ACCCF / Applied knowledge library

13

VOLUME

Secure decisions before deleting or accusing

Spanish edition · 2026

Suspected Digital Surveillance: A Guide to Checking Indicators and Preserving Evidence with Zero Breach Toolkit

Crisis, false indicators, verified downloads, privacy, report interpretation, and delivery to forensic examiners

Help a concerned person check indicators without destroying evidence or introducing another security risk, with simple steps and a reproducible appendix for whoever reviews the case.

For anyone concerned about their phone or computer and for forensic examiners who receive these cases. No knowledge of intrusion, physical extraction, JTAG, or chip-off is required. The local check is optional; asking for help never depends on completing it.

Editorial coordinator: Jocsan Laguna · American Council on Cybersecurity and Forensic Computing

General technical guide and open educational material. It does not constitute legal advice, an expert opinion, or instructions for accessing systems without authorization. Examples and data are fictitious; figures are editorial reconstructions.

Content

The visible page numbering corresponds to the PDF edition. Word can update this table of contents when the document is opened; headings retain internal navigation.

1. Before touching anything: safety and calm 3
2. Normal Behavior That May Look Like Surveillance 3
   2.1 An Indicator Is Not an Explanation 3
   2.2 False positive does not mean imagination 4
3. What Zero Breach Does and When Not to Use It 5
   3.1 A Local Check of Published Indicators 5
   3.2 When to stop and ask for help 5
4. Package download and verification 6
   4.1 Official repository, not forwarded links 6
   4.2 Verification of the Windows executable 6
   4.3 Alternative: source code and reproducible comparison 7
5. Privacy and Preparation Before Running the Tool 7
   5.1 Local Does Not Mean Harmless 7
   5.2 Preparation of the folder and scope 7
   5.3 Preview and description 8
6. Step-by-Step Execution 8
   6.1 First, practice without examining an actual device 8
   6.2 Next: Authorized Local Review 8
   6.3 If you choose a phone 9
7. How to read the report before sharing it 9
   7.1 Result, grade, scope and gaps 9
   7.2 Codes and operational significance 9
   7.3 ‘Worth a Look’ Is Not a Verdict 10
8. The Four Laboratory Scenarios 10
   8.1 `spyware`: six findings, no hasty conclusions 10
   8.2 `worth-a-look`: Items to Ask About, Not to Accuse 11
   8.3 `clean`: absence of matches with four gaps 11
   8.4 `cellebrite`: forensic access, not spyware 11
9. Safe Delivery to the Forensic Examiner or Response Team 15
   9.1 First the Summary, Then the Complete Case File 15
   9.2 Hash and EML for verifiable delivery 16
   9.3 The Explanation That Prevents a Second Crisis 16
Appendix A. Reproducible Protocol for the Forensic Examiner 17
   A.1 Environment and Provenance Record 17
   A.2 Worksheet for an Authorized Live Run 17
   A.3 Interpretation Matrix 17
Appendix B. Legal Framework, Privacy, and Final Check 18

1. Before touching anything: safety and calm

If you think someone is monitoring your phone or computer, the first step is not to download a program. It is to prevent haste from causing you to lose information or create another problem. Do not delete files, reset the device, install miracle suites, or allow a stranger to control the device remotely. A concern can arise from something legitimate, a setting, or a real incident. We do not know yet, and we do not need to decide this minute.

If there is a physical threat, a risk to minors, active stalking, or someone who may discover that you are seeking help, prioritize safety and your local emergency channels. Do not run a check merely because this guide exists. An analysis can change logs, take up space, or indirectly alert someone who controls the environment. Seek help using a secure device and channel before proceeding.

Make a short list: what you observed, when it started, what changed, what you installed, who had physical access, and which accounts could be compromised. Use approximate times if you do not remember exact ones. Do not capture or forward intimate content to seek help. A message, URL, setting, application name, and date are usually more useful than an entire folder of your private life.

> **What Is Necessary Before What Is Possible**
> Breathe. Do not delete anything, pursue the suspected attacker, or share passwords or codes. If there is danger, seek help now. If there is time, preserve the minimum and check without dramatizing. Duriva will ask you this question several times: what can you prove, and what merely seems possible?

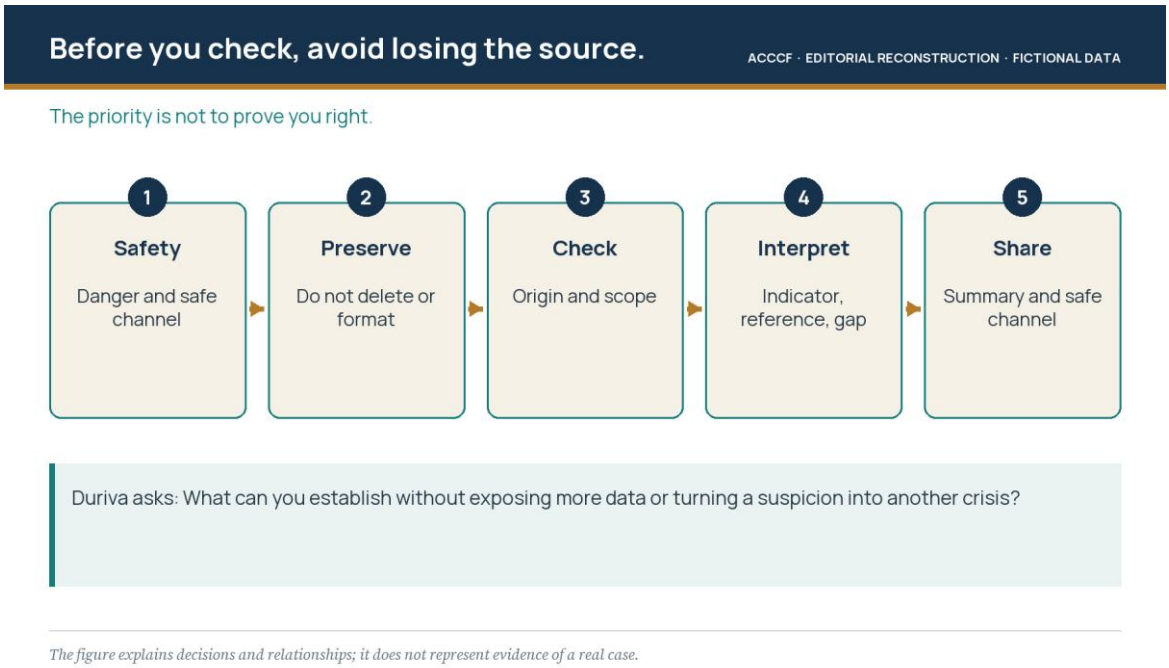


Figure 1. Before checking, avoid losing the source. The priority is not to prove that you were right. Editorial reconstruction; not actual evidence.

2. Normal Behavior That May Look Like Surveillance

2.1 An Indicator Is Not an Explanation

A different MAC address, a disconnection, a rapidly draining battery, an unexpected notification, an unknown application, or a new IP address does not by itself prove that someone is monitoring you. These observations can have causes related to privacy, updates, coverage, synchronization, a legitimate

application, or a shared account. They can also be part of something more serious. The mistake is choosing the most alarming explanation before reviewing the source.

Apple documents that its devices can use different private Wi-Fi addresses for each network and, with Rotating mode on supported systems, change them every two weeks. This feature is intended to reduce tracking, not to demonstrate surveillance. A disconnection is a separate question: it can involve the router, coverage, updates, compatibility, power, software, or enterprise configuration. Do not attribute it to a single cause without review.[1]

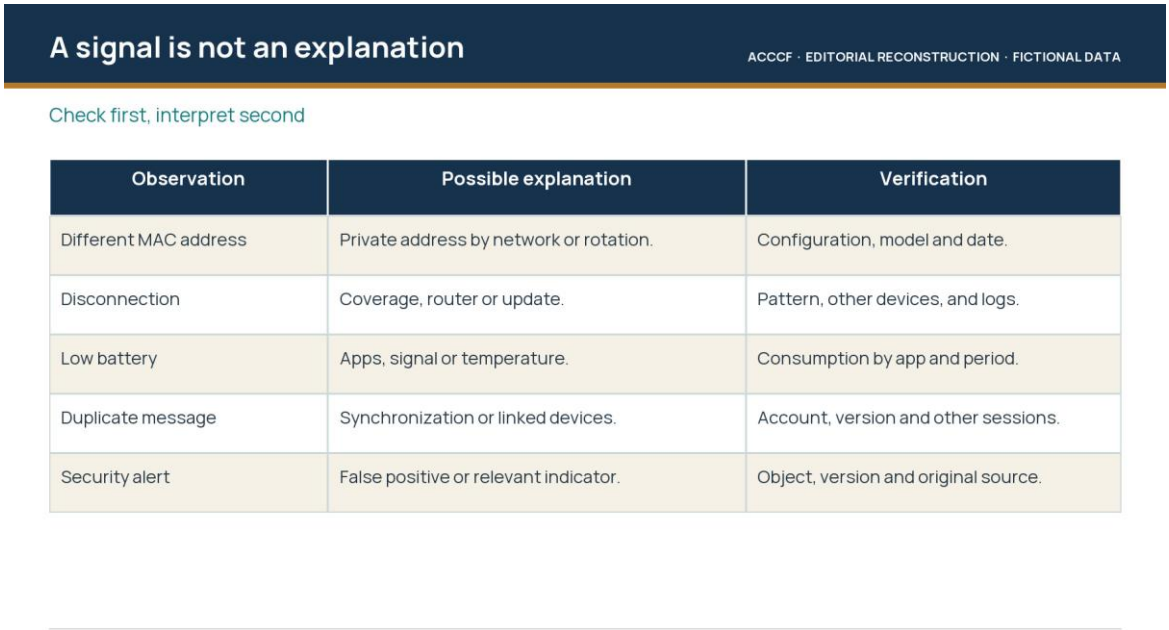
What you see	First Calm Check	What to Keep for Review
The MAC address changed	Check the private address settings for each network and the device model/system.	Screenshot of settings, network, and date; not the entire history.
It disconnects	Note frequency, other devices, coverage, time and recent changes.	Model, system, router, pattern and errors; no Wi-Fi password.
Battery drains quickly	Check consumption by app, signal, temperature and updates.	System statistics and time period; no chat content.
Duplicate message	Check synchronization, other devices, and linked accounts.	Application, version, time, accounts and context message.
Security alert	Read which file or behavior the alert detects and which version of the tool is present.	Complete alert, path, date, and explanation; do not run the file.
Overnight activity	Distinguish updates, backups, tasks, and physical access.	Logs, lock status, and who had the device.

2.2 False positive does not mean imagination

A false positive is an alert that does not represent the feared problem, but not every unusual behavior is a false positive, and neither is every result without findings. The person does not need to be told they are imagining things: they need to know what check would change the interpretation. If a setting explains the data, document it. If it does not, continue investigating without assigning blame or jumping to conclusions.

> **The right phrase**
> 'This may have a normal explanation. I will check it before calling it surveillance.' And also: 'If the explanation does not fit, I will preserve the source so a qualified person can review it.'

[1] Apple Support. Use private Wi-Fi addresses on Apple devices: the private address can vary by network and, with Rotating, every two weeks on supported systems. The feature is intended to reduce tracking; it does not constitute evidence of surveillance or explain every disconnection. Official online source



A signal is not an explanation

ACCCF · EDITORIAL RECONSTRUCTION · FICTIONAL DATA

Check first, interpret second

Observation	Possible explanation	Verification
Different MAC address	Private address by network or rotation.	Configuration, model and date.
Disconnection	Coverage, router or update.	Pattern, other devices, and logs.
Low battery	Apps, signal or temperature.	Consumption by app and period.
Duplicate message	Synchronization or linked devices.	Account, version and other sessions.
Security alert	False positive or relevant indicator.	Object, version and original source.

The figure explains decisions and relationships; it does not represent evidence of a real case.

Figure 2. An indicator is not an explanation. Check first; interpret afterward. Editorial reconstruction; not actual evidence.

3. What Zero Breach Does and When Not to Use It

3.1 A Local Check of Published Indicators

Zero Breach Toolkit is a free, open-source tool that searches for documented indicators of certain spyware on computers, Android collections, and iPhone backups. It can review files, browsers, persistence records, and other supported artifacts. It is not a complete forensic examination, does not detect every form of surveillance, and does not establish that a person is safe merely because it finds nothing.[2][3]

The tool is especially useful when you want an initial local reading of known indicators and an explicit list of what it could not check. Its value is not to say 'no goblins,' but to separate matches, weak references, gaps, and questions for a specialist. New or unknown sources do not magically appear in a database of published indicators, and some traces disappear over time.

3.2 When to stop and ask for help

Do not run a check if it could endanger you, you are not authorized to access the device or files, another person could observe the process, or you cannot protect the report. Also do not use it to examine the device of a partner, employee, client, or family member without permission. Being able to read a file does not make you an authorized owner of its contents.

If there is already a credible security notification, a confirmed extraction, or a targeting concern, seek specialized help without waiting to finish your own review. Journalists, activists, human rights defenders, and civil society can contact the Access Now helpline or Amnesty International Security Lab, whose links appear in the report itself. For anyone else, an incident responder or qualified forensic examiner is the appropriate route.[4]

[2] Zero Breach Toolkit, interplains/Zero-Breach-Toolkit repository. Local checks for published spyware indicators, with code under Apache 2.0 and documentation of scope and limitations. Official online source

[3] Zero Breach Toolkit. Coverage by family of checks and limitations: files, browsers, persistence, records, Android, and iPhone backups. It does not measure detection or false-positive rates. Official online source

[4] Zero Breach Toolkit. Guide to synthetic training scenarios: spyware, worth-a-look, clean, and cellebrite. The indicators are invented, and the examples do not read the device or real lists; they do not support inferences about the state of a real device. Official online source

The situation	What to do first	What to Avoid
Curiosity about strange behavior	Check configuration and timeline before scanning.	Installing many tools at random.
Reasonable suspicion and safe environment	Local check with defined scope and privacy.	Sharing the full report with a group.
Danger or active surveillance	Specialized assistance and secure device/channel.	Run tests that can report the query.
Someone else's device	Express authorization and documented scope.	Reading content merely because it is accessible.
Testing a guide or course	Synthetic built-in scenarios, not real devices.	Presenting training as a real detection.

You don't need to become a hacker.

There is no need to use test points, access the processor, or perform chip-off. If a simple check yields no answer, preserve the evidence and escalate the case. Technical complexity is not a prerequisite for seeking help.

4. Package download and verification

4.1 Official repository, not forwarded links

The source used in this guide is `github.com/interplains/Zero-Breach-Toolkit`. From there, open the Releases section to download the package for Windows, macOS, or Linux, or the source code. Do not download a file with the same name from a video, URL shortener, screenshot, or comment. An identical name does not establish identical content.[5]

The project documentation states that the Windows program is not signed with a code-signing certificate. SmartScreen or an antivirus may therefore display a warning. Do not disable protections or accept the file on blind faith. The project provides build workflow attestation and, for recent executables, signed SHA-256 manifests. Verify before running.[6]

4.2 Verification of the Windows executable

With GitHub CLI installed and the executable downloaded into the current folder, the documentation proposes this provenance check:

Attestation Verification Does Not Establish Absence of Malware

```
gh attestation verify zero-breach-toolkit-windows-x64.exe --repo interplains/Zero-Breach-Toolkit
```

A valid attestation links those bytes to a public build workflow and a commit. It does not establish that the program is free of errors or suitable for your situation. You can also use the signed SHA-256 manifests described by the project. Do not treat a hash found on another page as the hash for your file: calculate your own and compare it with the official source for that version.

[5]Zero Breach Toolkit, interplains/Zero-Breach-Toolkit repository. Local checks for published spyware indicators, with code under Apache 2.0 and documentation of scope and limitations. Official online source

[6]Zero Breach Toolkit. Release verification guide: attestation for programs built by GitHub Actions, SHA-256 manifests, and signing; the Windows package does not have a Windows code signature. Official online source

4.3 Alternative: source code and reproducible comparison

The other route is to clone the repository, review the code, and compare the generated Python file with the expected version. The project describes the deterministic single-file build and the release checks. Nontechnical users do not have to compile: they can ask for help verifying the package or use the menu's practice option. What they must not do is bypass verification of the source's identity because they are in a hurry.

Example of obtaining the official code

```
git clone --depth 1 https://github.com/interplains/Zero-Breach-Toolkit.git
```

> **Duriva asks**
> Where exactly did that executable come from? If you cannot answer with the repository, version, and verification, it is not yet time to run it.

5. Privacy and Preparation Before Running the Tool

5.1 Local Does Not Mean Harmless

Ordinary analysis is designed not to upload your data or visit indicators. List updates do use the network, and Android acquisition downloads a separate collector with consent and changes the phone's state. In addition, internal network blocking is not an operating-system sandbox: network mounts, other applications, and synchronization still exist. If you need strict isolation, decide on it with a specialist.[7]

The report can contain usernames, profiles, paths, history, SMS senders, and message excerpts. The shareable summary contains less information, but it is not a complete forensic examination and must not be published without review. Choose a local, nonsynchronized folder; avoid OneDrive, iCloud, Dropbox, and shared folders; and decide who may open the report. Do not send keys, cookies, passwords, or personal files to the repository.

5.2 Preparation of the folder and scope

Decision	What to Choose	Why?
The output folder	Local, new, nonsynchronized, and access-restricted.	Avoid leaking history and paths.
First execution	Practice scenario or limited scope.	Learn the report format without inventing a real case.
Indicator updates	A separate, deliberate step; do not confuse it with scanning.	The network and the sources are changing.
Open applications	Close browsers and messaging apps if the procedure requires it.	Reduces locked files and concurrent changes.
Permissions	Only those necessary; do not elevate privileges out of habit.	Avoid checking other accounts or changing settings.
Person receiving results	Recipient and secure channel before creating the file.	Avoid impulsive sharing later.

[7] Zero Breach Toolkit. PRIVACY: ordinary analysis performs no uploads by design; updating and Android acquisition are distinct activities. Reports can contain sensitive data, and the shareable summary does not replace the full report. Official online source

5.3 Preview and description

Before analyzing real data, you can request a view of the scope and available checks. `--preview` displays the scope without scanning; `--describe` returns JSON describing the available reads and their limits. These steps help determine whether a check answers the question and whether a less intrusive alternative exists.[8]

Description of scope and readings

```
python -X utf8 scan/zero-breach-toolkit.py --preview
python -X utf8 scan/zero-breach-toolkit.py --describe
```

> **Before Continuing**
> If the scope includes data you do not need to share, reduce the selection. If the concern requires help, do not delay seeking it in order to complete these steps. The tool is an option, not an obligation.

6. Step-by-Step Execution

6.1 First, practice without examining an actual device

The project includes scenarios created for learning: `spyware`, `worth-a-look`, `clean`, and `cellebrite`. They use an invented phone and indicators, with `.invalid` domains that cannot belong to real infrastructure. The report carries a visible training warning, and the temporary directory is deleted on completion. They do not generate a shareable summary or an evidence package because no one should confuse them with a real case.[9]

Four Practice Scenarios

```
python scan/zero-breach-toolkit.py --training spyware
python scan/zero-breach-toolkit.py --training worth-a-look
python scan/zero-breach-toolkit.py --training clean
python scan/zero-breach-toolkit.py --training cellebrite
```

If you use the Windows launcher, look for the practice option in the menu; the documentation identifies it as `Practise`. If you are using source code, run the commands from the repository folder. Do not combine `--training` with files, phones, updates, or real lists: the program rejects this by design. First learn where to find the result, evidence grades, and gaps.

6.2 Next: Authorized Local Review

Once the source is verified, authorization is clear, and the output folder is protected, you can run a review of the chosen scope. Do not use `--quick` if you want to avoid deliberately incomplete coverage. If you choose a specific target, select it deliberately: a targeted review is not equivalent to checking the entire device.

Example Run with Report, JSON, and Minimal Summary

```
python -X utf8 scan/zero-breach-toolkit.py --report reporte.txt --json reporte.json --share-json
resumen.json
```

The text report is for reading, the JSON for reviewing structure, and the summary for an initial conversation with less exposure. None establishes the authenticity of the device or proves that the entire

[8] Zero Breach Toolkit. Result and coverage contract: codes 0, 1, 2, 3, and 4; distinction between findings, references, gaps, exit without scanning, and limited scope. A result without matches is never a guarantee of safety. Official online source

[9] Zero Breach Toolkit. Guide to synthetic training scenarios: spyware, worth-a-look, clean, and cellebrite. The indicators are invented, and the examples do not read the device or real lists; they do not support inferences about the state of a real device. Official online source

system has been examined. Do not combine training with `--share-json` or an evidence package: these are generated only for an authorized real review.

6.3 If you choose a phone

An Android collection and an iPhone backup review are not the same. The tool reads available artifacts and states what it cannot access. An acquisition changes the phone's state and stores private information; do not perform it without explicit consent, a secure destination, and an understanding of the coverage. The local copy may require a separate password or decryption; do not share it or upload it to analysis services.[10][11]

> **There Is No Truth Button**
> If you do not know what scope you have just selected, stop. The answer is not to click 'full,' but to know what was checked and what could not be checked.

7. How to read the report before sharing it

7.1 Result, grade, scope and gaps

Read four things before any figure: what the result states, what grade of evidence it has, what scope was reviewed, and what was left out. The same number can mean different things depending on the source. Six findings are not six infections, zero findings does not establish an absence of surveillance, and a reference is not a malicious file running.

Element	What It Tells You	Error It Prevents
Result and code	What happened during the selected run.	Turning it into an absolute label.
Degree of evidence	Whether it is a file, record, reference, log, or infrastructure.	Treating everything as proof of execution.
Scope	What phone, files, accounts and options it includes.	Generalizing to the entire device.
Gaps	What the tool could not read or check, and why.	Calling unreviewed items clean.
Indicators and dates	What sources were used and if they are up to date.	Confusing a recent copy with a current indicator.
Next step	Preserve, close gaps, or seek help, as appropriate.	Deleting or 'cleaning' reflexively.

7.2 Codes and operational significance

Code / situation	Correct Interpretation	Next decision
0: no actionable findings or gaps	No actionable matches were found within that scope.	Do not call it a safe device; review the scope and reason for concern.
1: error	The run or output failed.	Correct the input or destination; do not interpret this as absence.

[10] Zero Breach Toolkit. Coverage by family of checks and limitations: files, browsers, persistence, records, Android, and iPhone backups. It does not measure detection or false-positive rates. Official online source

[11] Zero Breach Toolkit. PRIVACY: ordinary analysis performs no uploads by design; updating and Android acquisition are distinct activities. Reports can contain sensitive data, and the shareable summary does not replace the full report. Official online source

Code / situation	Correct Interpretation	Next decision
2: actionable matches	There are indicators that require interpretation and preservation.	Do not delete, run, or pursue anything; seek help.
3: missing data or sources	There are gaps; it's not a clean result.	Complete coverage and check again.
4: exit without scanning	There was no review or verdict.	Do not claim that there is no spyware.
Withdrawn references or indicators	The origin of the indicator changes its current meaning.	Review context and source; do not force an accusation.

Sources of the table:[12]

7.3 'Worth a Look' Is Not a Verdict

An application installed outside the store, accessibility access, an old version, or a disabled verification setting may warrant a question. It is not a finding on its own. Accessibility tools, screen readers, password managers, and automation applications can be legitimate. The person familiar with the device can confirm or rule out those explanations with additional information.

> **Duriva breaks the fourth wall**
> If you read only 'there are six matches,' it looks like a verdict. If you also read 'there are four checks not run,' you understand that the case remains open. That is the difference between reacting and reviewing.

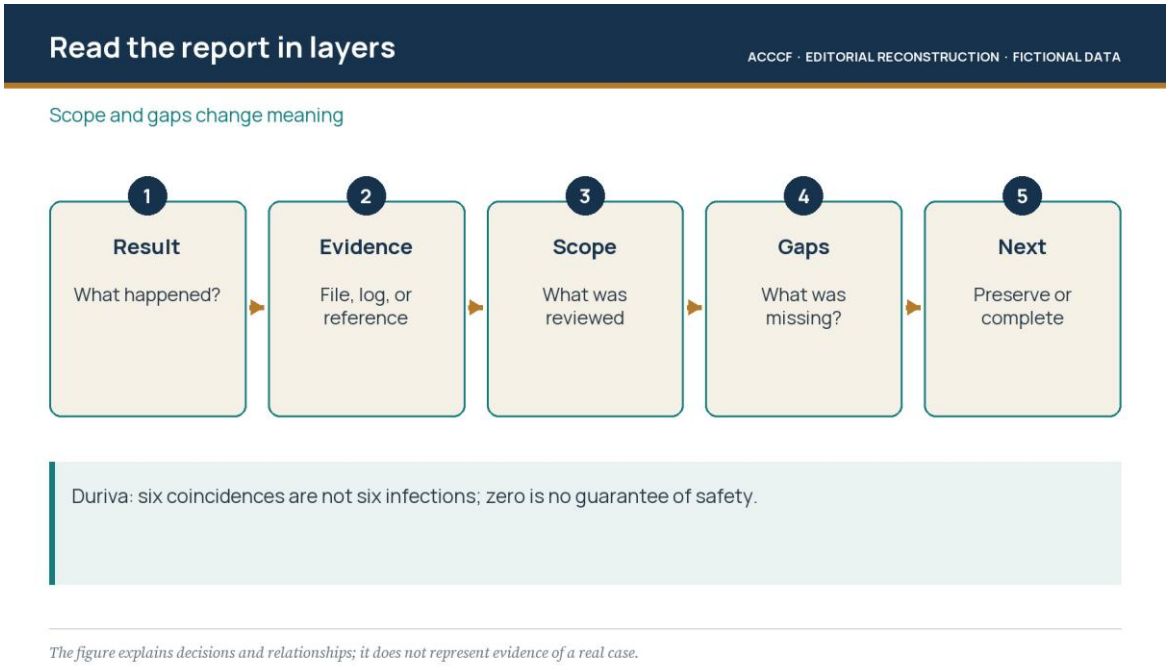


Figure 3. Read the report in layers. Scope and gaps change the meaning. Editorial reconstruction; not actual evidence.

8. The Four Laboratory Scenarios

8.1 `spyware`: six findings, no hasty conclusions

The synthetic `spyware` scenario produced six matches: five pieces of evidence on the device and one in the registry. It includes an application, a file fingerprint, a certificate, a property, a path, and an invented

[12]Zero Breach Toolkit. Result and coverage contract: codes 0, 1, 2, 3, and 4; distinction between findings, references, gaps, exit without scanning, and limited scope. A result without matches is never a guarantee of safety. Official online source

infrastructure reference. It also left four gaps: no file fingerprints, no battery history, no crash report, and no SMS backup. The result was `INDICATORS_FOUND`, code 2, and `scan_state: partial`.[13]

The lesson is not 'you have spyware,' but how different items are grouped and why each requires interpretation. The output itself emphasizes that a match calls for investigation, not a declaration of compromise or a cleanup. The presence of a file or setting does not by itself prove execution, and an infrastructure reference does not establish successful contact. The entire phone and all indicators are fictitious.

8.2 `worth-a-look`: Items to Ask About, Not to Accuse

The `worth-a-look` scenario found no known indicators but displayed four items to ask about: a directly installed application with accessibility access, old updates, an enabled accessibility service, and disabled application verification. The result was `NO_KNOWN_INDICATORS_WITH_GAPS`, code 3, with the same four coverage gaps.[14]

These items do not prove infection or falsehood. They are an invitation to ask: Do you recognize the application? Why did you install it? Were you expecting that permission? Are updates pending? What changed before the behavior? The manual does not claim that the owner is wrong or that everything is normal. Learning to ask before accusing is the objective.

8.3 `clean`: absence of matches with four gaps

The `clean` scenario produced no known matches but retained four gaps and code 3. The output expressly states that it is not a certificate of good health. It teaches that 'nothing found' can refer only to what was reviewed and the known indicators. It does not prove the absence of new, hidden, targeted, or undocumented spyware, or that every location was examined.[15]

If a person has a concrete reason for concern, the result does not eliminate that concern. The next step may be to complete coverage, review logs, consult a specialist, or simply document that the first check provided no actionable indicators. There is no need to force a false positive for the person to feel understood.

8.4 `cellebrite`: forensic access, not spyware

The `cellebrite` scenario produced one match in the USB registry and code 2. Its purpose is to show how the tool recognizes an indicator of forensic access and how the recommendations change: preserve, review applications from around that time, and change passwords from another device if the context justifies it. The registry entry and serial number are invented; no real person or device is involved.[16]

This case is not spyware, nor does it alone establish a complete extraction. The forensic questions are who had access to the phone, for how long, with what authorization, and what happened before and afterward. The conclusion must distinguish a connection indicator from the meaning that the context can support.

[13]ACCCF local laboratory. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, execution of the four synthetic scenarios. The spyware, worth-a-look, clean, and cellebrite files are in TXT/JSON. No personal information or real devices were examined.

[14]ACCCF local laboratory. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, execution of the four synthetic scenarios. The spyware, worth-a-look, clean, and cellebrite files are in TXT/JSON. No personal information or real devices were examined.

[15]ACCCF local laboratory. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, execution of the four synthetic scenarios. The spyware, worth-a-look, clean, and cellebrite files are in TXT/JSON. No personal information or real devices were examined.

[16]ACCCF local laboratory. Zero Breach Toolkit 2.0.6, commit 10ceaba497e40da1f327916a0a3fe0af0ff5994f, execution of the four synthetic scenarios. The spyware, worth-a-look, clean, and cellebrite files are in TXT/JSON. No personal information or real devices were examined.

Four different lessons

Matches do not equal infection; items to review do not equal a false positive; zero matches does not equal safety; and a forensic lead does not equal proof of complete extraction. The report is the beginning of a review, not a verdict.

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · spyware

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: spyware. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:33   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: SERIOUS FINDING - seek expert help promptly.

  WHAT WAS FOUND
    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       org.example.training.spyapp  [artifact]
          Where: app org.example.training.spyapp

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       e36c3fee5d43ffb61b91fbee792cd8b7b4ebd9076f77e9002a9eaa0ea5648a84  [sample]
          The file fingerprint of a published spyware sample (its family
          is named where the source gives one). A match here is
          conclusive, not circumstantial.
          Where: app org.example.training.spyapp (/data/app/training-spyapp/base.apk)

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       d472b7c9d957a9e55ce56bd80388b97be9e2132644c0a51cac03aa618905e6d2  [artifact]
          Where: app org.example.training.spyapp

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       persist.training.spy.flag  [artifact]
          Where: system property persist.training.spy.flag

    >> SOMETHING THE RESEARCHERS TIE TO SPYWARE IS ON THIS PHONE
       /data/local/tmp/training-spy-daemon  [artifact]
          Where: /data/local/tmp/training-spy-daemon

    >> THE PHONE'S SYSTEM LOGS NAME THIS SPYWARE INFRASTRUCTURE
       training-spyware-server[.]invalid  [infrastructure]
          A server the cited researchers attribute to the named spyware
          family. Its exact role - delivering an exploit, controlling an
          implant or receiving stolen data - is not stated in the source,
          so treat contact as serious but unspecified. A domain can change
          hands after a campaign ends: compare the date of the evidence
          with the date of the research.
          the phone's own system logs name it - it may have been a
          connection, a lookup, or only text an app wrote to the log
          Where: phone log dumpsys.txt, line 1

  WHAT TO DO
    Seek expert help promptly. Preserve this report and the named
    files or registrations. Do NOT delete, move, run or try to clean
    them. A file match establishes presence; a registration
    establishes configuration. Neither alone establishes that spyware
    executed.

    Contact a qualified incident responder or your organisation's
    security team. You do not need to finish investigating first.
    Support options are at the end of this report.
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

Figure 4. Actual training report for the spyware scenario. Verbatim excerpt; all data are synthetic. Editorial reconstruction; not actual evidence.

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · worth-a-look

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: worth-a-look. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:33   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: no known indicator was found in anything that could be
          checked.

  This is NOT a clean bill of health. See the two sections below for
  what was searched and, more importantly, what could not be.

  ALSO: 4 items under "WORTH A LOOK" further down. They are NOT
  a finding; each comes with its usual, ordinary explanation.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
========================================================================

Indicator set : 6 indicators, unknown age
  ** WARNING: one or more source dates are unknown; copying files does not refresh indicators. **

DETAIL  —  what was examined, and the evidence behind the summary

--- android-intrusion check  [NOT_APPLICABLE] ---
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

Figure 5. Actual training report for the worth-a-look scenario. Verbatim excerpt; all data are synthetic. Editorial reconstruction; not actual evidence.

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · clean

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: clean. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:34   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: no known indicator was found in anything that could be
          checked.

  This is NOT a clean bill of health. See the two sections below for
  what was searched and, more importantly, what could not be.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
========================================================================
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

Figure 6. Actual training report for the clean scenario. Verbatim excerpt; all data are synthetic. Editorial reconstruction; not actual evidence.

ESCENARIO SINTÉTICO · ZERO BREACH TOOLKIT 2.0.6 · cellebrite

```
########################################################################
  TRAINING EXAMPLE - NOT A REAL CHECK
  Scenario: cellebrite. This is a made-up phone checked against made-up
  indicators. It says nothing about this computer or any real device.
########################################################################
========================================================================
  Zero Breach Toolkit 2.0.6 - spyware indicator check
  Scope: default (phone evidence only)
  Checks for TRACES of known mercenary spyware. A clean result is NOT a
  clean bill of health - see what could not be checked, below.
  2026-11-10T18:37:34   Windows 11
========================================================================

========================================================================
  SUMMARY  —  read this part
  TRAINING EXAMPLE: a made-up phone and made-up indicators, not a real check.
========================================================================
  RESULT: SERIOUS FINDING - seek expert help promptly.

  WHAT WAS FOUND
    >> SIGNS THIS PHONE WAS UNLOCKED WITH A PHONE-FORENSICS TOOL (CELLEBRITE)
       cellebrite usb 04f2:b071  [forensic]
          A trace of Cellebrite, the phone-forensics tool police and
          security services use to unlock seized phones and copy their
          contents. It is not spyware: it shows the phone was unlocked, or
          an unlock was attempted, while it was out of its owner's hands.
          the phone's own system logs name it - it may have been a
          connection, a lookup, or only text an app wrote to the log
          Where: phone log logcat.txt, line 2

  WHAT TO DO
    Someone unlocked this phone, or tried to, with Cellebrite: the
    phone-forensics tool police and security services use to copy
    everything on a seized phone. Assume what was on the phone then -
    messages, photos, contacts, saved passwords and the accounts
    signed in - was copied. Change the passwords of important accounts
    from another device, sign out other sessions, and tell the people
    whose conversations were on it. In documented cases spyware was
    installed after such an unlock, so check the apps installed around
    that time and get expert help.

    Seek expert help promptly. Preserve this report and the named
    files or registrations. Do NOT delete, move, run or try to clean
    them. A file match establishes presence; a registration
    establishes configuration. Neither alone establishes that spyware
    executed.

    Contact a qualified incident responder or your organisation's
    security team. You do not need to finish investigating first.
    Support options are at the end of this report.

    Do NOT open, visit or look up indicator addresses. Keep the [.]
    spelling when sharing them.

  WHAT COULD NOT BE CHECKED  (4 gaps, grouped)
    - android/android:file-hashes: the collection has no file
      fingerprints (AndroidQF's "hash files" option was off), so files
      were checked by path and name only
    - android/android:history: no battery history in the collection
    - android/android:crashes: bug report missing or unreadable; crash
      records were not checked
    - android/android:messages: no SMS backup in the collection, so
      links in messages were not checked
    (The full report lists them again at its end.)

  Before you share this report: it can contain your Windows username,
  browser profile names, file paths and browsing details, SMS senders
  and message excerpts. --share-json writes a minimal summary without
  artifact text. Ask a responder how to share evidence securely; do
  not post the full report publicly.
```

Fragmento literal del reporte real de entrenamiento. No representa un dispositivo real.

Figure 7. Actual training report for the cellebrite scenario. Verbatim excerpt; all data are synthetic. Editorial reconstruction; not actual evidence.

9. Safe Delivery to the Forensic Examiner or Response Team

9.1 First the Summary, Then the Complete Case File

Before sending everything, ask the person receiving the case what they need and through which channel. An initial conversation can be limited to the reason for concern, device, scope, date, result, and gaps. The minimal summary helps determine whether the full report is needed and avoids transmitting history or messages that do not contribute to the question.

When the full report is needed, deliver it through a secure channel, not as a public file. Separate the working version from the shareable version. The recipient may need original items, but this must be

agreed expressly. Do not upload Android collections, iOS backups, or reports to unknown services, chat groups, or generic analysis sites.[17]

9.2 Hash and EML for verifiable delivery

If the report is sent by email, preserve the complete EML with its body, headers, and attachments. The body can include the algorithm and hash for each file. The recipient calculates their own values and compares them. A match establishes equality with the file declared in that delivery, not the authenticity of the device or the truth of the findings. A hash calculated afterward establishes integrity only from that moment onward.

Email encryption, signatures, and hashes solve different problems. Encryption limits who can read the message; a signature helps verify origin and detect alteration; a hash compares items. None establishes that the person who wrote the message is who they claim to be or that the content is true. Do not send the private key or file password in the same message. Use a separate, agreed channel.

Item	What is recorded	What It Does Not Establish
Delivery EML	Body, headers, attachments, and receipt.	That the human sender wrote the contents.
TXT / JSON report	Name, size, hash, date and version.	That the scope was complete or the device authentic.
Summary to share	Result, scope, gaps and next step.	A complete forensic examination or an absence of risk.
Key or password	Separate channel and confirmed recipient.	That delivery was authorized by any recipient.
Original collection	Authorization, coverage, chain of custody, and hash for each item.	That any tool can read all the artifacts.

9.3 The Explanation That Prevents a Second Crisis

Brief Text for Submitting the Case

```
Reason for concern: [behavior observed and date]
Device and authorization: [type, owner, and permission]
Tool and version: [origin and verification]
Scope: [what was reviewed and what was not]
Result: [matches, references, and gaps]
Actions already carried out: [without deleting or cleaning]
Items delivered: [summary / report / originals]
Hash of each file: [algorithm and value]
What I need: [scope review, interpretation and next step]
Data I did not include: [keys, passwords, or intimate or irrelevant content]
```

> **It's not about winning an argument.**
> The forensic examiner does not need the person to prove they were right. They need a source, a timeline, and an explanation of what was done. Well-preserved uncertainty is more useful than fabricated certainty.

[17] Zero Breach Toolkit. PRIVACY: ordinary analysis performs no uploads by design; updating and Android acquisition are distinct activities. Reports can contain sensitive data, and the shareable summary does not replace the full report. Official online source

Appendix A. Reproducible Protocol for the Forensic Examiner

A.1 Environment and Provenance Record

Record used to produce examples of this guide

```
Repository: https://github.com/interplains/Zero-Breach-Toolkit
Commit: 10ceaba497e40da1f327916a0a3fe0af0ff5994f
Version shown: Zero Breach Toolkit 2.0.6
JSON schema: 1.6
File: scan/zero-breach-toolkit.py
SHA-256: 4f7294b0d72ae901552e3ac44f64148c0059d43d587a1638654ab00e7c80e627
Scenarios: spyware, worth-a-look, clean, and cellebrite
Type of data: completely synthetic
Personal information: not examined
Real devices: not used
```

This record describes a repository clone and training runs; it is not an attestation of the Windows executable or a verification of the latest version. The downloaded executable must be checked against its own version and build workflow. All four scenarios were run and produced TXT and JSON, as well as JSON output from `--describe`.

A.2 Worksheet for an Authorized Live Run

Forensic Examination Record Template

```
Case and authorization: [identifier, owner, scope, and exclusions]
Reason for the check: [behavior and question]
Device and initial state: [model, system, date, time zone]
Package: [repository, version, file and verification]
Hashes of the package and indicators: [values and date]
Environment: [analysis system, isolation, and synchronization]
Scope: [default / full / targeted / browser / phone]
Command and parameters: [no secrets]
Start and end times with time zone: [literal values]
Outputs: [TXT, JSON, summary, manifest and hashes]
Result and code: [literal]
Findings: [degree, object, source and context]
Gaps: [checks not run and reasons]
Issues: [errors, limitations, and unavailable files]
Preservation and custody: [location, access, and transfers]
Review: [person, date and subsequent verification]
```

A.3 Interpretation Matrix

Question	Source That Answers It	What Cannot Be Claimed
What did it find?	Hits, grade, and item.	Automatic infection or identity of the attacker.
What could it not review?	Coverage.not_checked and scan_state.	That omitted locations are clean.
What sources did it use?	Indicators, versions and dates.	That a recent copy constitutes current evidence.
What can be normal?	Settings, applications, and the device owner's context.	False positive without corroboration.
What is missing for attribution?	Authorization, sessions, device, and timeline.	A natural person from an IP address, app, or MAC address.
What is being shared?	Summary or full report as required.	That publishing the report is harmless.

Acceptance Criterion

The report must allow another person to reproduce the scope, locate each finding, understand each gap, and know what remains unproven. If it contains only a 'clean' or 'infected' label, the review is not yet complete.

Appendix B. Legal Framework, Privacy, and Final Check

A security check also involves personal data. In Mexico, the current LFPDPPP's principles of purpose limitation, proportionality, security, and confidentiality, as well as its breach provisions, apply. Peru, Chile, Argentina, Colombia, Ecuador, and Spain/EU contain equivalent but non-identical provisions on minimization, security, rights, and providers. In Chile, the modernization under Law 21.719 has a deferred effective date of 1 December 2026 and must not be treated as a fully effective regime before then. There is no universal authorization to read someone else's device.[18][19][20][21][22][23][24]

Check before closing	Required response
Was the person safe and authorized?	No tests were conducted out of curiosity or without permission.
Was the package verified?	Repository, version and provenance documented.
Was the output protected?	Local folder, access and sync controlled.
Were findings, references, and gaps distinguished?	Neither infection nor safety was asserted on the basis of a label.
Were normal explanations considered without ruling out something serious?	Configuration and context were checked.
Was the report shared with data minimization?	Summary first; complete case file through a secure channel.
Can the forensic examiner reproduce the review?	Version, scope, commands, hashes, gaps, and custody are included.

Conclusion

The useful question is not 'Am I paranoid?' but 'What can I check without causing myself more harm?' The answer may be a setting, a match, a gap, or a professional review. All are more useful than an accusation without a source.

[18] Mexico. Federal Law on the Protection of Personal Data Held by Private Parties, text published on 20-03-2025 and amended on 14-11-2025. Articles 5–9, 18–20, and 31: principles, security, confidentiality, breaches, and handling of rights requests. The current federal authority is the Secretariat of Anti-Corruption and Good Governance. Official online source

[19] Peru. Law 29733 and its Regulation approved by DS 016-2024-JUS. Principles of purpose limitation, proportionality, security, and confidentiality; the new Regulation develops provisions on incidents, preventive assessment, and the progressive duties of the data protection officer. Official online source

[20] Chile. Law 21.719, amending Law 19.628 on the protection of personal data. The version containing the new regime has its entry into force deferred until 01-12-2026; before that date, review the law then applicable and do not present future obligations as currently in force. Official online source

[21] Argentina. Law 25.326, updated text. Articles 4–6, 9–10, 14–16, and 25: quality, information, security, confidentiality, data subjects' rights, and provision of processing services on behalf of third parties. Official online source

[22] Colombia. Statutory Law 1581 of 2012, articles 4, 8, 12, 17–18, and 26: principles, rights, information, duties of data controllers and processors, and transfers to third countries. Official online source

[23] Ecuador. Organic Law on the Protection of Personal Data, Official Register Supplement 459 of 26-05-2021. Articles 10, 37–44: principles, security measures, data protection by design, risks, and incident handling. Official online source

[24] European Union. Regulation (EU) 2016/679, articles 5, 25, 28, and 32–34: principles, data protection by design, processors, security, and notification/communication of security breaches. Spain also requires review of applicable national and sectoral legislation. Official online source