Privacy by Design

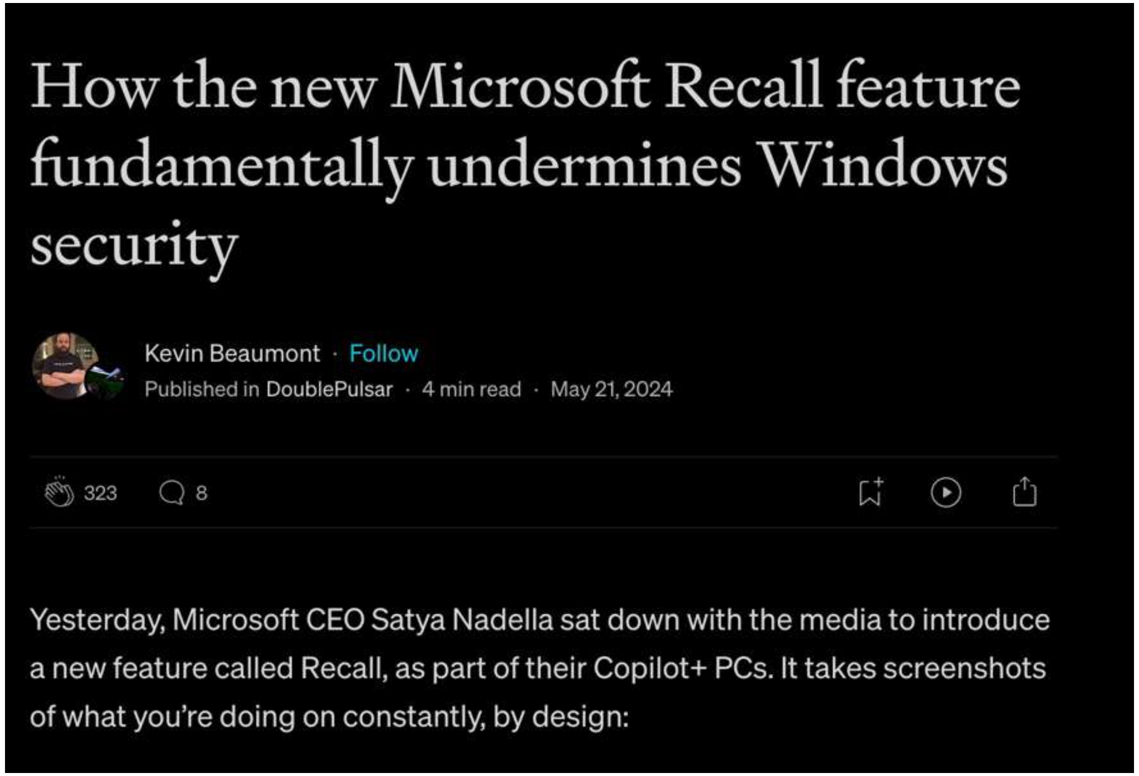
Integrating privacy by design in the software development lifecycle.

Bart van Buitenen

- Managing Director Dasprive vzw
- Host Dasprive podcast
- CISO, DPO, consultant Data Protection & Security
- Lecturer Data Protection & Security Thomas More University
- Chair of the Flemish Comittee for the Exchange of Personal Data
- Linkedin or via https://dasprive.be

Windows now includes Keylogger

- Microsoft Recall is a new “feature” for Windows
- Takes screenshots every three seconds and classifies anything you see or type via OCR / Azure AI (local)
- At least 3 months (25GB) & instantly indexed/searchable



How the new Microsoft Recall feature fundamentally undermines Windows security

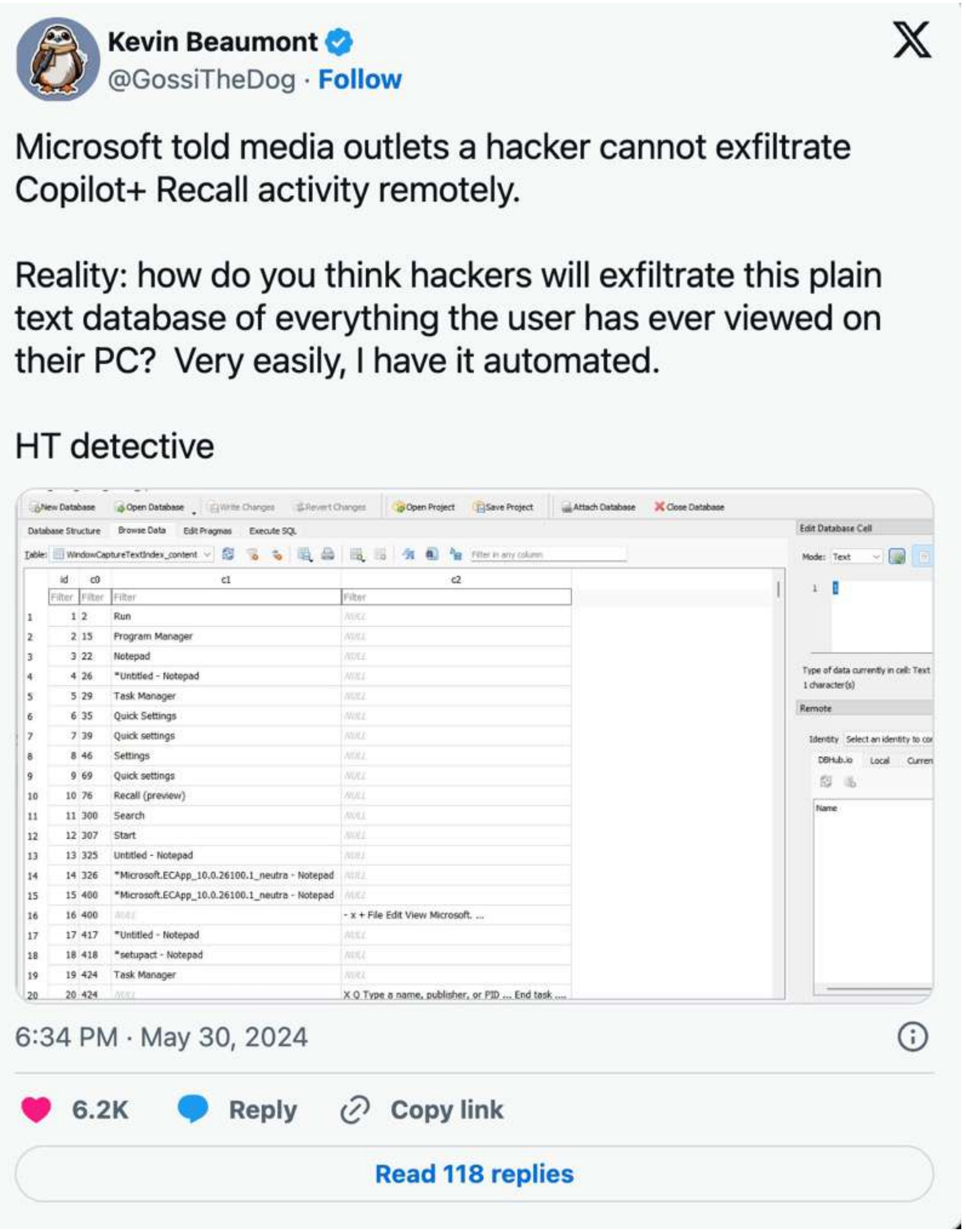
Kevin Beaumont · Follow

Published in DoublePulsar · 4 min read · May 21, 2024

Yesterday, Microsoft CEO Satya Nadella sat down with the media to introduce a new feature called Recall, as part of their Copilot+ PCs. It takes screenshots of what you're doing on constantly, by design:

Windows now includes Keylogger

- Microsoft Recall is a new “feature” for Windows
- Takes screenshots every three seconds and classifies anything you see or type
- 3 months (25GB) & instantly indexed/searchable
- This includes anything anyone shows on your screen (meeting), messages, etc.
- Stored in plain text, easily extracted (TotalRecall)
- Access screenshots from another user? L33t h4cks engaged -> C:/Users



Kevin Beaumont
@GossiTheDog · Follow

Microsoft told media outlets a hacker cannot exfiltrate Copilot+ Recall activity remotely.

Reality: how do you think hackers will exfiltrate this plain text database of everything the user has ever viewed on their PC? Very easily, I have it automated.

HT detective

Table: WindowCaptureTextIndex_content

	id	c0	c1	c2
	Filter	Filter	Filter	Filter
1	1	2	Run	NULL
2	2	15	Program Manager	NULL
3	3	22	Notepad	NULL
4	4	26	*Untitled - Notepad	NULL
5	5	29	Task Manager	NULL
6	6	35	Quick Settings	NULL
7	7	39	Quick settings	NULL
8	8	46	Settings	NULL
9	9	69	Quick settings	NULL
10	10	76	Recall (preview)	NULL
11	11	300	Search	NULL
12	12	307	Start	NULL
13	13	325	Untitled - Notepad	NULL
14	14	326	*Microsoft.ECApp_10.0.26100.1_neutra - Notepad	NULL
15	15	400	*Microsoft.ECApp_10.0.26100.1_neutra - Notepad	NULL
16	16	400	NULL	- x + File Edit View Microsoft. ...
17	17	417	*Untitled - Notepad	NULL
18	18	418	*setupact - Notepad	NULL
19	19	424	Task Manager	NULL
20	20	424	NULL	X Q Type a name, publisher, or PID ... End task ....

Type of data currently in cell: Text
1 character(s)

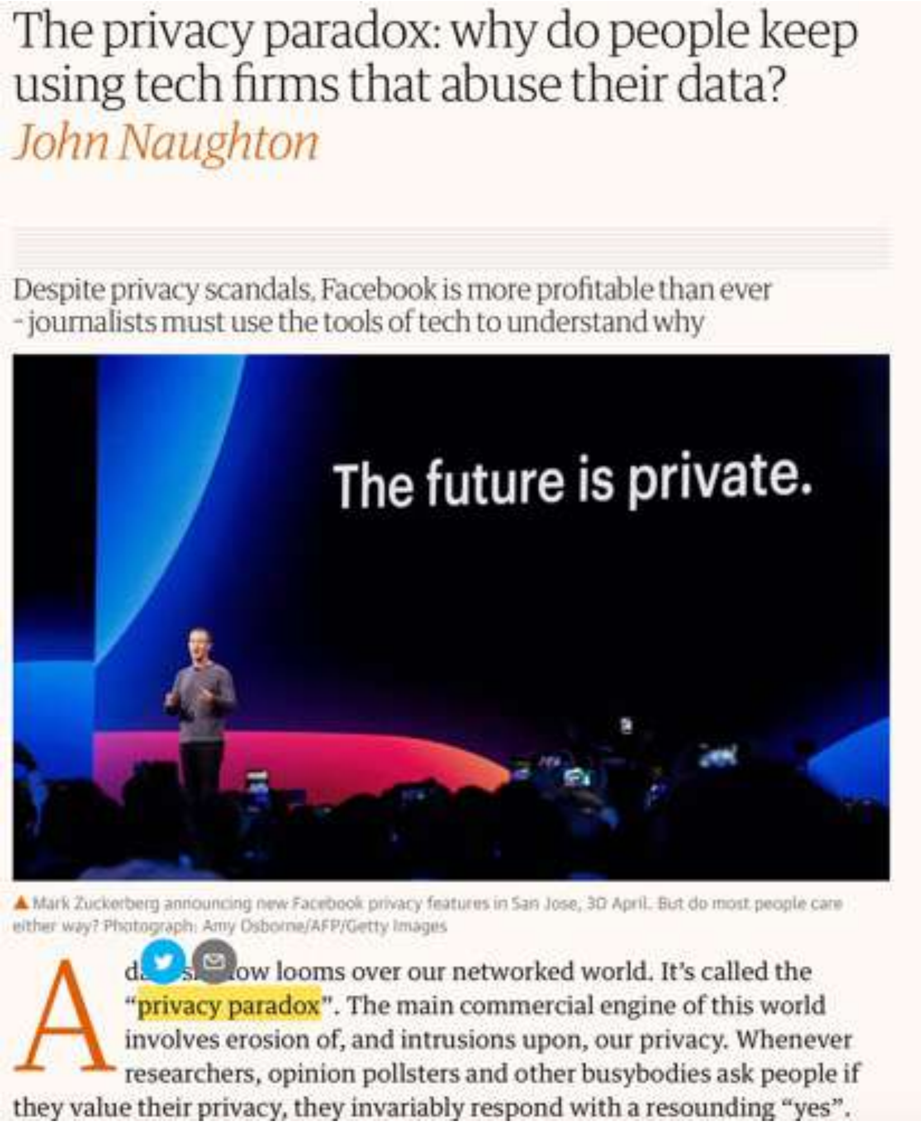
6:34 PM · May 30, 2024

6.2K Reply Copy link

Read 118 replies

Do we need privacy by design?

- The privacy paradox is real.
  - Power balance
  - Peer pressure
  - Necessity vs. Choice
  - Priorities
- But the onus shouldn’t be on the user
- Enter privacy by design: now a legal requirement.



The privacy paradox: why do people keep using tech firms that abuse their data?

John Naughton

Despite privacy scandals, Facebook is more profitable than ever - journalists must use the tools of tech to understand why

▲ Mark Zuckerberg announcing new Facebook privacy features in San Jose, 30 April. But do most people care either way? Photograph: Amy Osborne/AFP/Getty Images

A dark shadow looms over our networked world. It’s called the “privacy paradox”. The main commercial engine of this world involves erosion of, and intrusions upon, our privacy. Whenever researchers, opinion pollsters and other busybodies ask people if they value their privacy, they invariably respond with a resounding “yes”.

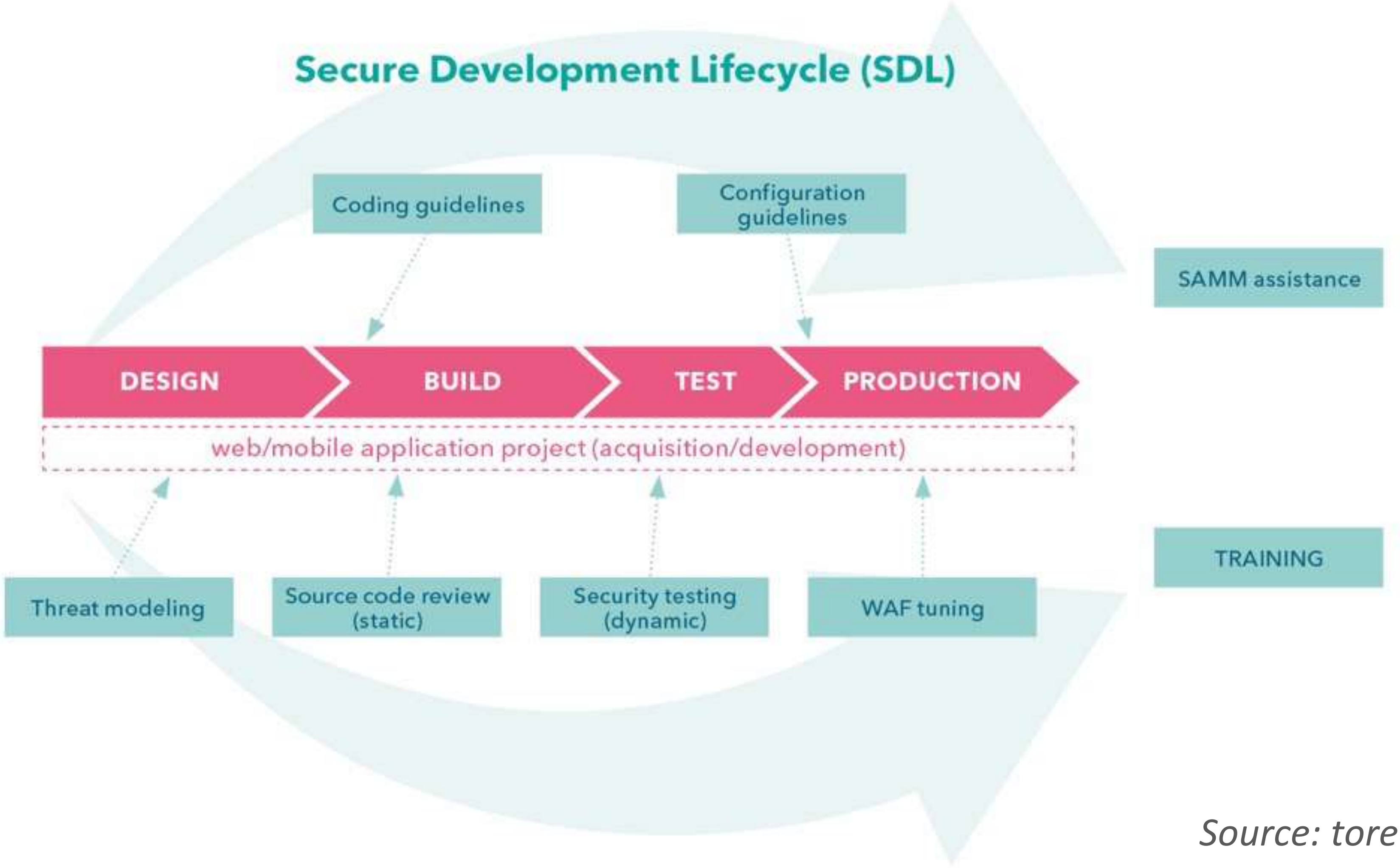
Privacy by design

Recital 4 GDPR: The processing of personal data should be designed to serve mankind.

Privacy by design:

- A principle or intent to include privacy as a basic element into all processes of an organization involved with personal data
- It is not a separate topic, software feature or project: privacy is included as a basic requirement in anything that is made or designed
- When talking about software development, this means looking at all different stages of a project to incorporate privacy, and especially the start

Integrating PbD into the SDL


Secure Development Lifecycle (SDL)
Coding guidelines
Configuration guidelines
SAMM assistance
DESIGN
BUILD
TEST
PRODUCTION
web/mobile application project (acquisition/development)
TRAINING
Threat modeling
Source code review (static)
Security testing (dynamic)
WAF tuning

Source: toreon.com

Design.

- Privacy Threat modeling: data flow, identify threats, propose mitigations
  - Transparency, purpose, necessity & data minimization, storage, accuracy, security
- Features, design/UI/structure, physical setup
- Training & awareness project/dev team
  - Data Protection Impact Assessment?

I'VE GOT A NEW PROJECT, AND WANT TO INVOLVE YOU FROM THE START.
PRIVACY PROFESSIONAL

Develop / Build.

- May not always require input at this stage.
- But in this phase software security requirements = privacy requirements
- For example:
  - Test data (sometimes developers test)
  - Secure development guidelines
  - Code review
  - Documentation (accountability principle)

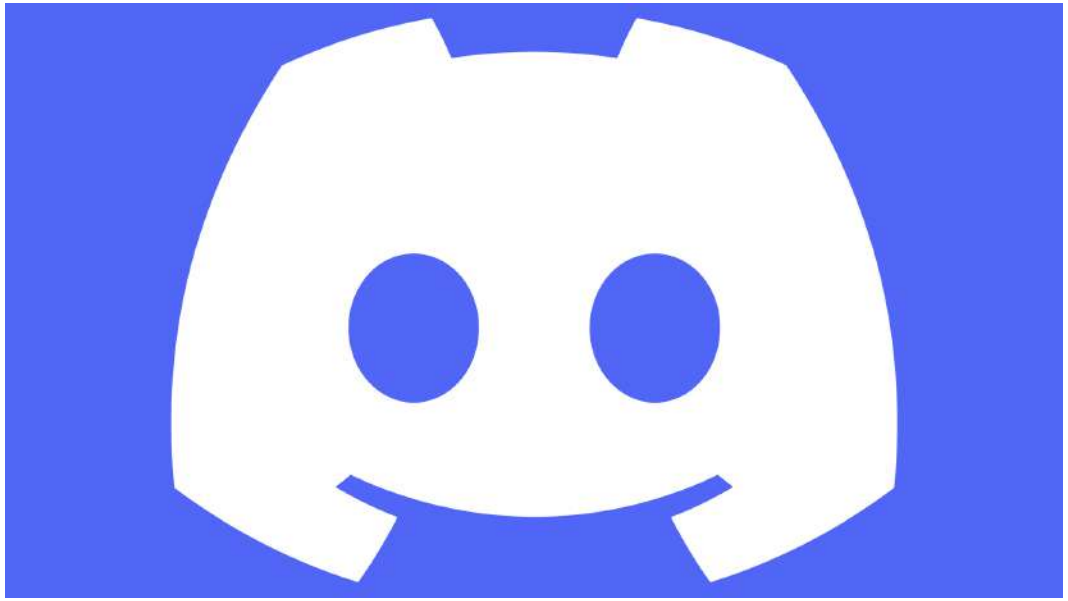
Test.

- Whether digital or non-digital project: time to test it.

- For example
  - Test logging function
  - Defaults in the app
  - DSRs: access, portability

Example: Discord

- Received a 800k fine by the CNIL
- Why?
  - 2.4 million user accounts that had noyt been used in over 3 years
  - Default behavior: clicking X (macOS vs windows)
  - Password of 6 characters accepted
  - No DPIA carried out



Production / Deployment.

- Trust, but verify.

- Examples
  - Similar to Test phase, but for real
  - User feedback
  - Regression testing

Governance.

- Doing the activities as described previously is great but needs to be part of a larger process.
- Privacy by Design also means implementing this on an organizational level.
- Management involvement, culture, privacy champions

Examples: PrivSec team, CAB, Project kick-off, Approval process

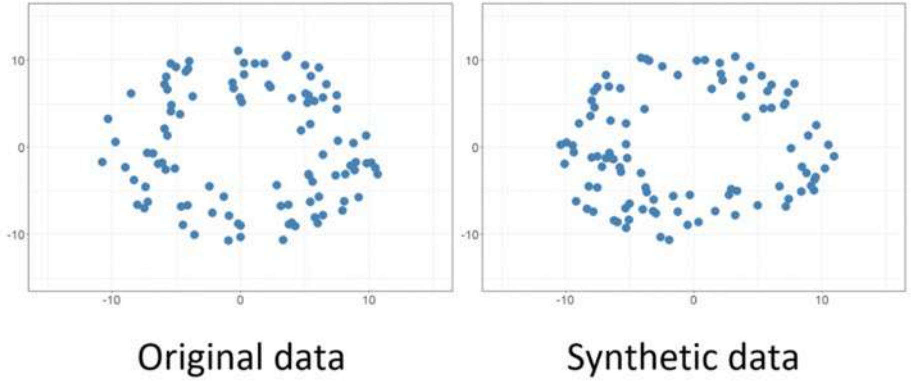
Privacy by design also means a proper governance structure.
We just made a checklist per phase.

What's the ROI?

- Better software = $$
  - Code quality
  - Security risks
- Better documentation
- Trustworthy reputation
- Happy customers
- Happy developers

PETs

- Synthetic data (testing)

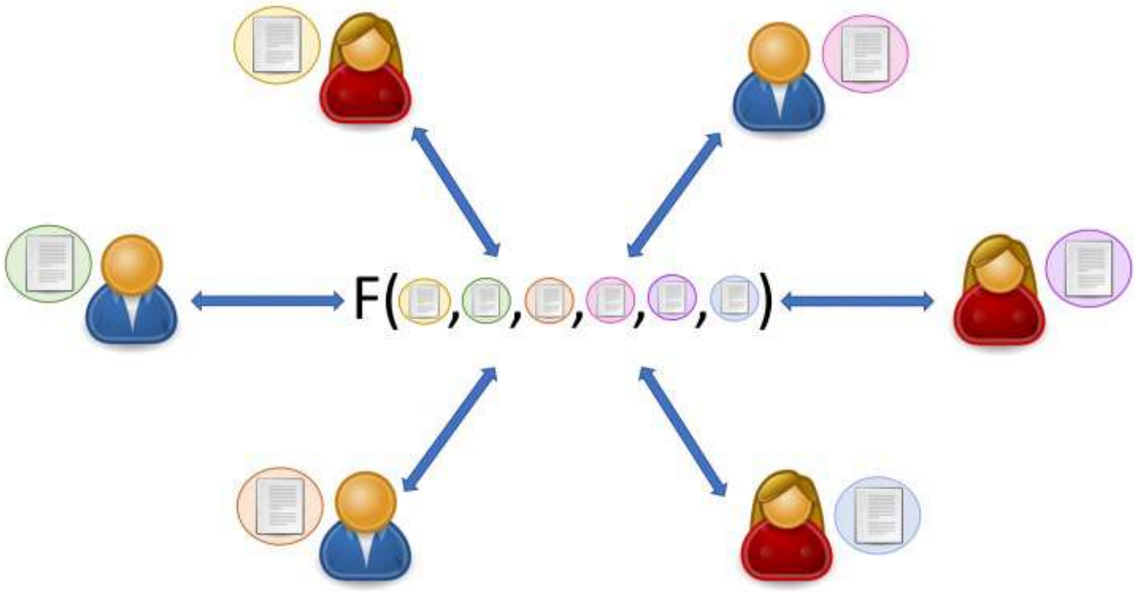


The synthetic data retains the structure of the original data but is not the same

https://dataingovernment.blog.gov.uk/2020/08/20/synthetic-data-unlocking-the-power-of-data-and-skills-for-machine-learning/

PETs

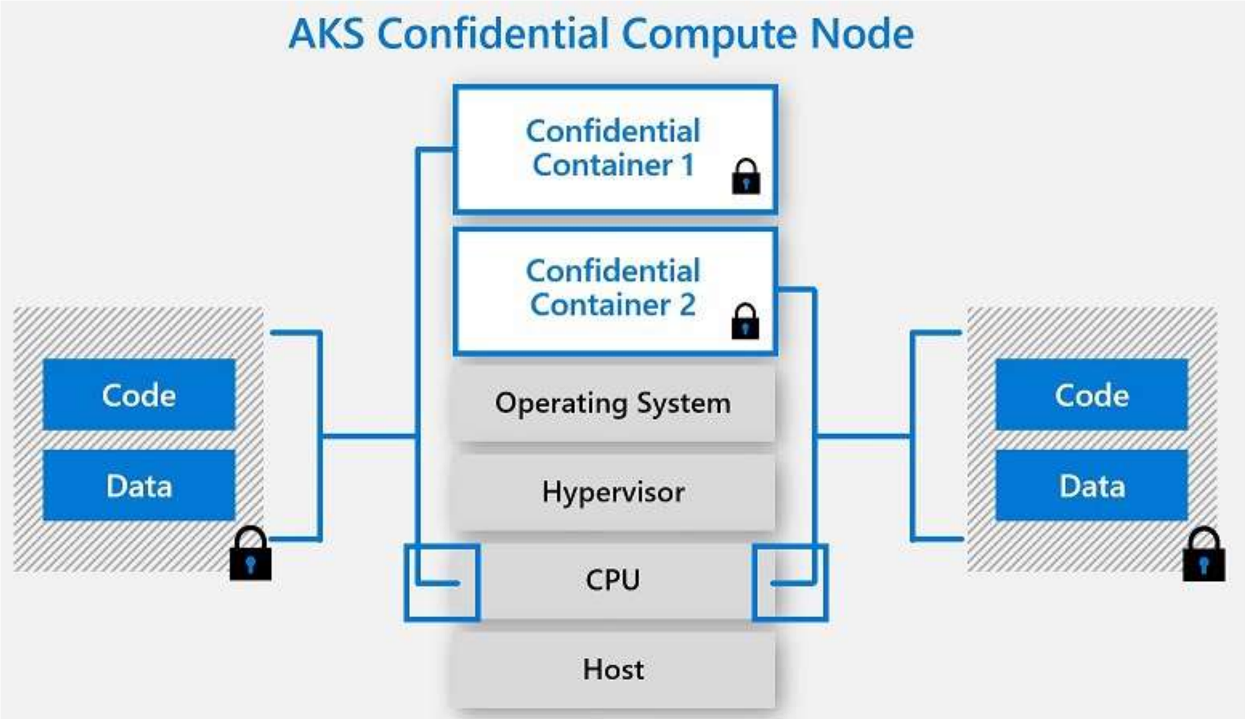
- Synthetic data (testing)
- Multiparty computation (design)



https://www.esat.kuleuven.be/cosic/blog/the-three-musketeers-of-secure-computation-mpc-fhe-and-fe/

PETs

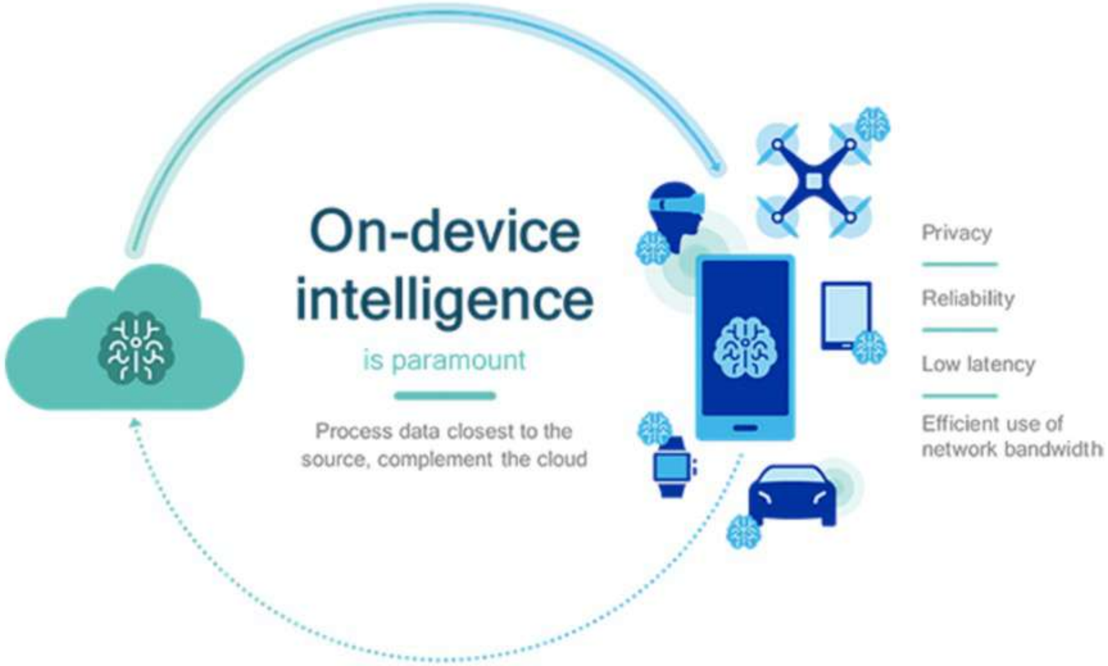
- Synthetic data (testing)
- Multiparty computation (design)
- Confidential Compute (implementation)



https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-nodes-aks-overview

PETs

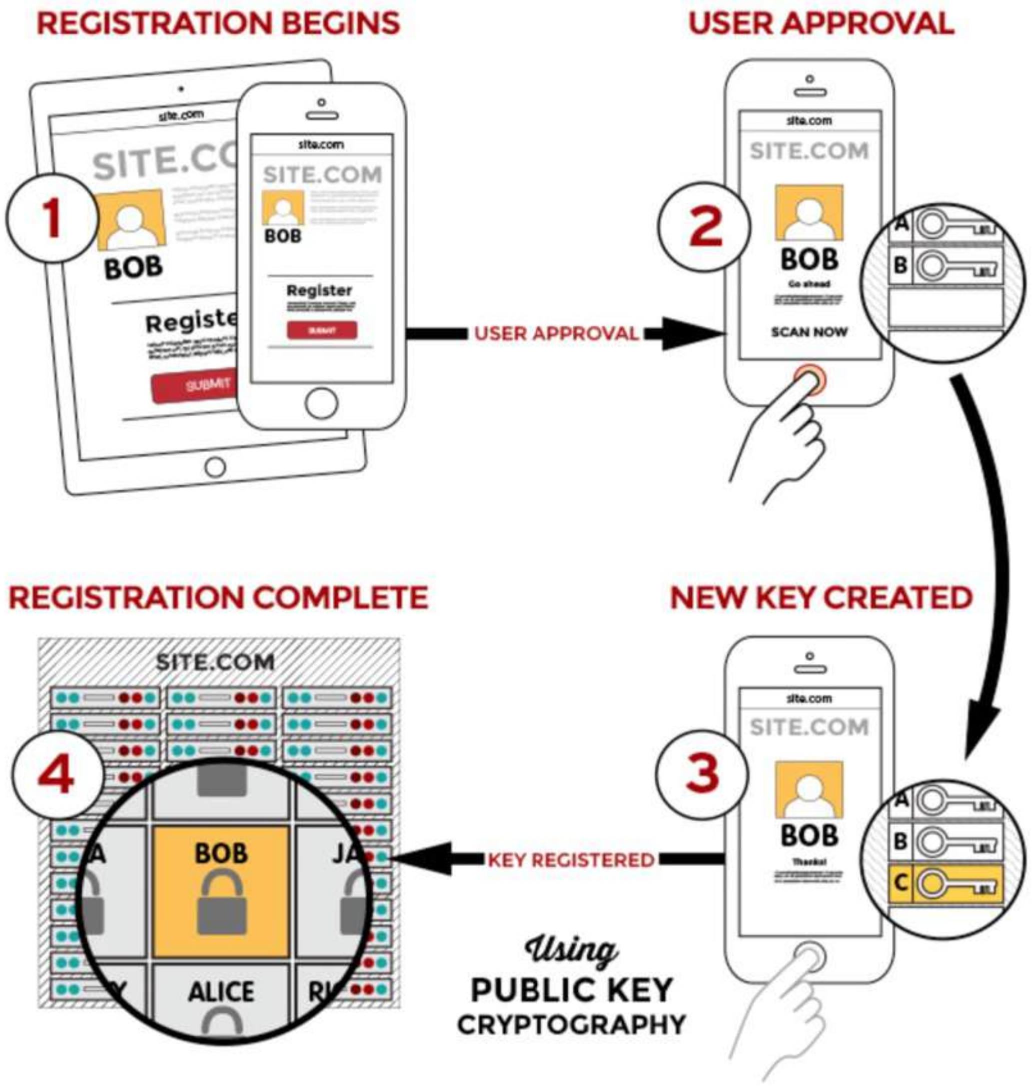
- Synthetic data (testing)
- Multiparty computation (design)
- Confidential Compute (implementation)
- On Device processing (design, implementation)


On-device intelligence
is paramount
Process data closest to the source, complement the cloud
Privacy
Reliability
Low latency
Efficient use of network bandwidth

https://www.qualcomm.com/news/onq/2017/08/we-are-making-device-ai-ubiquitous?cmpid=oofyus181544

PETs

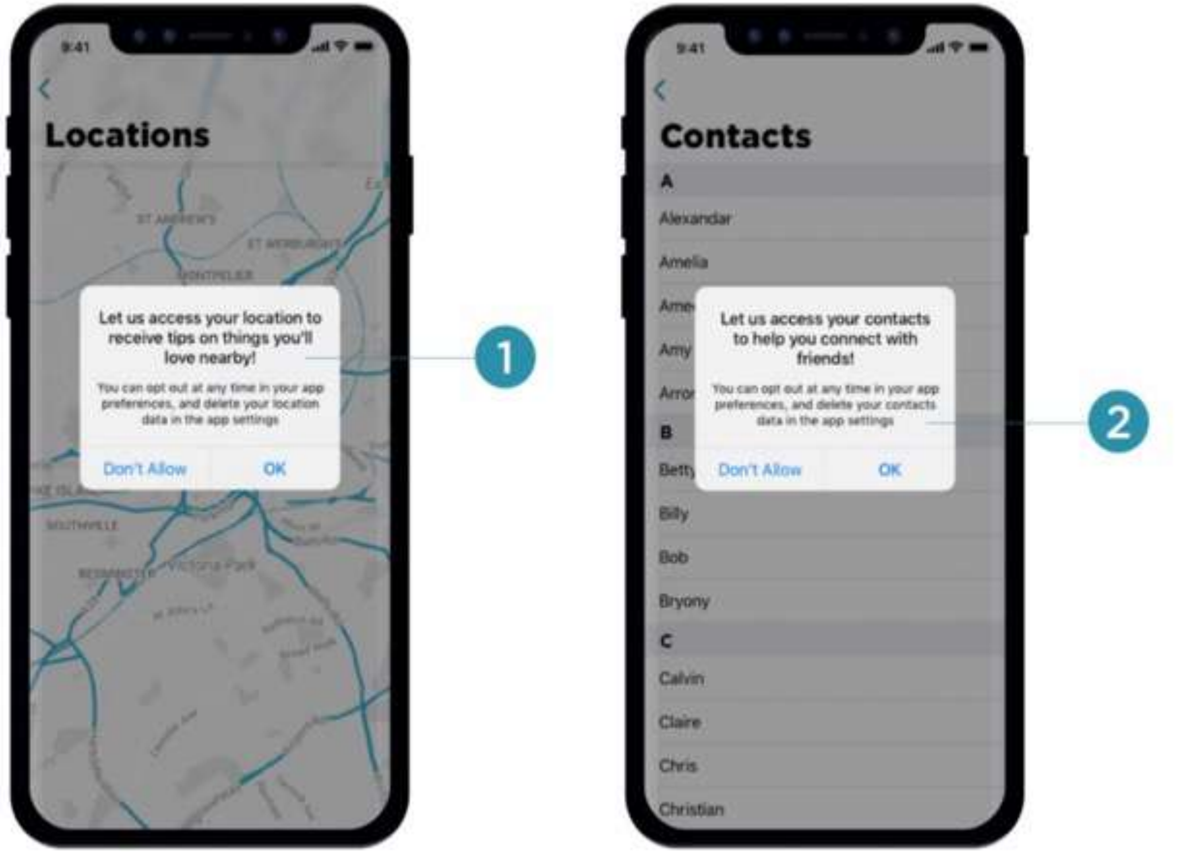
- Synthetic data (testing)
- Multiparty computation (design)
- Confidential Compute (implementation)
- On Device processing (design, implementation)
- Privacy enhanced authentication eg FIDO (design, implementation)



https://fidoalliance.org/how-fido-works/

PETs

- Synthetic data (testing)
- Multiparty computation (design)
- Confidential Compute (implementation)
- On Device processing (design, implementation)
- Privacy enhanced authentication eg FIDO (design, implementation)
- The UX: "Just in Time" notifications



Let us access your location to receive tips on things you'll love nearby!

You can opt out at any time in your app preferences, and delete your location data in the app settings

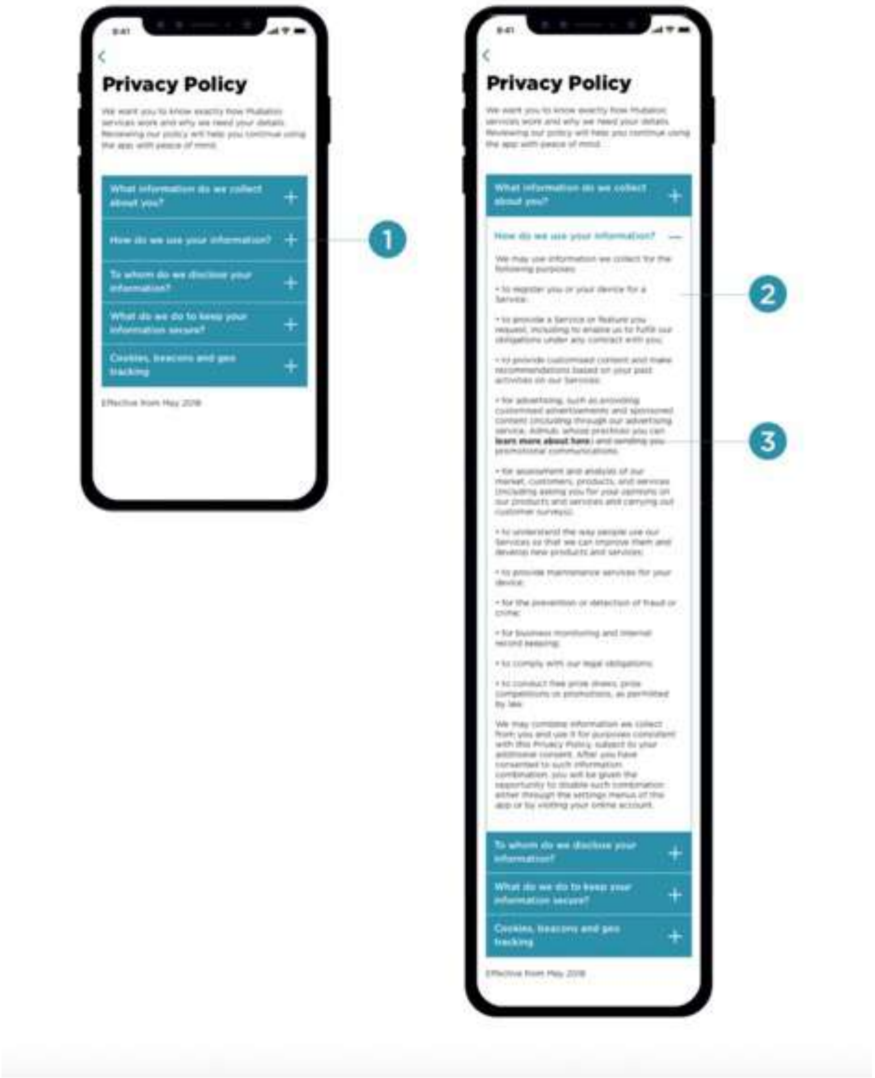
Let us access your contacts to help you connect with friends!

You can opt out at any time in your app preferences, and delete your contacts data in the app settings

Source: Mubaloo GDPR framework

PETs

- Synthetic data (testing)
- Multiparty computation (design)
- Confidential Compute (implementation)
- On Device processing (design, implementation)
- Privacy enhanced authentication eg FIDO (design, implementation)
- The UX: "Just in Time" notifications, layered privacy policy



Privacy Policy

We want you to know exactly how Mubaloo services work and why we need your details. Reviewing our policy will help you continue using the app with peace of mind.

What information do we collect about you? +

How do we use your information? +

To whom do we disclose your information? +

What do we do to keep your information secure? +

Cookies, beacons and geo tracking +

Effective from May 2018

Privacy Policy

We want you to know exactly how Mubaloo services work and why we need your details. Reviewing our policy will help you continue using the app with peace of mind.

What information do we collect about you? +

How do we use your information? —

We may use information we collect for the following purposes:

- to register you or your device for a Service;
- to provide a Service or feature you request, including to enable us to fulfil our obligations under any contract with you;
- to provide customised content and make recommendations based on your past activities on our Services;
- for advertising, such as providing customised advertisements and sponsored content (including through our advertising service, Admob, whose practices you can **learn more about here**) and sending you promotional communications;
- for assessment and analysis of our market, customers, products, and services (including asking you for your opinions on our products and services and carrying out customer surveys);
- to understand the way people use our Services so that we can improve them and develop new products and services;
- to provide maintenance services for your device;
- for the prevention or detection of fraud or crime;
- for business monitoring and internal record keeping;
- to comply with our legal obligations;
- to conduct free prize draws, prize competitions or promotions, as permitted by law.

We may combine information we collect from you and use it for purposes consistent with this Privacy Policy, subject to your additional consent. After you have consented to such information combination, you will be given the opportunity to disable such combination either through the settings menus of the app or by visiting your online account.

To whom do we disclose your information? +

What do we do to keep your information secure? +

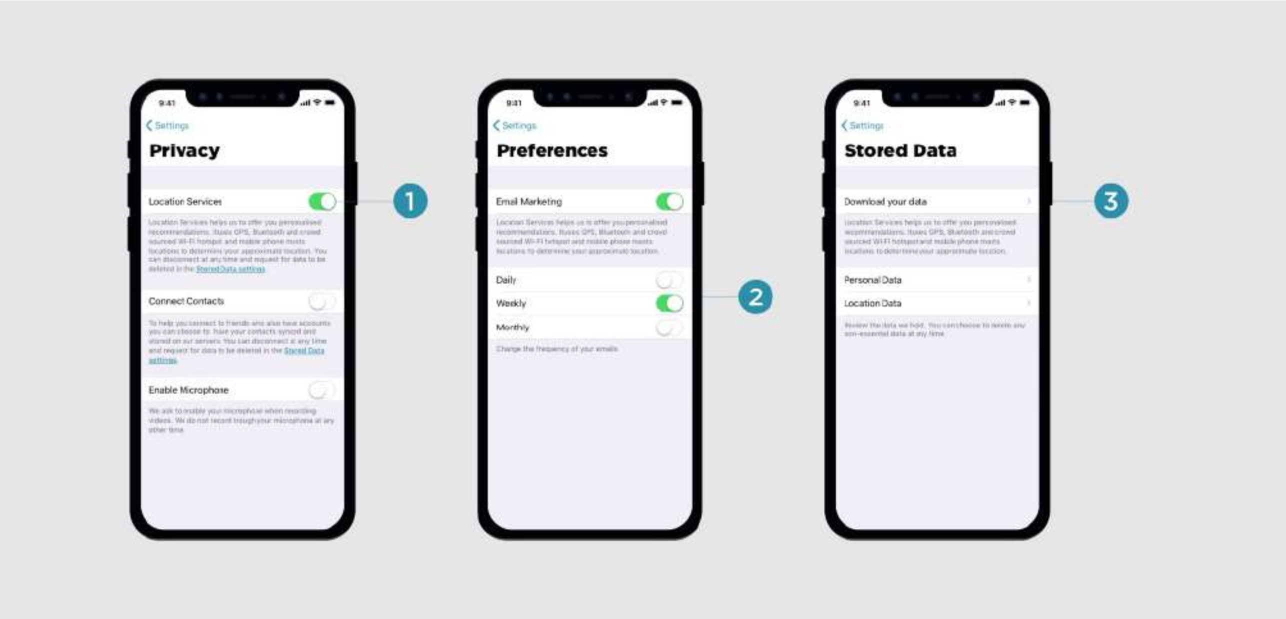
Cookies, beacons and geo tracking +

Effective from May 2018

Source: Mubaloo GDPR framework

PETs

- Synthetic data (testing)
- Multiparty computation (design)
- Confidential Compute (implementation)
- On Device processing (design, implementation)
- Privacy enhanced authentication eg FIDO (design, implementation)
- The UX: "Just in Time" notifications, layered privacy policy, user control



‹ Settings

Privacy

Location Services ●

Location Services helps us to offer you personalised recommendations. It uses GPS, Bluetooth and crowd sourced Wi-Fi hotspot and mobile phone masts locations to determine your approximate location. You can disconnect at any time and request for data to be deleted in the Stored Data settings.

Connect Contacts ○

To help you connect to friends who also have accounts you can choose to have your contacts synced and stored on our servers. You can disconnect at any time and request for data to be deleted in the Stored Data settings.

Enable Microphone ○

We ask to enable your microphone when recording videos. We do not record trough your microphone at any other time.

‹ Settings

Preferences

Email Marketing ●

Location Services helps us to offer you personalised recommendations. It uses GPS, Bluetooth and crowd sourced Wi-Fi hotspot and mobile phone masts locations to determine your approximate location.

Daily ○

Weekly ●

Monthly ○

Change the frequency of your emails.

‹ Settings

Stored Data

Download your data ›

Location Services helps us to offer you personalised recommendations. It uses GPS, Bluetooth and crowd sourced Wi-Fi hotspot and mobile phone masts locations to determine your approximate location.

Personal Data ›

Location Data ›

Review the data we hold. You can choose to delete any non-essential data at any time.

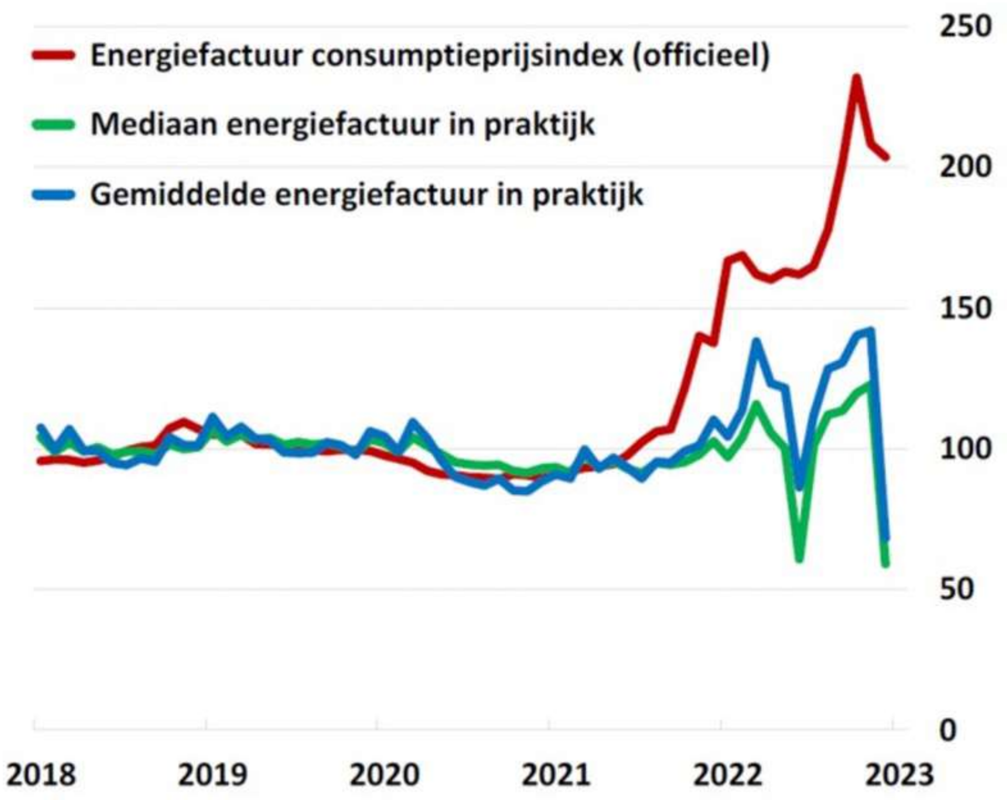
Source: Mubaloo GDPR framework

Cases: BNP - UGent

Objective: investigate energy spending of average households (bank, university, BE)

- Transaction data anonymized *and* remains at the bank
- Ethics board approval within university, algorithm is made at university
- Run from within bank systems, output is verified by the bank before sending.
- Output is transferred to university, statistical results

Figuur 1 – Evolutie van de energiefactuur volgens de consumptieprijsindex versus de praktijk (2018 = 100)



Cases: Local government

Objective: use smart cameras to measure population density along the coast (Local government, COVID, BE)

- Images stored on camera for only a few milliseconds
- Afterwards immediately blur passersby irreversibly, on-device
- Processing limited: only summer months and places likely to be crowded
- Security: severely limited access to system and images.
- Deactivate non-necessary functions in firmware

Final thoughts

- It can't *just* be about privacy.
- Long term investment, but tangible benefits
- Need to involve organizations as a whole, especially management.
- Making privacy by design the default will take some time.

Resources

- EDPB guidance on Data Protection by Design & Default: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf
- Privacy Design strategies by Jaap Henk Hoepman Little Blue book: https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf
- Seven Foundational Principles: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf
- A guide to privacy by design: https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf
- Privacy in the product design lifecycle: https://ico.org.uk/for-organisations/privacy-in-the-product-design-lifecycle/
- Datatilsynet data protection by design: https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/