UNIT 10 · SESSION 11

Ethics and Data Privacy

Last Saturday you learned how people steal your data. Today: what the law says anybody is allowed to do with it in the first place.

2ND SEMESTER · SCHOOL YEAR 2026-2027

Introduction to Computing · Prof. Ryan V. Labrador

Saturday, 24 October 2026 · 2-hour lecture

TODAY

Two hours, four parts

Part 1	**Ethics and citizenship**	Why a technical course has an ethics unit at all
Part 2	**RA 10173**	The Data Privacy Act of 2012, in real depth. The centre of today.
Part 3	**Owning ideas**	Copyright, plagiarism, and licences that let people share
Part 4	**AI ethics**	Bias, hallucination, attribution, disclosure
After	**Laboratory**	A data privacy case clinic — and you audit your own site

Part 2 is the examinable heart of the unit and it takes half the session. Do not let Part 1 run long.

LEARNING OBJECTIVES

By the end of today you will be able to…

1. Explain why something can be perfectly legal and still be wrong.
2. Name the core principles of the ACM Code of Ethics and apply one to a real case.
3. Tell personal information from sensitive personal information, with examples.
4. List the eight rights of a data subject under RA 10173 and say what each one lets you do.
5. Describe what the National Privacy Commission is and what it can do.
6. State when a personal data breach must be reported, to whom, and how quickly.
7. Explain copyright, fair use and what an open licence actually grants you.
8. Describe three ways an AI system can cause harm, and what disclosure is for.

Legal is not the same as right

The law tells you

- The minimum you must do.
- What somebody can prosecute you for.
- Rules written after the harm was already done.
- The same standard for everyone, enforced unevenly.
- Nothing at all about situations it never imagined.

Ethics tells you

- What you should do when nobody is checking.
- How to act where no rule exists yet.
- Who gets hurt by a decision that is technically fine.
- Whether you would be comfortable explaining it publicly.
- What kind of professional you are becoming.

The law is the floor, not the ceiling. Every serious scandal in technology was legal on the day it started.

The ACM Code of Ethics — the general principles

Contribute to society

Computing professionals should aim at human well-being — and consider everyone affected, not only the client who paid.

Avoid harm

Harm means injury or negative consequences: lost data, lost privacy, lost livelihood. Foreseeable harm has to be weighed, not shrugged at.

Be honest and trustworthy

Do not misrepresent what a system does, what it costs, or what its limitations are. Include the limitations.

Be fair, do not discriminate

Systems can discriminate without anybody intending it. Fairness is something you have to test for, not assume.

Respect others' work

Credit ideas, honour licences, do not pass off somebody else's code, design or writing as your own.

Respect privacy, honour confidentiality

Collect only what you need. Use it only for what you said. Keep what you were told in confidence.

EVERY DAY

Digital citizenship, in practice

Before you post	**Would you sign it?**	Anonymity online is thinner than people think, and screenshots outlive accounts.
Before you share	**Is it true?**	Forwarding something false makes you part of how it spread. 'I just shared it' is not a defence.
Before you upload	**Is it yours to upload?**	Other people are in your photos. Their consent is not implied by them standing near you.
Before you install	**What did you just agree to?**	Permissions are a contract. Contacts, location, camera, files — read what you granted.
Before you speak	**Would you say it to their face?**	Distance makes cruelty easy. That is a fact about people, not about the internet.

Your digital footprint is a CV you did not mean to write. Employers here read it. So do scholarship panels.

PART 2

RA 10173

The Data Privacy Act of 2012. This is the law that decides what anybody in this country may do with information about you.

What RA 10173 is, and who it covers

The name	**Data Privacy Act of 2012**	Republic Act No. 10173. Its Implementing Rules and Regulations followed in 2016 and carry much of the operational detail.
The purpose	**Protect the individual**	It protects the fundamental right to privacy while allowing the free flow of information needed for growth. Both halves are in the policy.
Who it binds	**Anyone processing personal data**	Government and private sector alike. A barangay, a school, a hospital, a lending app, a sari-sari store keeping a ledger of names.
Reach	**Beyond our borders**	It can reach processing done outside the Philippines where there is a link to Philippine residents or to an entity here.
What it created	**A regulator**	The National Privacy Commission, an independent body with investigation and enforcement powers.

There is no size exemption. A two-person business collecting customer names is a personal information controller.

THREE ROLES

Learn these three words first

Data subject

The living person the information is about. You. Rights belong here, and only here.

Personal information controller

The organisation that decides WHAT is collected and WHY. It carries the legal duties. Usually shortened to PIC.

Personal information processor

A party that processes data on the controller's instructions — a cloud host, a payroll service. Shortened to PIP.

IN THIS SCENARIO	DATA SUBJECT	CONTROLLER	PROCESSOR
CIC keeps your grades	You	The college	Its student records system vendor
You order online	You	The online shop	The courier and the payment gateway

THE CENTRAL DISTINCTION

Personal versus sensitive personal information

Personal information

- Information from which your identity is apparent,
- or can reasonably and directly be worked out,
- or which combined with other data identifies you.
- Name. Address. Mobile number. Email. Photograph.
- Processing needs a lawful basis — Section 12.

Sensitive personal information

- A defined list in Section 3, not a matter of opinion.
- Health, religion, ethnicity, sexual life, offences.
- Government-issued numbers and records.
- Processing is PROHIBITED unless a narrow exception
- in Section 13 applies. Higher penalties apply too.

Both are protected. Sensitive personal information is protected harder, and mishandling it is punished harder.

What falls in each set

PERSONAL INFORMATION

identity is apparent, or can reasonably and directly be worked out

- Full name
- Home address
- Mobile number
- Email address
- Photograph
- Date of birth
- Student number
- Employer and job title

Processing needs a lawful basis — Section 12

SENSITIVE PERSONAL INFORMATION

a defined list in Section 3 — not a matter of opinion

- Health and medical records
- Religion or belief
- Race or ethnic origin
- Marital status and age
- Education records
- Sexual life
- Offences and court records
- SSS, PhilHealth, TIN, licences

PROHIBITED unless a Section 13 exception applies

Both sets are protected. The right-hand set is protected harder — and mishandling it is punished harder.

Point at any field on a real enrolment form and ask which set it lands in. That is the whole skill.

SECTION 3

What actually counts as sensitive

CATEGORY	INCLUDES	EVERYDAY EXAMPLE
About the person	Race, ethnic origin, marital status, age, colour, religious, philosophical or political affiliation	A membership list showing religion
Health and life	Health, education, genetic or sexual life	A clinic logbook. A medical certificate.
Offences	Any proceeding for an offence, its disposal, or the sentence of a court	A barangay blotter entry
Government-issued	Numbers and records peculiar to an individual — social security numbers, health records, licences and their denial or revocation, tax returns	SSS, PhilHealth, TIN, driver's licence
Classified	Anything an executive order or an act of Congress establishes as classified	Set by law, not by the organisation

SECTION 11

Three principles that govern everything

Transparency

The data subject must know that processing is happening, why, by whom, for how long, and how to reach the people responsible. Surprise is a failure.

Legitimate purpose

The purpose must be declared, specified, and not contrary to law, morals or public policy. 'Because it might be useful later' is not a purpose.

Proportionality

Processing must be adequate, relevant, suitable, necessary and not excessive. If the purpose can be achieved with less data, collect less.

Ask three questions of any form you are ever asked to design: do they know, did we say why, and do we really need this field?

SECTIONS 12 AND 13

Consent is only one lawful basis

Personal information — Sec 12

- Consent of the data subject; or
- necessary for a contract with the data subject; or
- necessary for a legal obligation, or to protect life and health; or
- necessary for a public authority's function, or a national emergency; or
- the controller's legitimate interests — unless your rights override them.

Sensitive information — Sec 13

- Prohibited, except in the cases the Act lists, including:
- consent, given specifically and before processing; or
- an existing law or regulation that guarantees protection; or
- to protect life and health where consent cannot be given; or
- medical treatment under confidentiality; or the defence of legal claims.

Consent must be freely given, specific, informed — and it can be withdrawn. A tick-box nobody could refuse is not consent.

The eight rights of a data subject

To be informed

You must be told that your data is being collected and processed, and why — before it happens, or as soon as practicable.

To object

You may refuse processing, including for direct marketing, profiling and automated decisions. Refusal must be possible in practice, not in theory.

To access

You may demand a copy of what they hold about you, where it came from, who received it, and how it was used.

To rectification

If it is wrong, you can require it corrected — and require the correction to be passed on to anyone who already received the bad data.

These are yours by law. You do not have to be polite about them and you do not have to explain why you are asking.

And the four that give the first four teeth

To erasure or blocking

You may require data to be suspended, withdrawn, blocked, removed or destroyed where it is incomplete, outdated, unlawfully obtained or no longer necessary.

To damages

You may be indemnified for damage sustained because of inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorised use of your data.

To file a complaint

You may complain to the National Privacy Commission. It is free, and you do not need a lawyer to start.

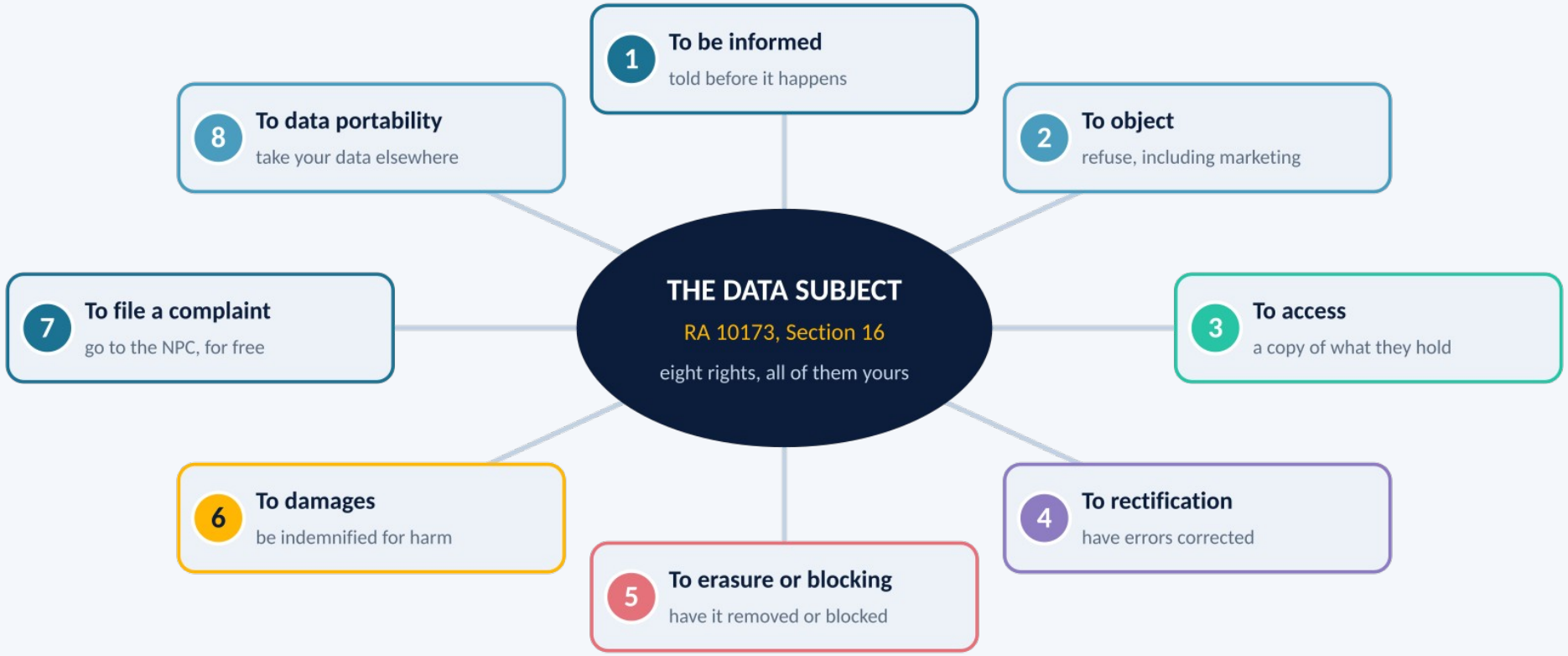
To data portability

Where your data is processed electronically and in a structured format, you may obtain a copy in a form that lets you move it elsewhere.

Rights 6 and 7 are why the other six are not merely advice. There is somewhere to go and something to recover.

ALL EIGHT AT ONCE

The wheel of data subject rights



Rights 6 and 7 are what stop the other six from being merely advice: something to recover, and somewhere to go.

Cover the wheel. Name all eight. Then uncover it and see which one you forgot — it is usually number eight.

THE REGULATOR

The National Privacy Commission

What it is	**An independent body**	Created by RA 10173 to administer and implement the Act. It sits under the DICT for budget purposes but decides its own cases.
Rule-making	**It writes the detail**	Its circulars and advisories fill in what the statute leaves open — breach management, registration, the role of a Data Protection Officer.
Complaints	**It hears you**	It receives and investigates complaints from data subjects, and it can act on its own initiative.
Enforcement	**It has powers**	Compliance orders, cease-and-desist orders, and the ability to recommend prosecution to the Department of Justice.
Guidance	**It publishes**	Advisories, templates and public education material. Read them before you design anything that collects data.

The NPC does not prosecute. It investigates, orders, and refers. The criminal case is filed by the Department of Justice.

What the law requires you to actually do

Section 20	**Secure it**	Reasonable and appropriate organisational, physical and technical measures. Locked drawers count. So do access controls, and so does training.
Section 21	**Be accountable**	The controller stays responsible for data it transfers to a processor. Outsourcing the work does not outsource the duty.
Appoint a DPO	**Someone is answerable**	Every controller and processor designates an individual accountable for compliance — the Data Protection Officer.
Register	**Tell the regulator**	Organisations above a certain size, or handling sensitive data about large numbers of people, must register their data processing systems with the NPC.
Keep only as long as needed	**Then dispose of it properly**	Retention has to end. Disposal has to be secure — improper disposal is itself an offence.

'We did not know' is not a defence, and negligence has its own penalty section. Not knowing is the thing being punished.

SECTION 20(F)

When a breach must be reported

Notification is mandatory when ALL THREE of these are true. Two out of three is not enough — and if you are unsure, the NPC's own guidance is to notify anyway.



The kind of data

Sensitive personal information, or any information that could be used to enable identity fraud.



Reasonable belief

There is reasonable belief that the data has been acquired by an unauthorised person.



Real risk of harm

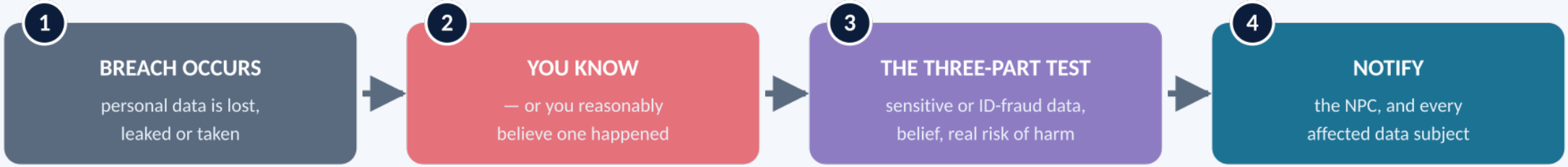
The breach is likely to give rise to a real risk of serious harm to the affected data subjects.

72 HOURS from knowledge of the breach, or from reasonable belief that one occurred. Notify the NPC and the affected people.

Concealing a breach that requires notification is a separate criminal offence.

SECTION 20(F)

The breach notification flow, and the clock





72 HOURS

The clock starts at KNOWLEDGE of the breach, or at reasonable BELIEF that one occurred.

Not when you finish investigating. Not when you are certain. Nobody gets three quiet weeks first.

Notify the National Privacy Commission AND the affected data subjects.

All three parts of the test must be true. Two out of three is not enough — and if you are unsure, the NPC's own guidance is to notify anyway.

Concealing a breach that requires notification is a separate criminal offence.

Write 72 on the board and circle it. It is the one number from this unit that is worth memorising exactly.

CONSEQUENCES

What breaking this law costs

6 mo – 7 yr

Imprisonment

range across offences

₱100k – ₱5M

Fines

range across offences

Heavier

For sensitive data

same act, worse penalty

100+

Data subjects affected

the maximum applies

Offences include	**Unauthorised processing**	Processing personal data with no lawful basis at all.
	Access due to negligence	You did not mean to let it out. You let it out. That is its own offence.
And	**Disposal, disclosure, concealment**	Improper disposal, unauthorised disclosure, concealing a breach, and processing for a purpose you never declared.

The ranges above cover the whole Act. The exact penalty depends on which offence, and on whether sensitive data was involved.

PART 3

Owning ideas

Copyright, plagiarism, and the licences that exist so people can share on purpose.

Copyright, here, in the Philippines

The law	**RA 8293**	The Intellectual Property Code of the Philippines. Copyright, trademarks, patents and related rights, in one statute.
When it starts	**The moment of creation**	Copyright exists from the instant an original work is fixed in a form. No registration, no notice, no fee required.
What it covers	**Expression, not ideas**	The article, the photo, the song, the source code. Not the underlying fact or the idea itself.
Fair use	**A real but narrow doorway**	Criticism, comment, news reporting, teaching, scholarship and research can qualify. It is judged case by case, not granted automatically.
Plagiarism	**A different thing entirely**	Passing off someone's work as your own. It can be an academic offence even where the copying was legal, and legal where it is dishonest.

Copyright is about permission. Plagiarism is about credit. You can violate either one without touching the other.

What an open licence actually grants

LICENCE	YOU MAY	YOU MUST	TYPICAL USE
CC BY	Use, change, sell	Give credit	Photos, articles, teaching material
CC BY-SA	Use, change, sell	Credit, and share alike	Wikipedia, community projects
CC BY-NC	Use and change	Credit, non-commercial only	Educational resources
CC0	Anything	Nothing	Public-domain dedication
MIT	Use in anything, including paid products	Keep the licence notice	A great deal of open-source code
GPL	Use and change	Publish your changes under GPL too	Linux and much of its ecosystem

'Free to use' almost never means 'no conditions'. Read the two words after the licence name — they are the entire deal.

PART 4

AI ethics

You have been using these tools since Session 1. Now we say plainly what they get wrong, and what you owe when you use them.

FOUR HONEST PROBLEMS

How these systems cause harm

Bias

A model learns from what it was shown. If the material under-represents people like you, the output will too — and it will be confidently normal about it.

Hallucination

Fluent, well-formatted, entirely invented. Court cases, section numbers, statistics, citations. The confidence is not evidence of anything.

Opacity

Often nobody can explain why a particular answer came out. That is a serious problem when the answer decides a loan, a job, or a grade.

Displacement of judgement

The real risk is not that it is wrong. It is that it is right often enough that you stop checking.

You have caught all four of these in this course already — in Session 5, Session 7 and last Saturday.

WHAT YOU OWE

Attribution and disclosure

Attribution	**Say where it came from**	For text, images, code and data. A link is usually enough. Silence is not.
Disclosure	**Say that you used a tool**	Which tool, what you asked, what you changed. That is exactly the AI Usage Log on every worksheet this semester.
Verification	**You own the output**	If you published it, it is yours — including the mistake. 'The AI said so' has never once worked as a defence.
Privacy	**Never paste other people's data**	Pasting a class list, a patient record or a customer file into a chatbot is a disclosure to a third party. Part 2 applies to it.
Honesty	**Do not pretend**	Undisclosed use is not clever. It is the same offence as any other misrepresentation of your own work.

Row four is the one that will get somebody in this room into real trouble at work. Say it out loud twice.

HOLD ON TO THIS

Six things from today

	One	The law is the floor	Legal and right are different questions. Ask both.
	Two	Two tiers of data	Personal information is protected. Sensitive personal information is protected harder.
	Three	Three principles	Transparency, legitimate purpose, proportionality. They fit on one sticky note.
	Four	Eight rights	Informed, object, access, rectification, erasure, damages, complain, portability.
	Five	72 hours	From knowing or reasonably believing. Concealment is its own crime.
	Six	Disclosure is not optional	Credit what you used. Log what you asked. Own what you publish.

Midterm on 7 November covers Units 6 to 10. This unit is on it, and the eight rights are the obvious question.

AFTER THE BREAK

In the laboratory today

Analyse	**Six real scenarios**	A school posting grades. A barangay posting an ayuda list. A leaked HR database. Real situations, from here.
Rule on them	**Against the Act**	Which principle is broken, whose rights, what should have happened instead.
Audit	**Your own site**	Eight real names have been on your homepage since August. Today you decide whether that is defensible.
Build	**/log**	A page that records the date of each visit and nothing else — then the greedy version, which you delete.
AI task	**Ask it to rule**	Then check every legal claim it makes. Watch which country's law it thinks you are asking about.

Bring the notes from Part 2. The clinic is not open-book from the internet — it is open-book from your own handwriting.

PROGRAMMING LAB ACTIVITY

This afternoon

The page remembers — and what it must not remember

What you are building today

Together	**The group page**	A /log page that records the date of every visit and nothing else. Then you write the greedy version that records far more, look at it, and delete it.
On your own	**Your own version — this is the marked one**	Your own small file, read back onto your page, with a kind message when it is missing — and one line saying what you chose not to keep.
To match	**Your page.html twin**	The same thing again, typed out by hand as HTML.

WHERE IT GOES LIVE

`gNN.cic.rmlsystems.net/log`	`gNN.cic.rmlsystems.net/<yourfolder>/`	`gNN.cic.rmlsystems.net/<yourfolder>/page.html`

Eight identical pages is eight zeros. Your version has to be yours — your data, your words.

NEW THIS WEEK

The Python you have not used before

`with open(path, "a") as f:`
open a file to ADD to it — "w" would erase it

`f.write(line + "\n")`
put one more line at the end

`f.readlines()`
read it back, one line per item

`except FileNotFoundError:`
for the first visit, when there is no file yet

at the shell

```
path = "visits.txt"

with open(path, "a") as f:
    f.write("2026-10-24\n")

try:
    with open(path) as f:
        lines = f.readlines()
except FileNotFoundError:
    lines = []

print(len(lines), "visits so far")
```

It prints: 1 visits so far — then 2, then 3, because the file survives

TWENTY POINTS

How this is marked

6	**It runs**	Your address loads and there is no traceback on it.
6	**It does this week's thing**	A file written, read back, and surviving a restart, with try/except for a missing one.
4	**It is yours**	The three lines you chose, and one honest line about what you left out.
2	**The twin matches**	page.html shows the same thing, by hand.
2	**Worksheet complete**	Including the AI sentence and the twin count.

DUE Sunday 25 October, 11:59pm · the full guide is at labs.cic.rmlsystems.net/guides/

Somebody is holding data about you right now.

A school, a barangay, a telco, a lending app, a shop you used once. Until today you had no idea what they owed you. Now you know the name of the law, the eight rights it gives you, and the address of the office that will take your complaint for free.

Questions?