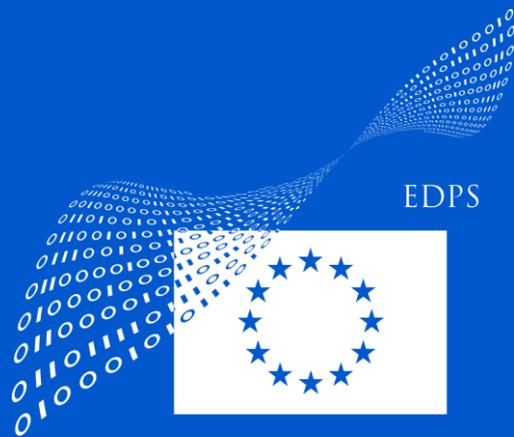


Data Protection in Mobile Apps

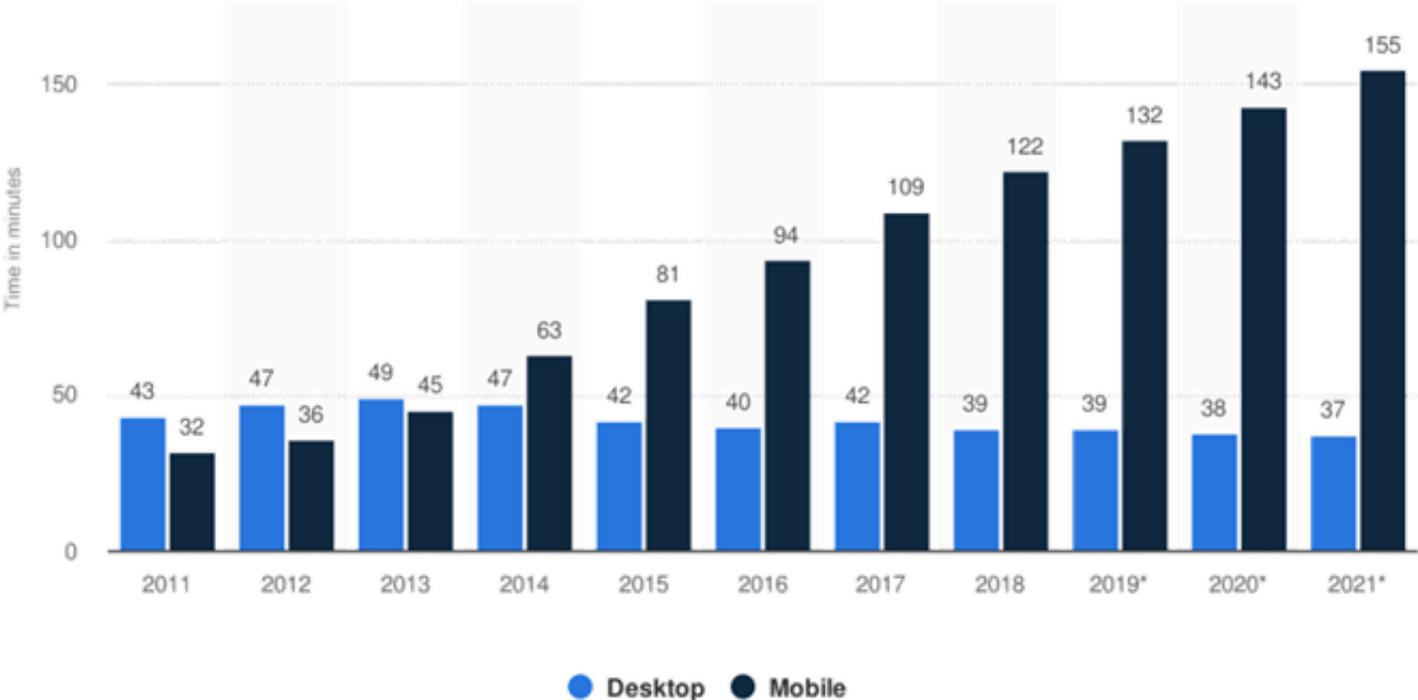
EUI DPO Meeting in Florence,
7 November 2019

Dr Robert RIEMANN, EDPS IT Policy Unit





Daily Internet Time spent per Capita by Device

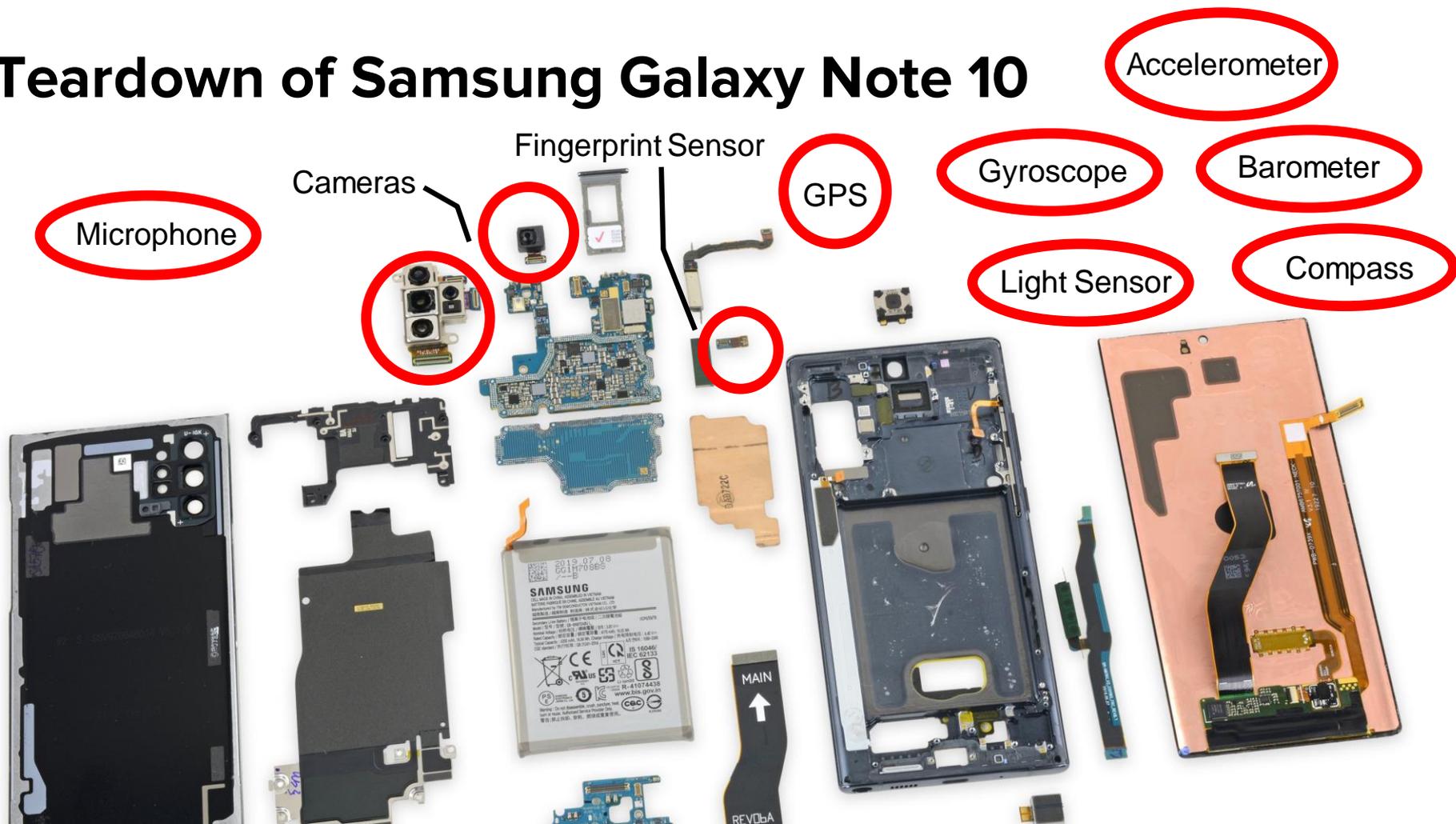


Source
Zenith
© Statista 2019

Additional Information:
Worldwide; Zenith; 2011 to 2018

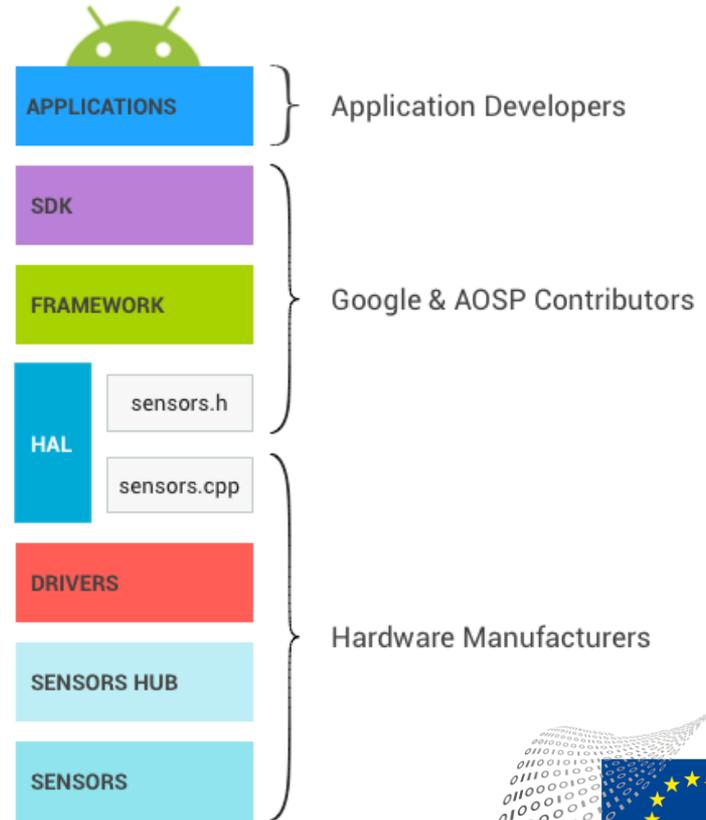


Teardown of Samsung Galaxy Note 10

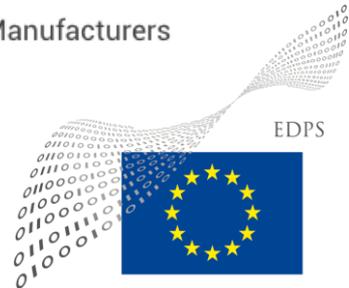


Development of Mobile Apps

- every mobile app is developed on top of many building blocks
- building blocks offer simple API to carry out complex tasks:
 - Sensor API to take photos, record audio, get geo localisation, etc.
 - Software Development Kit (SDK) to e.g. authenticate against Facebook using cryptography
- most apps use building blocks provided by third parties



(Source: android.com)



Privacy of Mobile Phone Users at Stake

**PRIVACY
INTERNATIONAL**

Forbes



EDITOR'S PICK | 4,062 views | Oct 16, 2019, 8:00 am

Top Travel Apps Fail The Privacy And Security Test

Davey Winder Senior Contributor

Cybersecurity

I report and analyse breaking cybersecurity and privacy stories

[Home](#)

No Body's Business But Mine: How Menstruation Apps Are Sharing Your Data

Monday, September 9, 2019

[Home](#)

How Apps on Android Share Data with Facebook - Report

Saturday, December 29, 2018

ZDNet



MENU

EU

Mobile security: These health apps aren't good for your phone or your privacy

As people turn to mobile apps to help manage health conditions, cyber criminals have realised there's money to be made.

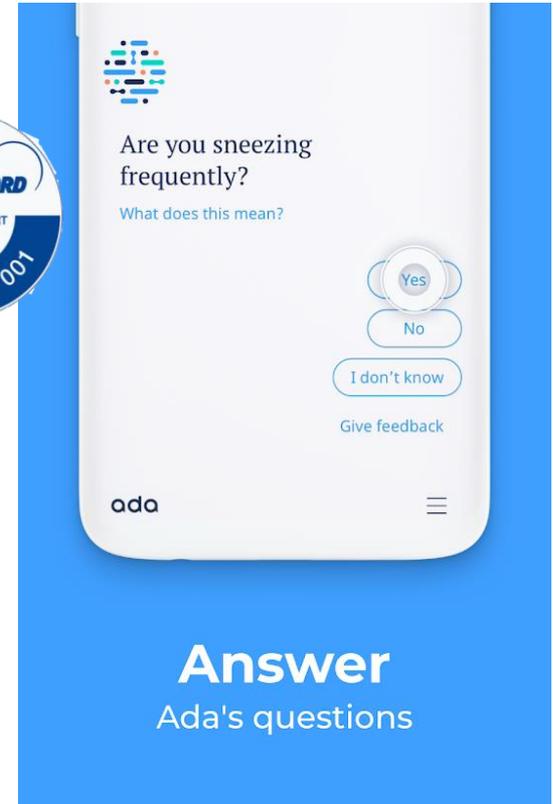


By [Danny Palmer](#) | October 7, 2019 -- 13:54 GMT (14:54 BST) | Topic: [Security](#)



Example: Health Insurance Endorsed Health App

- Mobile app [Ada](#) helps users to log health conditions and provides automated diagnoses.
- App incorporated *Facebook* login and in-app analysis with [Amplitude](#)
- In Q1 2018, TÜV Nord certified ADA: ISO/IEC 27001
- In 09/2019, app was found to transfer identifiers and health data to third parties, amongst others: session id, android ad id, user id, device id, age, sex, and user input like **finding=UrinaryIncontinence**



Sources: [Ada App](#) on Google Play Store

[Kuketz IT Security Blog](#) (German), 25/09/2019

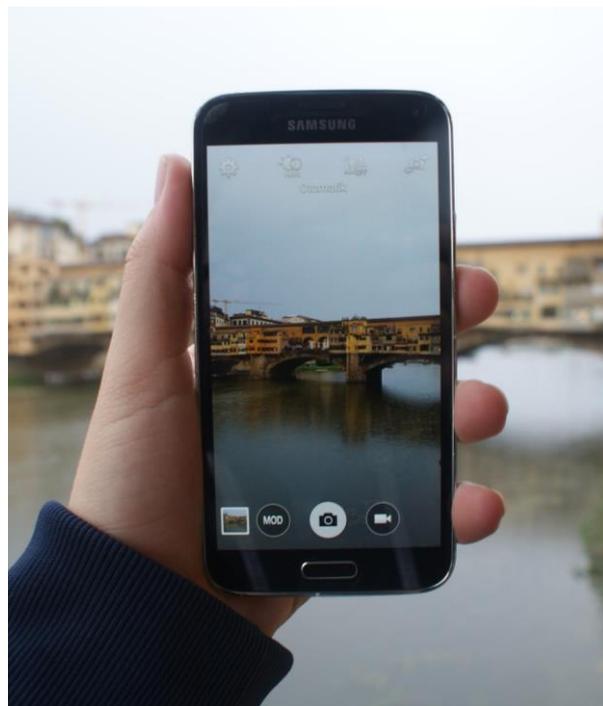
The EDPS Mobile App Inspection comes certainly



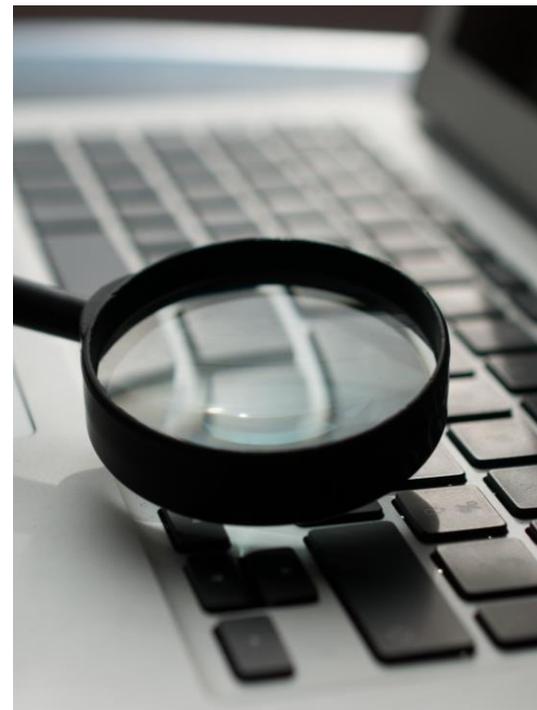
Guidelines on the
protection of personal
data processed by
**mobile
applications**
provided by European
Union institutions



Step 1: Guidance ([link](#))



Step 2: Awareness
Training in Florence



Step 3:
Inspection



Hands-On Exercise in Groups

(inverse class)

Work in Groups: Data Collection Practices of Mobile Apps

Use your smartphone to investigate data processing practices of any app!

Transparency

Who is the controller?

How to contact the DPO?

Which personal data is processed by the app?

Find the shortest and longest policy for apps on your phone!

App Permissions

Which permissions do apps have?

Can you link these permissions to app purposes?

Are some permissions too broad or not always necessary?

Find the app with most and least permissions on your phone!

Consent

In the life cycle of an app, when are users asked to give consent?

How can valid consent be obtained on smartphones?

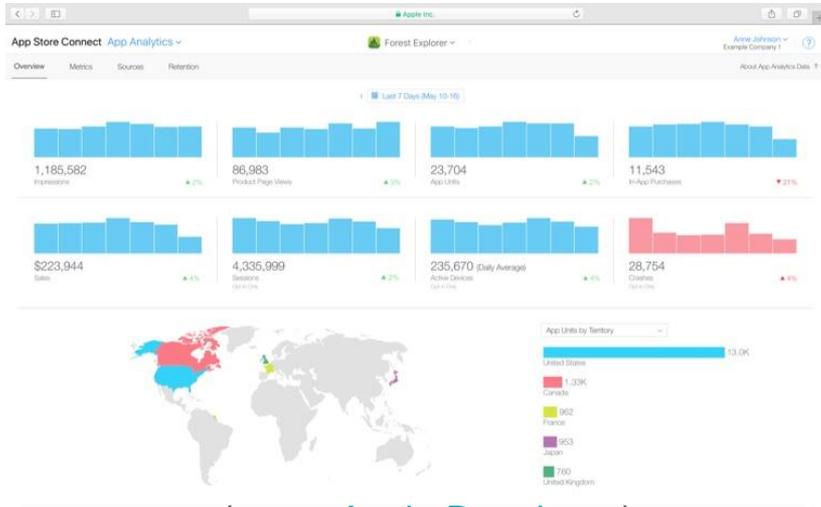
How is consent withdrawn?



Plenum Debate: App Stores

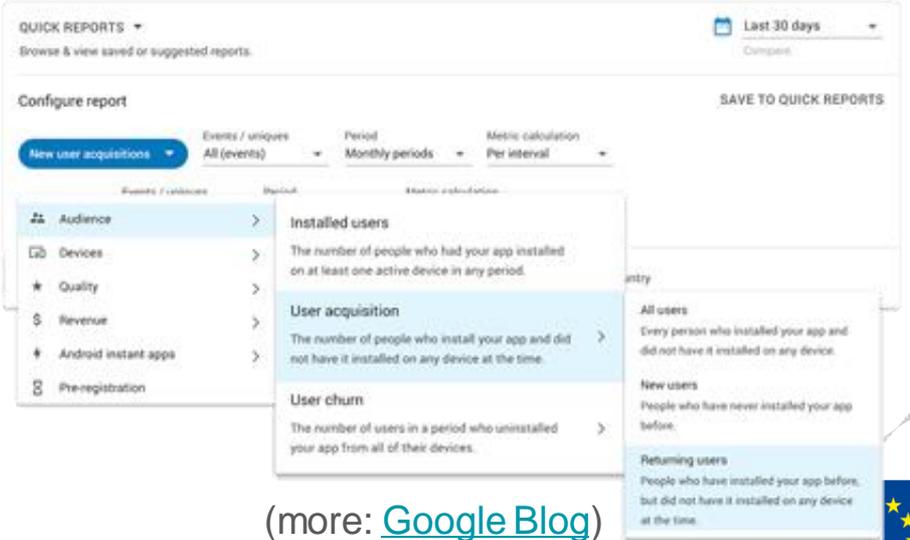
- Are App Stores Data Controllers, Processors or Joint-Controllers?

Apple App Store Statistics



(more: [Apple Developer](#))

Google Play Store Developer Dashboard



(more: [Google Blog](#))

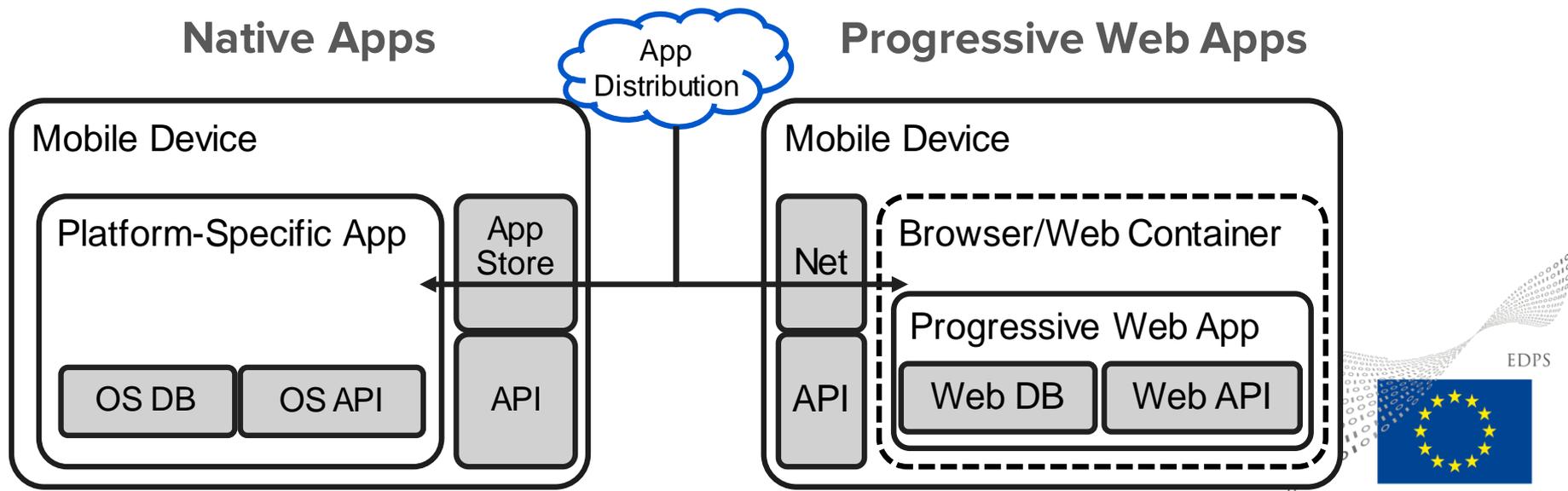
EDPS



Progressive Web Apps: Concept



- PWA are websites optimised for modern mobile browser and their web APIs.
- They provide several features that give them the same user experience advantages as native apps (offline, notifications, etc). Read [more](#).



Progressive Web Apps: Advantages



Data Protection Advantages

- no app stores means less 3rd parties
- one version for all terminal devices for less complexity/documentation
- no interference with other installed apps (shared contacts, calendar, etc.)
- open standards, linkable, searchable

Examples

- <https://www.instagram.com>
- <https://mobile.twitter.com>
- <https://m.uber.com>
- <https://m.alibaba.com>
- <https://tinder.com>
- <https://app.ft.com>



Wrap-Up

Personal Data Processing with Mobile Apps: Cheat Sheet

Is a mobile app required or is a mobile-friendly website (PWA) enough?

Transparency

employ layered data protection notices and in-context notices

consider target audience (children, etc.)

Check [EDPS Guidelines on Mobile Apps and Devices!](#)

Privacy by Default/Design

limit processing to the strictly necessary

use as few permissions as possible

employ optional permissions if possible

monitor security throughout lifecycle

test the app and assess all its data flows

Third-Party Services

avoid 3rd-party services whenever possible

conclude data processing agreements

monitor for changes of their terms of service



Homework

Mobile App Inventory

Some EU institutions and bodies required several months to compile the inventory of their web services for the EDPS inspection.

1. Please update your mobile app inventory.
2. Please update your related records of processing activities (EU-DPR Art. 31)
3. Please ensure that data processing agreements with third-parties are in place.

The Mobile App Inspection team may inquire technical documentation and software from controllers to carry out their analysis.



Your Questions

Further Reading

- EDPS Guidelines:
[Mobile Applications \(2016\)](#), [Mobile Devices \(2015\)](#)
- WP29 Opinion:
[Opinion 02/2013 on apps on smart devices](#)
- Progressive Web Apps:
https://developer.mozilla.org/en-US/docs/Web/Progressive_web_apps
- Spanish DPA Technical Survey on mobile app privacy (2019):
<https://www.aepd.es/media/notas-tecnicas/nota-tecnica-IMDEA-android-en.pdf>



EDPS

Credits

- Images:

- Crowd with Mobile Phones: [unsplash/@bpro1360](https://unsplash.com/@bpro1360) ([unsplash license](#))
- Smart Phone Teardown: [ifixit/Sam Goldheart](https://ifixit.com/SamGoldheart) ([Creative Commons BY-NC-SA license](#))
- Florence Photo: [Pexels/@Tookapic](https://pexels.com/@tookapic) ([Creative Commons Public Domain](#))
- Magnifying Glass: [unsplash/@olloweb](https://unsplash.com/@olloweb) ([unsplash license](#))

- Screenshots:

- <https://www.zdnet.com/article/mobile-security-these-health-apps-arent-good-for-your-phone-or-your-privacy/>
- <https://www.forbes.com/sites/daveywinder/2019/10/16/top-travel-apps-for-android-and-iphone-fail-privacy-and-security-tests>
- <https://www.privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruation-apps-are-sharing-your-data>
- <https://privacyinternational.org/appdata>



EDPS