



Το έργο χρηματοδοτήθηκε από το  
Πρόγραμμα Δικαιώματα,  
Ισότητα και Ιθαγένεια 2014-2020  
της Ευρωπαϊκής Ένωσης



# DPbD – Transparency, Lawfulness & Fairness

*Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT products  
and services ([www.bydesign-project.eu](http://www.bydesign-project.eu))*





# Key design elements for transparency

- **Clarity** – Information shall be in clear and plain language, concise and intelligible.
- **Semantics** – Communication should have a clear meaning to the audience in question.
- **Accessibility** - Information shall be easily accessible for the data subject.
- **Contextual** – Information should be provided at the relevant time and in the appropriate form.
- **Relevance** – Information should be relevant and applicable to the specific data subject
- **Universal design** – Information shall be accessible to all data subjects
- **Comprehensible** – Data subjects should have a fair understanding of what they can expect with regards to the processing of their personal data, particularly when the data subjects are children or other vulnerable groups.
- **Multi-channel** – Information should be provided in different channels and media, not only the textual,
- **Layered** – The information should be layered in a manner that resolves the tension between completeness and understanding



# DPdD - Bad practices in transparency

- Common bad formulations in privacy policies:
  - **“We may...”** : Introduces ambiguity
  - **“Personally Identifiable Information”** : This is only a sub-category of personal data
  - **“by <....>, you consent to this processing”**: Consent must be free, informed, specific and unambiguous (and thus, obtaining valid consent necessitates specific implementation)
  - **“administration purposes”**: Needs clarification (maybe in a second-level)
  - **“including, but not limited to....:”** Not clear information – implies non-compliance with the minimization principle
  - **A long page/doc**: Difficult to read.



# Key design elements for lawfulness/fairness

- **Relevance** – The correct legal basis shall be applied
- **Differentiation** – The legal basis used for each processing activity shall be differentiated.
- **Specified purpose**
- **Autonomy** – The user should be granted the highest degree of autonomy as possible
- **Gaining consent** – free, specific, informed and unambiguous (“opt-in”)
- **Consent withdrawal** – Withdrawal shall be as easy as giving consent.
- **Cessation** – If the legal basis ceases to apply, the processing stops
- **No deception** – Information and options should be provided in an objective and neutral way, avoiding any manipulation
- **Predetermination** – Establishment of legal basis before the processing takes place.
- **Adjust** – If there is a valid change of legal basis, the actual processing must be adjusted
- **Fair algorithms** – Algorithms functioning in line with the purposes (transparently for users)
- **Interaction** – Users must be able to communicate and exercise their rights
- **Respect rights**



# DPdD - Bad practices in lawfulness/fairness



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

- Common bad practices in implementations:
  - Consent obtained is not valid
    - The user is “forced” to provide consent
    - The actual legal basis is not the user’s consent
    - One  for all processes, for several different purposes
    - Etc.
  - Change of legal basis during the process
    - E.g. the user tries to revoke consent but this right is not fulfilled due to “legitimate interests” of the controller
  - The algorithms do much more things than the users think
    - E.g. Profiling of users and making decisions for them



# Possible design patterns for transparency

	Language complexity	Vagueness of terms	Wall of text	Excessive length	Lack of audience-tailoring	Wrong timing	Lack of familiarity	Scattered information
Illustrative examples								
FAQs								
Timeline								
Swimlane								
Comics								
Meaningful organization								
Companion icons								
Layered notice								
Videos								
Highlighted text								
Alert icons								

**Table 1 – The design patterns organized per category.**

Explanation	Navigation	Overview	Emphasis
Illustrative examples	Meaningful organization	Layered notice	Highlighted text
FAQs	Companion icons	Videos	Alert icons
Timeline			
Swimlane			
Comics			


Fig. 1 – Matrix illustrating the problem(s) that each design pattern can solve. The different shades of colors indicate the category to which the pattern belongs.

- **Source:** A. Rossi, G. Lenzini, “Transparency by design in data-informed research: A collection of information design patterns”, Computer Law and Security Review, Elsevier, 2020



# DPdD - Good and bad examples on information notices

## Privacy notices, transparency and control



Date of Birth

Occupation

Address

Post Code

**How information about you will be used**

We may share your information with credit reference agencies and other companies for use in credit decisions, for fraud prevention and to pursue debtors.

We would like to send you information about our own products and services, by post, telephone, email and SMS. If you agree to being contacted in this way, please tick the relevant boxes.

Post  Email  Phone  SMS  Automated phone call

We would also like to share your information with other selected garden products retailers so that they may send you information about their products and services by post. If you agree to your information being shared in this way, please tick the box.


If you need any further information please write to us at 10 Street Name, Town Name, County Name AB123CD.

Customer signature  Date

Simple language, clear font and style.

Clear opportunity to agree to marketing.

Prior consent sought for postal marketing by other companies.



Date of Birth

Occupation

Address

Post Code

**LEGAL DECLARATION**

*X Limited is a company incorporated in England and is a member of the X Retail Group ("the Group"). The Group ("we/us") also includes Y Limited and Z Limited and their associated companies from time to time. The personal identifiable information you provide will be processed in accordance with the Data Protection Acts 1984 and 1998 and other applicable laws. We will use your information so that we can process your order. This includes administering any accounts, processing your bank/credit card details in order to obtain payment, arranging delivery of any goods purchased, and the prevention and detection of fraud. We can hand over your information to anyone to whom we transfer our rights and duties under our agreement with you or if we have a duty to do so and the law allows us to do it. We will use your information for market research and the marketing of our products and services. This may include contacting you by post, telephone, email or SMS unless you indicate you do not want to be contacted in any of these ways by calling us on 0870 23 45 67. We will use your information to search the files of credit reference agencies who will record that search. This information may be used by other lenders in making credit decisions about you, members of your household and those with whom you may be financially linked. Information held about you by the credit reference agencies may already be linked to records relating to people with whom you are financially linked. For the purposes of credit searching, you may be treated as financially linked and you will be assessed with reference to any associated records. We will share our information with other companies, for the purposes of market research and the marketing of their products and services, unless you indicate that you wish to be excluded from such uses by contacting us on 08701 23 45 67. By signing this form you consent to the information you provide being processed for the above purposes.*

Customer Signature  Date

Confusing and legalistic language. Closely spaced text, small italic font in light grey.

Unnecessary – means little to the public.

Specific opt-in consent is required for some e-marketing and is good practice for all direct marketing.

Confusing language.

No details of what type of companies.

Bad practice to seek one consent for several types of processing.

Source: ICO



# DPbD - Good and bad example on obtaining consent for data collection



Please provide telephone numbers in case we need to contact you about your claim.

You do not have to tell us your phone number but it will help us to contact you quickly if we have a question about your claim.

Home:

Mobile:

Clear explanation of why it would be helpful to provide this information.



You must provide the following telephone numbers. It will delay your claim if you don't provide your telephone numbers.

Home:

Mobile:

Implies it is mandatory to give this information when in this case it is voluntary.

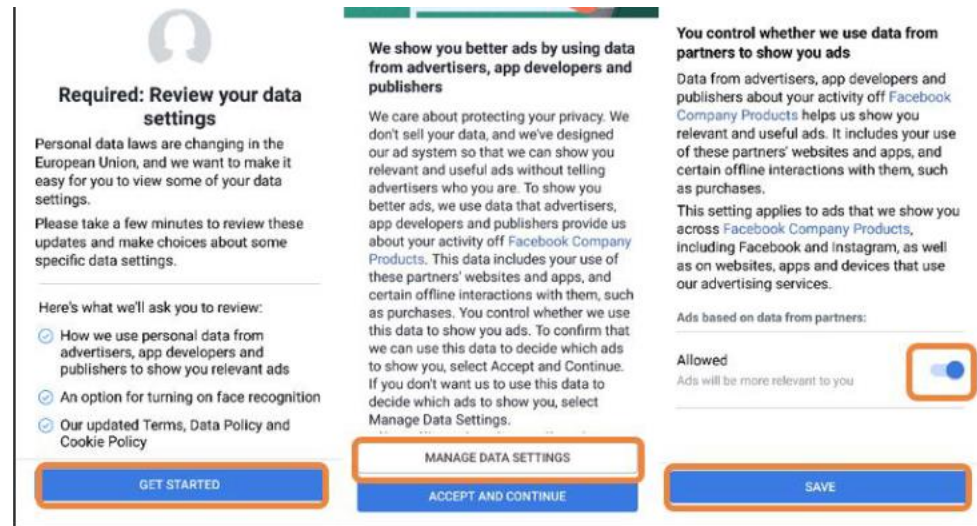
Source: ICO





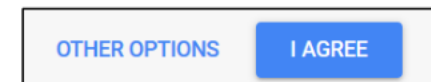
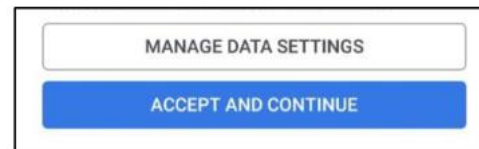
# DPdD – Bad practices on obtaining consent (“dark patterns”)

Source: “Deceived by Design” report, Norwegian Consumer Council , 2018.



Typically, opt-out consent is not correct

The user is somehow “motivated” to accept, due to the bad design





# DPbD – Trasparency (An example)

- The necessary information should be provided in the right context, at the appropriate time.
  - A general privacy policy may not be always sufficient
  - Design of information flows may be the proper way



**Source:** A. Rossi, G. Lenzini, “Transparency by design in data-informed research: A collection of information design patterns”, Computer Law and Security Review, Elsevier, 2020

An example for describing the process of revoking consent for a processing regarding research purposes

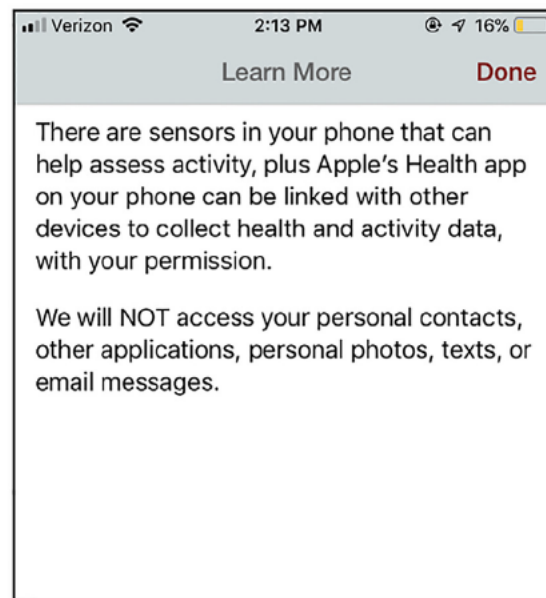
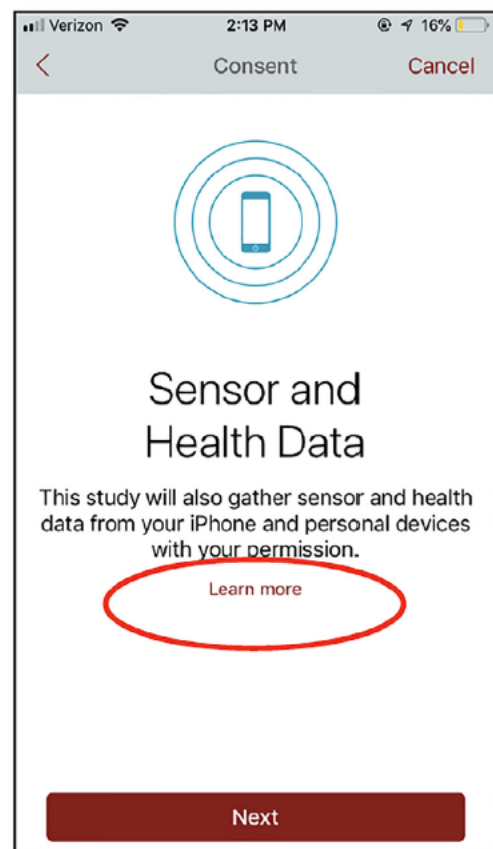


# DPbD – Fairness (An example)

- Streaming service where users may choose between a regular subscription of standard quality and a premium subscription with higher quality.
  - As part of the premium subscription, subscribers get prioritized customer service.
- With regard to the fairness principle, the prioritized customer service granted to premium subscribers cannot discriminate the regular subscribers' access to exercise their rights
  - Although the premium subscribers get prioritized service, such prioritization cannot result in a lack of appropriate measures to respond to request from regular subscribers without undue delay and in any event within one month of receipt of the requests.



# DPbD – Layered approach for transparency



Images from My Heart Counts (Stanford University)

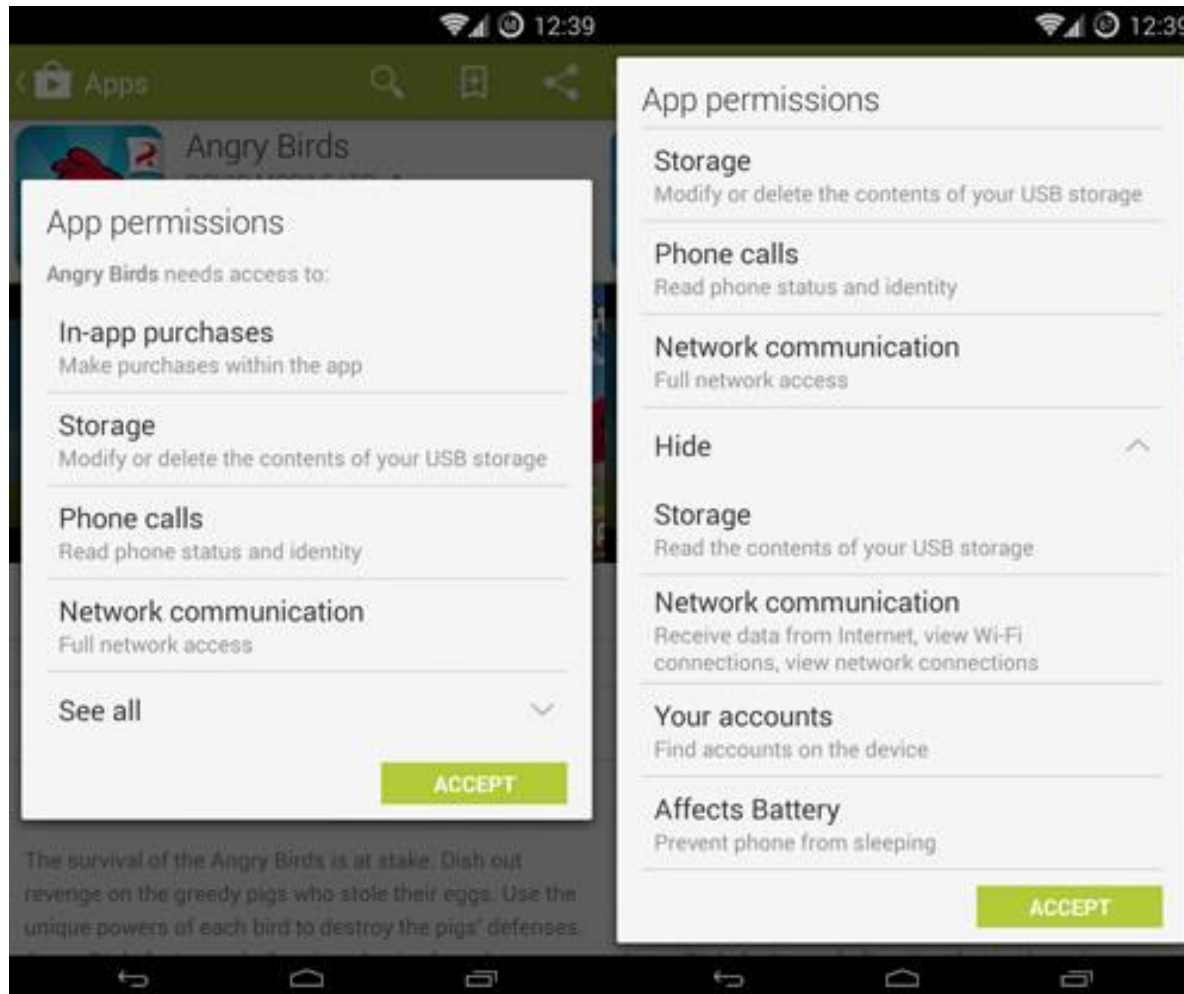
An example of a layered approach in a smart app being used for research purposes

- Consent is (indeed) the legal basis

- **Source:** A. Rossi, G. Lenzini, “Transparency by design in data-informed research: A collection of information design patterns”, Computer Law and Security Review, Elsevier, 2020



# DPbD – The permission model in smart apps

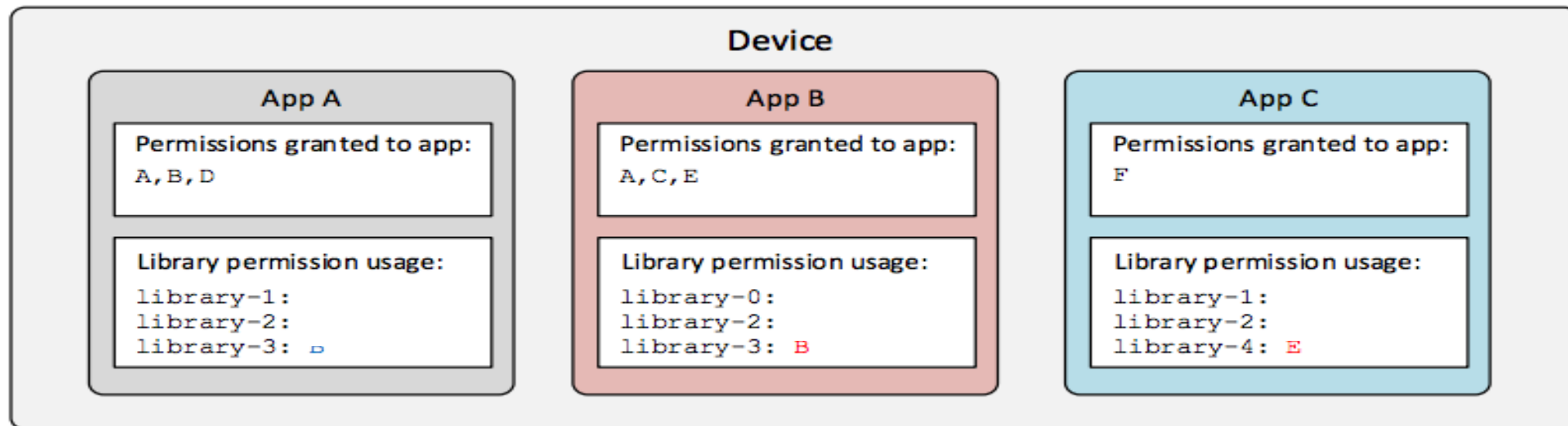


- Are all the permissions necessary?
- Are they justified?
  - Is the consent informed?
- What if the user does not grant a permission?
  - Is the consent free?
- Do other third-parties get access due to the permission granted?
  - Is the user informed on this?
  - See the intra-library collusion issue



# DPbD – The intra-library collusion issue

Source: Vincent F. Taylor, Alastair R. Beresford, Ivan Martinovic, «Intra-Library Collusion: A Potential Privacy Nightmare on Smartphones», arXiv:1808.03520, 2017.



- Library 2 is being used by apps A, B and C
- So, the library 2 provider obtains all the permissions A, B, C, D, E, F!!
  - Even if the user thoroughly examines all the permissions granted to her apps independently, she may believe that none gets all the permissions...



# Actual risks of intra-library collusion

- Libraries may abuse the privileges granted to the host applications.
  - Libraries may track the users.
  - Libraries may aggregate multiple signals for detailed user profiling.
  - => The user is not aware of these!
- 
- The developer should be very cautious on the use of third-party libraries
  - The designer should be very cautious on identifying the absolutely necessary permissions