. Removing a name can still leave enough detail to identify a patient.

Scope and legal status

Check clinical confidentiality and the legal conditions for sending information overseas. Assess what a recipient could infer from the full combination of details.

Worked example

Rehearse with an invented consultation in which the patient mentions a family member’s condition. Follow the draft through the clinician’s sign-off and then ask a second member of staff to demonstrate the clinic’s correction procedure.

Implementation guidance

- Identify the lawful basis and the applicable exception for health data before recording patients.
- Ask the supplier where it keeps audio and which support staff can hear it.
- Limit access to corrections and keep identifying excerpts out of demonstrations.

Decision and evidence to retain

The clinical lead should keep the signed test note and evidence that the amended diagnosis appears in the record the next clinician would see. If the wrong diagnosis persists, stop exporting drafts and review notes already filed through that workflow.

Sources and attribution

1. Wet bescherming persoonsgegevens BES, articles 16–23 and 27–28
2. Rijksdienst Caribisch Nederland, regulator findings on access and storage
3. Kingdom government, constitutional structure

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Saint Barthélemy

French law brings mainland data-protection rules into force in Saint-Barthélemy through an express provision.

Introduction

A guest asking a hotel for an accessible room may give the concierge more personal information than the booking itself requires. If the hotel plans to answer such requests through an AI service, its manager needs to know where messages go and who can read them. Saint-Barthélemy has an express French legal route for applying mainland data-protection rules. An EU AI Act assessment follows a different territorial test.

Legal framework

Saint-Barthélemy is a French overseas collectivity associated with the European Union (EU) as an overseas country and territory. Article 126 of France's Loi Informatique et Libertés names the island. For the purposes of that law, references to the EU General Data Protection Regulation (GDPR) mean the mainland French rules that apply by virtue of the GDPR. CNIL, France's data protection authority, explains that the same substantive regime applies overseas, subject to territorial provisions.

Article 2 of the EU AI Act has its own rules. An operator supplying the EU market, or an operator whose system produces output used in the Union, may fall within its scope in the circumstances the article defines.

Scope and legal status

Article 126 concerns data protection. Assess AI Act coverage separately using the operator's role, its connection to the EU market and where people use the output.

Worked example

Use a staged booking request for an accessible room. Trace the message to the staff member responsible for the room, the system storing the conversation and any supplier with access. Check whether the next guest who uses the assistant can recover any part of that request.

Implementation guidance

• Record who decides how the hotel uses guest messages, who processes them and from where. Give any separate use for model training its own legal review.

• Tell guests whom to contact for access, correction or deletion requests. Record the legal ground or safeguard for any transfer that requires one.

Decision and evidence to retain

The hotel manager should review a sample booking record and a list of everyone who can retrieve its chat. If another guest can see it, disable conversation retrieval, investigate the disclosure and arrange direct booking assistance. Restore the feature after separate test bookings keep their messages private.

Sources and attribution

1. European Commission, Overseas Countries and Territories
2. France, Loi Informatique et Libertés, Article 126
3. CNIL, how French data protection law applies overseas
4. European Union, AI Act, consolidated text of 27 July 2026
5. CNIL, recommendations on developing AI systems

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Saint Kitts and Nevis

When an automated ferry booking can bind a passenger.

Introduction

A passenger asking about a sailing between Saint Kitts and Nevis should be able to tell when an enquiry becomes a purchase. An assistant that mistakes a corrected date for a second booking creates a dispute over what the passenger authorised. The ferry operator can reduce that risk by showing the terms before payment and retaining a record of the action that completed each transaction.

Legal framework

Section 16 of the Electronic Transactions Act, chapter 18.44, recognises that a computer program can participate in forming a contract. Its conditions include the customer knowing or having reason to believe an action completes the transaction, and the parties being able to review the terms beforehand. Section 16(5) addresses a person’s material input error when dealing with an electronic agent. Its conditions concern the opportunity to correct the error, prompt notice and any benefit received.

The federation, called Saint Christopher and Nevis in its legislation, enacted the Data Protection Act, No. 5 of 2018. It sets out principles on security, retention, accuracy and access. Section 1(2) requires a ministerial commencement order in the Gazette. CAIA could not verify that order.

Scope and legal status

The 2018 privacy statute requires a commencement order separate from publication of the Act. Read section 16 of the Electronic Transactions Act in full for disputed contracts.

Worked example

Try changing a departure date after seeing the fare. The review screen should display the new sailing and terms, and the passenger should be able to go back. Check that only the confirmation action issues a ticket and that the receipt shows the agreed date.

Implementation guidance

• Test duplicate orders, corrections and cancellations. Check exactly what each button tells the passenger will happen.

• Provide a visible correction option before purchase and a staffed contact afterwards. Keep the booking confirmation and the resolution of disputed charges.

• Set separate retention periods for payment references and chat transcripts. Check who can retrieve either from backups.

Decision and evidence to retain

The booking manager should sign off on a test showing one confirmation, one charge and one correct ticket after a change of sailing. Keep the terms shown during that test. Hold ticket issuance if an enquiry alone can generate a charge.

Sources and attribution

1. Saint Kitts and Nevis Law Commission, Electronic Transactions Act, chapter 18.44, section 16
2. Saint Kitts and Nevis Law Commission, Data Protection Act 2018, No. 5
3. The University of the West Indies Data Protection Office, Saint Kitts and Nevis commencement note

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Saint Lucia

Language errors and medical information in an appointment queue.

Introduction

A Saint Lucian clinic considering an assistant for appointment requests needs to know what happens when it misunderstands a patient writing in Kwéyòl or switching between languages. A request placed in the wrong queue can delay contact with a clinician. Medical and reception staff should agree who reviews unclear messages, how the patient can reach the clinic directly and which parts of the Data Protection Act govern the information exchanged.

Legal framework

The Attorney General’s Revised Laws record partial commencement of the Data Protection Act, chapter 8.18. Statutory Instrument 4 of 2023 brought into force Part I, sections 32 to 43 of Part III, Part VI and paragraphs (a) to (g) of Schedule 2 on 31 January 2023. Sections 35 to 37 address sensitive and medical data. Sections 40 to 43 cover accuracy, use, security and destruction.

The 2023 order omits Part IV on registration, Part V on individual rights and section 45 on transfers. Check later instruments before treating any of those provisions as operative.

Scope and legal status

The verified 2023 order identifies provisions in force on its date. Check subsequent orders and clinical duties for the service being proposed.

Worked example

Ask clinicians and fluent local speakers to prepare two messages conveying the same concern in different words. Compare where the system sends each one. An authorised clinician should review uncertain and urgent messages, and a patient should still be able to contact the clinic by phone.

Implementation guidance

• Identify the condition permitting this use of health information. Restrict access to the people handling the appointment or clinical review.

• Record which test messages reached a clinician and which landed in the wrong queue. Repeat the test after changing the model or its language settings.

• Set a deletion rule for tool logs that accounts for separate retention duties governing the clinical record.

Decision and evidence to retain

The clinical lead should review paired language tests and a timed handover to a clinician. Keep the queue and outcome for each test message. Use staff intake while an unresolved error can leave a potentially urgent request in the routine queue.

Sources and attribution

1. Attorney General’s Chambers, Data Protection Act, chapter 8.18, commencement and arrangement of sections

2. National Printing Corporation, 2023 statutory instruments, including No. 4, Data Protection Act (Commencement) Order

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Saint Martin (French part)

A service shared across Saint-Martin and Sint Maarten must account for who can access data on each side.

Introduction

A visitor who reports a lost passport may want both sides of the island to check for it. A French-side tourism office considering a shared search tool must decide which details its partner needs to see. Sending a description and making a full passport number searchable have different consequences for the traveller. The French and Dutch parts of the island also have different relationships with the European Union.

Legal framework

French Saint-Martin is an EU outermost region. Sint Maarten is a Dutch overseas country and territory associated with the EU. The General Data Protection Regulation (GDPR) and French data-protection law apply within their scope on the French side. Identify every entity that receives or can remotely access a shared record. If a transfer falls under GDPR Chapter V, determine the applicable conditions before giving the recipient access. For the EU AI Act, Article 2 sets the rules for which operators and uses it covers.

Scope and legal status

Identify the legal recipient behind each trading name. Any transfer safeguard or exception must cover that specific recipient and flow.

Worked example

Have one office log a staged lost passport and the other office search for a match. A reference number and brief item description may be enough for the initial inquiry. Let a designated member of staff verify a claimant’s identity when a match appears.

Implementation guidance

• Map the host, partner offices and remote support teams separately. For each, record what staff can see and who can withdraw access.

• Plant a wrong match in the test. Ask both offices to correct it, then check the record the visitor sees from each side.

Decision and evidence to retain

The French-side service director should retain the access map and the results of the wrong-match test. If the partner can read an entire passport number without needing it, withdraw that access and use the two offices’ existing contact channels. Test the narrower permissions before reopening the shared search.

Sources and attribution

1. European Commission, Europe’s outermost regions
2. European Commission, Sint Maarten’s OCT status
3. European Union, General Data Protection Regulation, Articles 5, 6, 9, 22, 35 and Chapter V
4. European Union, AI Act, consolidated text of 27 July 2026
5. CNIL, how French data protection law applies overseas

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Saint Vincent and the Grenadines

Who may see a student record when a school prepares term reports.

Introduction

In Saint Vincent and the Grenadines, a school principal considering an AI report-writing tool must decide whether an outside provider would receive privileged student information. The tool might only return a paragraph, yet its operator may still see the marks and conduct notes supplied to produce it. The Education Act gives the principal a direct starting point for deciding who may see the record and who can request a correction.

Legal framework

Section 23 of the Education Act, chapter 202, identifies who may inspect or obtain a copy of a student record. Subject to the exceptions it lists, subsection (7) treats the record as privileged for school and Ministry use. Disclosure to another person or institution requires written permission from the parent for a student under 18, or from the student at 18 or older. Under subsection (9), an authorised person may ask the principal to correct inaccurate or incomplete information.

The House of Assembly records the Privacy Act, No. 18 of 2003, which concerns personal information held by public authorities. The University of the West Indies reported in February 2025 that the commencement order had not been issued. CAIA could not verify a later order.

Scope and legal status

Section 23 makes specific provision for sponsors and parents of adult students. Consult the full section for those access rights and the procedure following refusal of a correction.

Worked example

Give the tool invented marks for two students with similar names. Have a teacher trace each sentence in the draft reports to the correct record. If a mark crosses between reports, check whether the school can find and correct each affected copy.

Implementation guidance

• Establish what the outside provider and its support staff can see. Document any required written permission before disclosing identifiable records.

• Require the teacher to check the draft against the official mark and conduct records before filing it. Tell families how to approach the principal about an error.

Decision and evidence to retain

The principal should retain the access decision, the record of any permission required, and the teacher’s correction test. Withhold identifiable records if access by supplier staff remains unexplained.

Sources and attribution

1. Saint Vincent and the Grenadines Ministry of Education, Education Act, chapter 202, section 23

2. House of Assembly, 2003 Acts register, Privacy Act No. 18

3. The University of the West Indies Data Protection Office, scope and commencement of the Privacy Act

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Sint Eustatius

Fair access to a job interview when a model reads work histories.

Introduction

Two applicants may describe the same job differently. A contractor on Sint Eustatius could miss a qualified worker if its shortlisting tool recognises only the title used in its own payroll system. A hiring manager evaluating such a tool should compare the underlying work orders and decide who deserves an interview. That comparison gives the manager a way to examine both data quality and equal treatment in the proposed hiring process.

Legal framework

Sint Eustatius is a public body within the Netherlands. The Wet bescherming persoonsgegevens BES sets duties for data quality and security. Article 34 restricts certain decisions based wholly on automated assessments of aspects of a person’s personality where the decision has legal or similarly serious effects. Exceptions carry conditions, including an explanation of the processing logic when one applies. The Dutch legislative register records 1 January 2026 as the commencement date for the BES equal-treatment measure.

Scope and legal status

Check which equal-treatment grounds apply to the employment decision. Passing an internal comparison cannot establish compliance with the law.

Worked example

Prepare two sample applications showing equivalent work under different job titles. Ask the hiring manager to compare the shortlist with the work orders, inspect omitted qualifications and decide whether the interview invitations should change.

Implementation guidance

• Check what happens to candidates with breaks in their work history.

• Give applicants a contact who can correct the record and reconsider who gets an interview. Keep the manager’s reasons for the final choice.

Decision and evidence to retain

The hiring manager should retain both test applications, the tool’s scores and the final invitations. If the system consistently drops an equivalent qualification, pause automated shortlisting and review candidates previously excluded on that basis.

Sources and attribution

1. Wet bescherming persoonsgegevens BES, including article 34
2. Dutch government legislative register, BES equal-treatment law
3. Kingdom government, constitutional structure

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Sint Maarten

Reviewing a credit decision on the Dutch side of the island.

Introduction

An applicant in Sint Maarten can have regular income that arrives on different dates. If a lender treats a model’s low score as the final answer, a mistaken reading of the bank statements can decide whether the applicant gets a loan. A credit officer and the lender’s compliance lead should establish what the system decides, who can reverse it and how Article 34 applies to that exact process.

Legal framework

Sint Maarten is a constituent country of the Kingdom of the Netherlands. Article 2 of its Landsverordening bescherming persoonsgegevens covers automated processing of personal data, with exclusions. Article 34 restricts decisions that produce legal effects or affect a person to a comparable degree when they rest entirely on automated assessments of aspects of personality. Its contractual and legislative exceptions carry conditions. A controller relying on an exception must communicate the logic behind the processing. Parliament established an internal AI workgroup in 2026.

Scope and legal status

French Saint Martin has a separate legal framework. A lender operating on both sides should trace the route each application takes.

Worked example

Take an application that the score would reject. Give the credit officer the original statements and the applicant’s explanation. Check that changing the decision also changes the outcome delivered to the applicant.

Implementation guidance

• Identify the specific exception and its safeguards if the lender intends to rely on Article 34.

• Let an applicant explain an unusual payment pattern and give the reviewer enough time to assess the evidence.

Decision and evidence to retain

The head of credit should retain the test application and the final outcome displayed in the lending system. If an officer approves a case but the applicant still receives a rejection, pause automated decisions and reopen the affected cases.

Sources and attribution

1. Sint Maarten ordinance, especially articles 2, 4 and 34
2. Kingdom government, constitutional structure
3. Parliament of Sint Maarten, workgroup announcement

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Suriname

Sovereign state. Privacy and accuracy when public services transcribe multilingual calls in Suriname.

Introduction

When a public service centre in Suriname turns a call into a case note, an error in the transcript or translation can change the remedy a person receives. The service director must be able to trace a disputed note to its source and give the caller a way to correct it. Article 17 of the Constitution makes the purpose and handling of the recording a matter for legal review.

Legal framework

Article 17 of the Constitution protects private and family life, the home, honour and reputation. It also protects the confidentiality of correspondence and calls, subject to limits established by law. A public authority considering speech analytics should identify what authorises recording, reuse and disclosure for each purpose.

The National Assembly’s published text of the Wet Bescherming Privacy en Persoonsgegevens is marked ontwerp (draft). UNESCO documented the launch of Suriname’s AI Readiness Assessment under its revised methodology in 2026. Officials can use the assessment to identify policy gaps.

Scope and legal status

CAIA located the parliamentary draft. Check the Staatsblad for an enacted successor and implementing measures applicable to the service.

Worked example

A service centre tests transcription of Dutch and Sranan Tongo calls. A summary changes a caller’s description of a housing problem. The officer lets the caller correct the note before it enters the case record.

Implementation guidance

• Separate permission and purpose for delivering the service, monitoring quality and training a model. Document the lawful basis for each use.

• Ask speakers to evaluate meaning in each language, including mixed-language calls. Route results with uncertain meaning to a qualified listener.

• Limit access to recordings, tell callers how to correct records, and keep evidence that a correction reached the officer handling the case.

Decision and evidence to retain

The service director approves the languages and types of call the tool may handle. Retain a restricted correction log linking each disputed phrase to the officer’s response. If reviewers find that a phrase regularly changes a caller’s meaning, pause automated summaries for that use until local speakers verify the correction.

Sources and attribution

1. Grondwet van de Republiek Suriname, Staatsblad 2025 no. 15, article 17
2. De Nationale Assemblée, draft Wet Bescherming Privacy en Persoonsgegevens
3. UNESCO, Suriname’s AI Readiness Assessment, September 2026

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Trinidad and Tobago

Sovereign state. Overseas transcription of financial instructions given by customers in Trinidad and Tobago.

Introduction

A customer may ask a financial institution in Trinidad and Tobago to cancel a transfer. A transcription service that misses the word “cancel” reverses the instruction. The operations manager needs a way to verify what the customer said before releasing funds. The compliance officer also needs to know where the recording travels and which provisions of the Data Protection Act apply to disclosure abroad.

Legal framework

The Data Protection Act, 2011 commenced in stages. Legal Notice No. 2 of 2012 brought Part I, including section 6 and its General Privacy Principles, and specified portions of Part II into operation. Section 6 addresses accountability, purpose, safeguards and overseas disclosure. Legal Notice No. 220 of 2021 separately brought section 42(a) and (b) into operation. A compliance review should record the proclamation supporting each provision it relies on.

The Central Bank’s Guideline for the Management of Outsourcing Risks addresses third-party services, including cloud computing, for covered financial institutions. The Ministry of Public Administration and Artificial Intelligence has also published work on national AI policy development.

Scope and legal status

CAIA verified the two cited proclamations. Check later Gazette notices before applying any other part of the Act or relying on a statutory enforcement route.

Worked example

A regulated institution wants an overseas transcription service to turn customer calls into searchable notes. Quality checks find that the system reverses the meaning of a caller’s instruction when the audio is poor.

Implementation guidance

• Record where the provider sends recordings, transcripts and backups and how the receiving jurisdiction safeguards them.

• Require a staff member to verify money-movement instructions against the call record. Test Trinidadian and Tobagonian speech samples with permission.

• Classify the outsourcing arrangement, check the applicable supervisory process and test a manual call-handling procedure before launch.

Decision and evidence to retain

The operations manager owns the decision to act on call notes. Keep the original instruction and its verified meaning according to the applicable retention rules. If a transcript changes a payment instruction, disable that use, trace transactions that relied on similar calls and follow the institution’s correction procedure.

Sources and attribution

1. Data Protection Act, 2011, section 6
2. Legal Notice No. 2 of 2012, first proclamation
3. Legal Notice No. 220 of 2021, section 42(a) and (b)
4. Central Bank, Guideline for the Management of Outsourcing Risks
5. Ministry of Public Administration and Artificial Intelligence, AI policy development

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Turks and Caicos Islands

British Overseas Territory. Access to original due-diligence records held by financial businesses in the Turks and Caicos Islands.

Introduction

A trust company in the Turks and Caicos Islands may use software to find documents across its client files. An index is useful only while staff can retrieve the original evidence when the Financial Services Commission examines a file. Managers should establish that they can recover records even if a supplier withdraws its service. Local financial-sector rules set conditions on outsourced access to those records.

Legal framework

Paragraph 9 of Schedule 2 to the Constitution Order protects private and family life and privacy of the home and other property, subject to the qualifications in that provision. For financial businesses, the anti-money-laundering code reproduced with the Proceeds of Crime Ordinance addresses outsourced record keeping. Paragraph 39 leaves responsibility with the financial business and bars arrangements where confidentiality or data protection restrictions are likely to impede access to records.

Financial Services Commission Regulatory Advisory No. 2 of 2021 covers material outsourcing by regulated entities. It addresses access for auditors and regulators, protection of customer information and exit planning.

Scope and legal status

The record-keeping rule and advisory have a financial-sector scope. Check the latest ordinances and sector rules before applying them to other organisations.

Worked example

A trust company buys a tool that uses machine learning to index due-diligence files. In a test, the supplier returns a well-written customer summary but cannot retrieve the original document. The company keeps the source records under its control and changes its acceptance test.

Implementation guidance

• Restore a random sample of original files, including their dates and links to the relevant customers. Record any case where an index or model update breaks retrieval.

• Agree on audit access, subcontractor duties and an exit process. Run a retrieval exercise before deleting records from the previous system.

• Give a compliance officer responsibility for contested matches and a route to correct a customer's record under the rules that apply.

Decision and evidence to retain

The compliance officer signs off on retrieval and exit tests. Keep the list of files requested, the originals recovered and the time taken. If a required document cannot be recovered, halt migration. Keep the old repository accessible and investigate every file affected by the same indexing error before restarting.

Sources and attribution

1. Turks and Caicos Islands Constitution Order 2011, Schedule 2, paragraph 9
2. Proceeds of Crime Ordinance, subsidiary legislation, code paragraph 39
3. Financial Services Commission, Regulatory Advisory No. 2 of 2021 on outsourcing

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

United States Virgin Islands

A territorial agency needs to know exactly which resident’s data a transcription service exposed.

Introduction

A mistaken transcript can be corrected in a resident’s file. A transcript that another resident can read poses a further question for a United States Virgin Islands agency. The case may trigger a duty to notify. The official responsible needs to know what information was available, whether anyone acquired it without authority and who controlled the records when the problem occurred.

Legal framework

Under 3 V.I.C. § 10h, the territorial Bureau of Information Technology establishes and enforces government-wide data security and confidentiality policies. Title 14, sections 2208 and 2209, address agencies and persons or businesses that own, license or maintain certain computerised personal information. The duty to notify depends on the operator’s role, the information and its encryption, and whether an unauthorised person acquired it or is reasonably believed to have done so.

Bill 36-0298 concerns materially deceptive political communications that use AI. The Legislature’s record reviewed for this edition shows introduction without an Act number.

Scope and legal status

Consult the current territorial code and any federal law applicable to the service before giving notice. The cited code is a republication. Confirm enactment in the Legislature’s register before relying on a proposed election measure.

Worked example

Suppose the vendor tells a benefits office that a resident using an ordinary account retrieved somebody else’s call transcript. Stop that retrieval function. Establish which account saw which record, the fields in it and whether the information meets the statutory definition.

Implementation guidance

• Agree who owns or maintains each recording and transcript, and how the vendor will alert the agency to suspected unauthorised acquisition.

• Preserve access logs for the affected accounts and record the system version. Limit the number of people who can view material collected for the investigation.

• Assign an official to determine the notice route. Have a second person verify the repair with test accounts that belong to separate cases.

Decision and evidence to retain

Before release, the service owner should see two staged accounts retrieve only their own transcripts. If either account can retrieve the other record, keep that feature closed. Following an incident, document the scope and notice decision and repeat the same access test against the repaired version.

Sources and attribution

1. US Virgin Islands Bureau of Information Technology, statutory responsibilities
2. Virgin Islands Code, Title 14, chapter 110, subchapter I, sections 2208 and 2209, reproduced by Justia
3. US Virgin Islands Legislature, status of Bill 36-0298
4. United States Code, Title 48, chapter 12

Online edition and citation for this jurisdiction

JURISDICTION GUIDE

Venezuela

Correcting the record behind a driver’s work assignment.

Introduction

A freight operator in Venezuela may consider customer complaints when assigning drivers to routes. A model could treat an unverified allegation as a confirmed safety breach and reduce a driver’s work. The manager responsible for dispatch should know where that allegation came from and who can change its status. A worker needs a way to identify the disputed entry and check that a correction reaches the next round of assignments.

Legal framework

Article 28 of the Constitution gives people access to information about themselves or their property in public or private records, subject to statutory exceptions. It provides a judicial route to update, correct or destroy data that are wrong or unlawfully affect their rights. Article 60 protects privacy, honour, reputation and confidentiality. The science ministry’s 2026 AI ethics code gives guidance on responsible development and use.

Scope and legal status

The constitutional remedy and the ministry’s ethics guidance have different legal force. Check the gazette for the status of proposed AI legislation.

Worked example

Try a dispatch record in which a customer’s allegation was later withdrawn. Check whether the person assigning routes can distinguish the original complaint from a confirmed violation and whether an amendment changes the next assignment.

Implementation guidance

• Give workers a contact who can show them the facts used and receive evidence of an error.

• Limit access to personnel files. Record the reason when an assignment is disputed so the next reviewer can check what changed.

Decision and evidence to retain

The dispatch manager should keep the disputed record, the corrected entry and the next allocation. If a withdrawn complaint still reduces work, stop using that feature and review assignments already made with it.

Sources and attribution

1. Constitution of Venezuela, articles 28 and 60
2. Ministry AI ethics code, reproduced text
3. Baker McKenzie, legal commentary on the code and legislative proposal

Online edition and citation for this jurisdiction