Data Protection by Default in Identity-Related Applications

Marit Hansen

April 8, 2013

IDMAN, London

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Overview

- Towards a definition of “Data Protection by Default”
- DP by Default – general remarks
- DP by Default in practice
  - Social networks
  - User tracking on the web
  - User-controlled identity management
- Conclusion & outlook

Towards a definition of

“Data Protection by Default”

/ “Privacy by Default”

Perspective of Ann Cavoukian, promoter of Privacy by Design

"Privacy by default":

- Part of "privacy by design"
- Privacy as the default setting:
  "If an individual does nothing, their privacy still remains intact.
  No action is required on the part of the individual to protect their privacy – it is built into the system, by default."

Photo: anncavoukian.com

→ *But what about an acting individual?*

→ *Is full system functionality achievable?*

Starting point: Draft of European DP Regulation (Jan. 2012)

Article 23 (2)

Data protection by default

"The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage.
In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals."

Criticism by the EDPS (2012)

European Data Protection Supervisor
The European guardian of personal data protection

"The principle of data protection by default aims at protecting the data subject in situations in which there might be a lack of understanding or control on the processing of their data, especially in a technological context.

The idea behind the principle is that privacy intrusive features of a certain product or service are initially limited to what is necessary for the simple use of it.

The data subject should in principle be left the choice to allow use of his or her personal data in a broader way."

Jan Philipp Albrecht (Rapporteur of the EU Parliament): Draft Report (Jan. 2013) – 1/2

Photo by Mathias Schindler

Data protection by default:

1. the default by the controller when the data subject is given a choice, and

2. the default of applying "data protection by design" by data processors and producers to ensure the privacy-compliant use by controllers

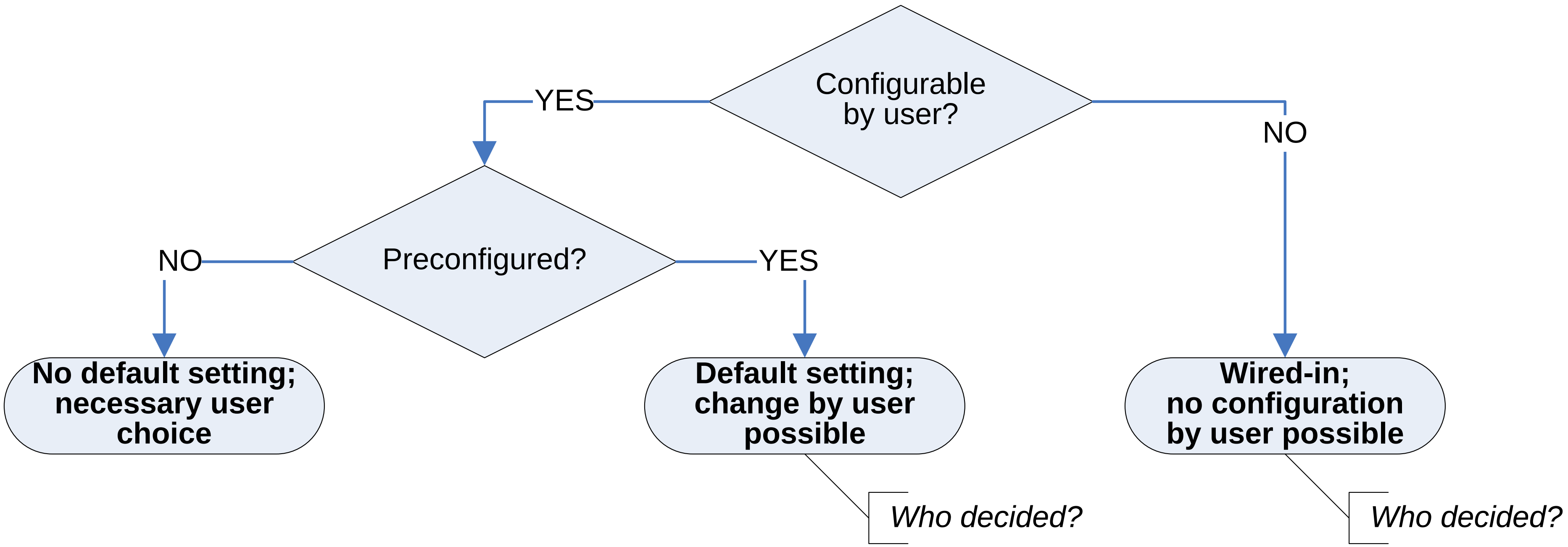
Not only for the data necessity principle,
but for all data protection principles
(e.g. data minimization, transparency, intervenability)

“Data Protection by Default”

– general remarks

Three cases for “(pre-)configurability”

Functionality/ behaviour


Configurable by user?

YES

Preconfigured?

NO

No default setting; necessary user choice

YES

Default setting; change by user possible

Who decided?

NO

Wired-in; no configuration by user possible

Who decided?

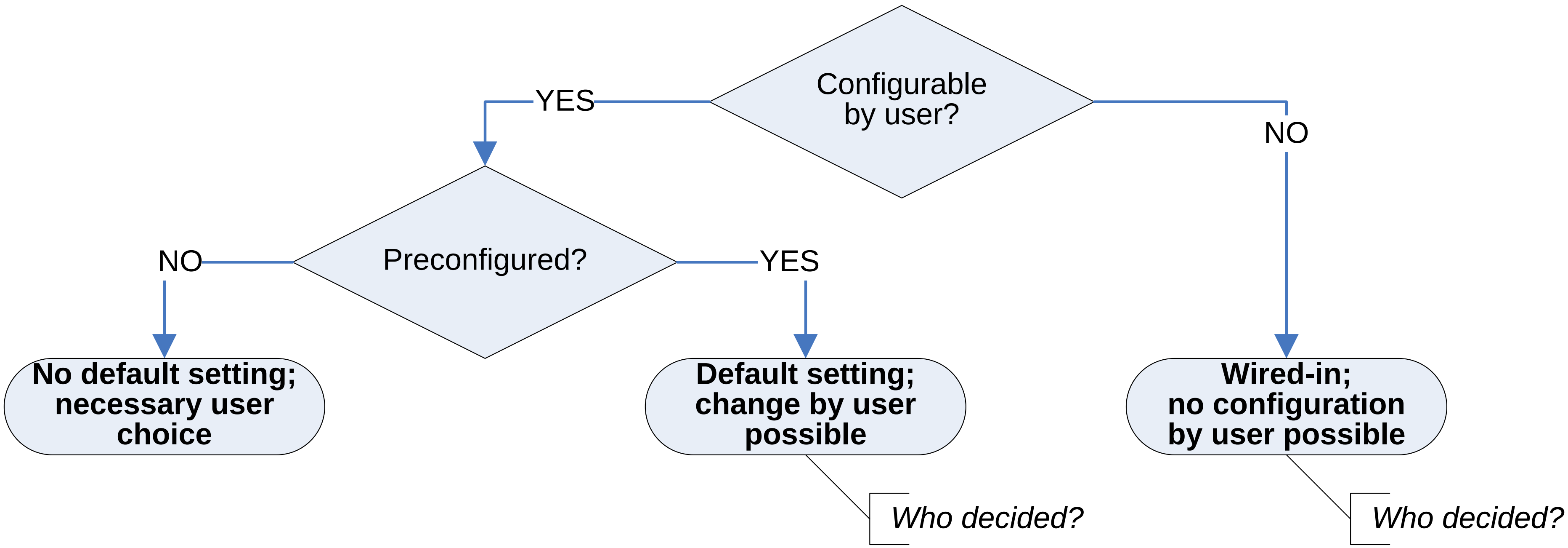
Decreasing configurability

Usually: decreasing configuration by user

Potentially: decreasing transparency / user understanding

Three cases for “(pre-)configurability”

Functionality/ behaviour



Configurable by user?

YES

NO

Preconfigured?

NO

YES

No default setting; necessary user choice

Default setting; change by user possible

Wired-in; no configuration by user possible

Who decided?

Who decided?

Ex.: choice of payment system

Ex.: anonymous use, no tracking

Ex.: encrypted communication

Two different types of configuration

1. Configuration of a process necessary for the purpose within the application

Not so easy answer on the best default
– depending on the functionality

2. Configuration of an additional process that is not strictly needed for the original functionality (≠ “simple use”)

Easy answer: Default = “NO”
if additional purpose / party / personal data processing

Checks for defaults w.r.t. necessary processes

Check:

- What do users expect?
  - In general?
  - On a more individual base?

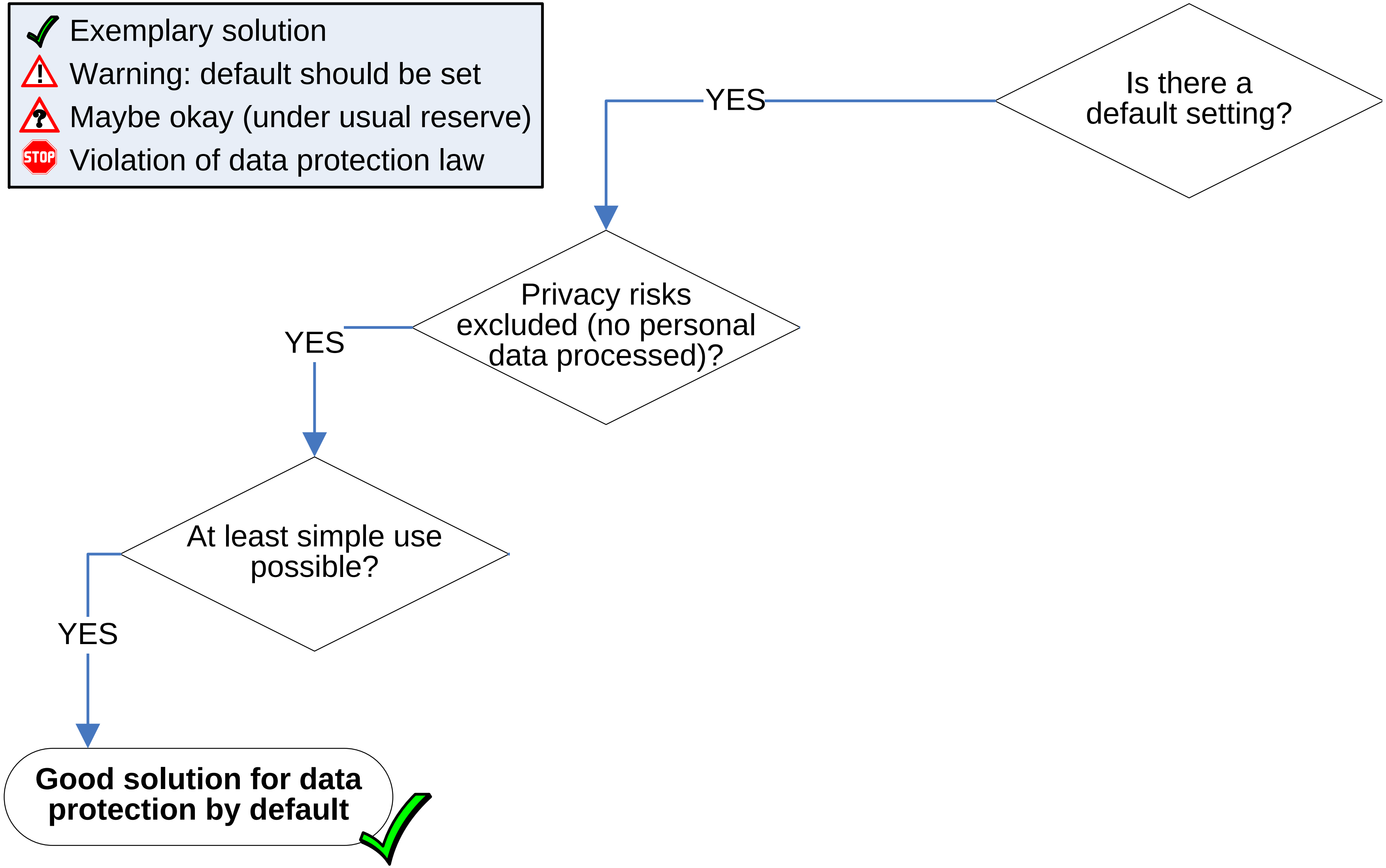
Granularity?
Usability?
User guidance?

- Where is user interaction necessary?
  - To decide on important parameters
    - Where to process data? Which jurisdiction?
    - Which additional parties?
    - Costs?
  - E.g.: choice of payment system
  - E.g.: choice of cloud storage location

"One size fits all" doesn't work here

Assessment: 1) Good default

- ✓ Exemplary solution
- ⚠ Warning: default should be set
- ⚠ Maybe okay (under usual reserve)
- 🛑 Violation of data protection law



Is there a default setting?

YES

Privacy risks excluded (no personal data processed)?

YES

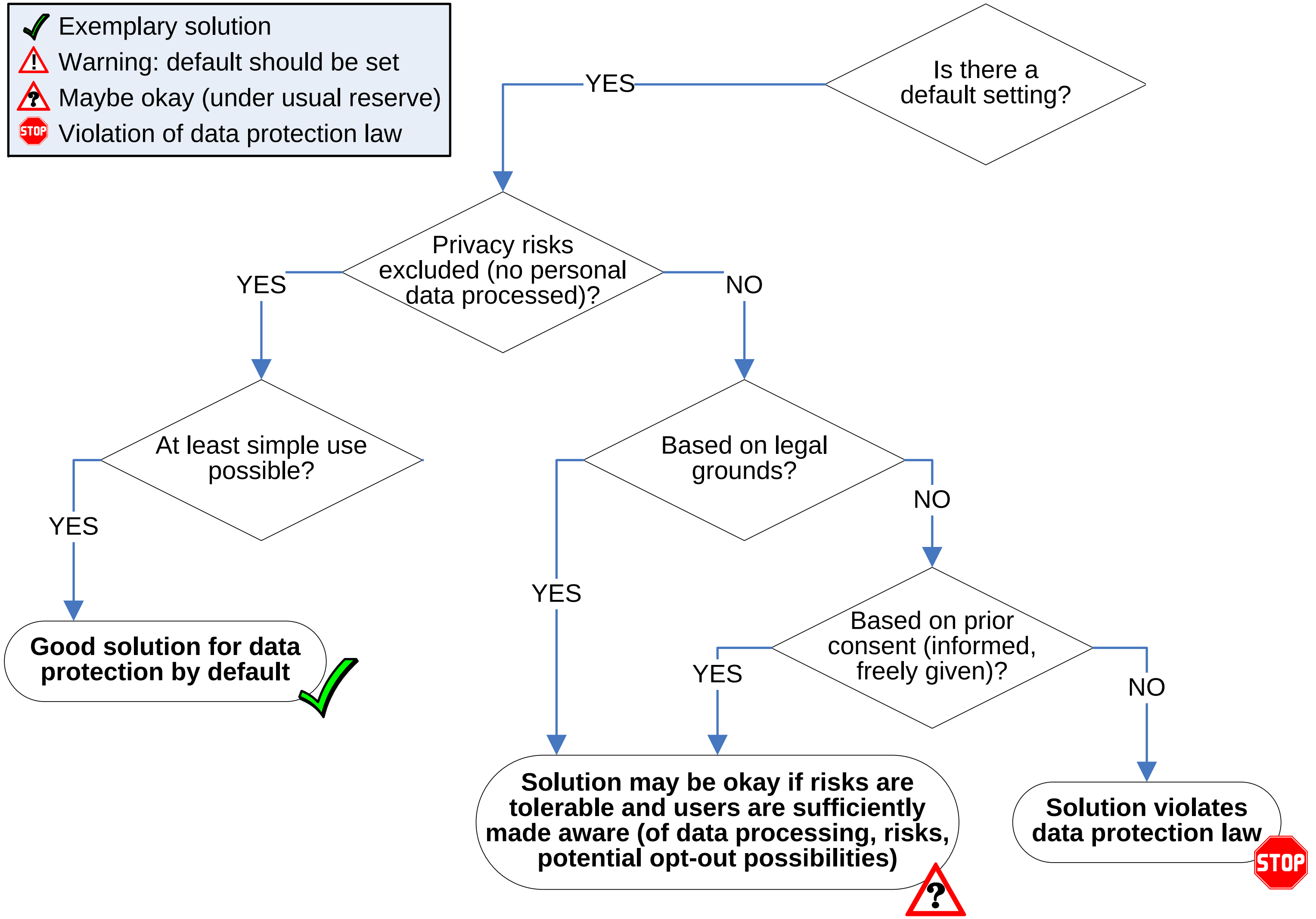
At least simple use possible?

YES

Good solution for data protection by default ✓

Assessment: 2) Default, but risks remain

- ✓ Exemplary solution
- ⚠ Warning: default should be set
- ⚠? Maybe okay (under usual reserve)
- STOP Violation of data protection law



Is there a default setting?

YES

Privacy risks excluded (no personal data processed)?

YES

At least simple use possible?

YES

Good solution for data protection by default ✓

NO

Based on legal grounds?

YES

NO

Based on prior consent (informed, freely given)?

YES

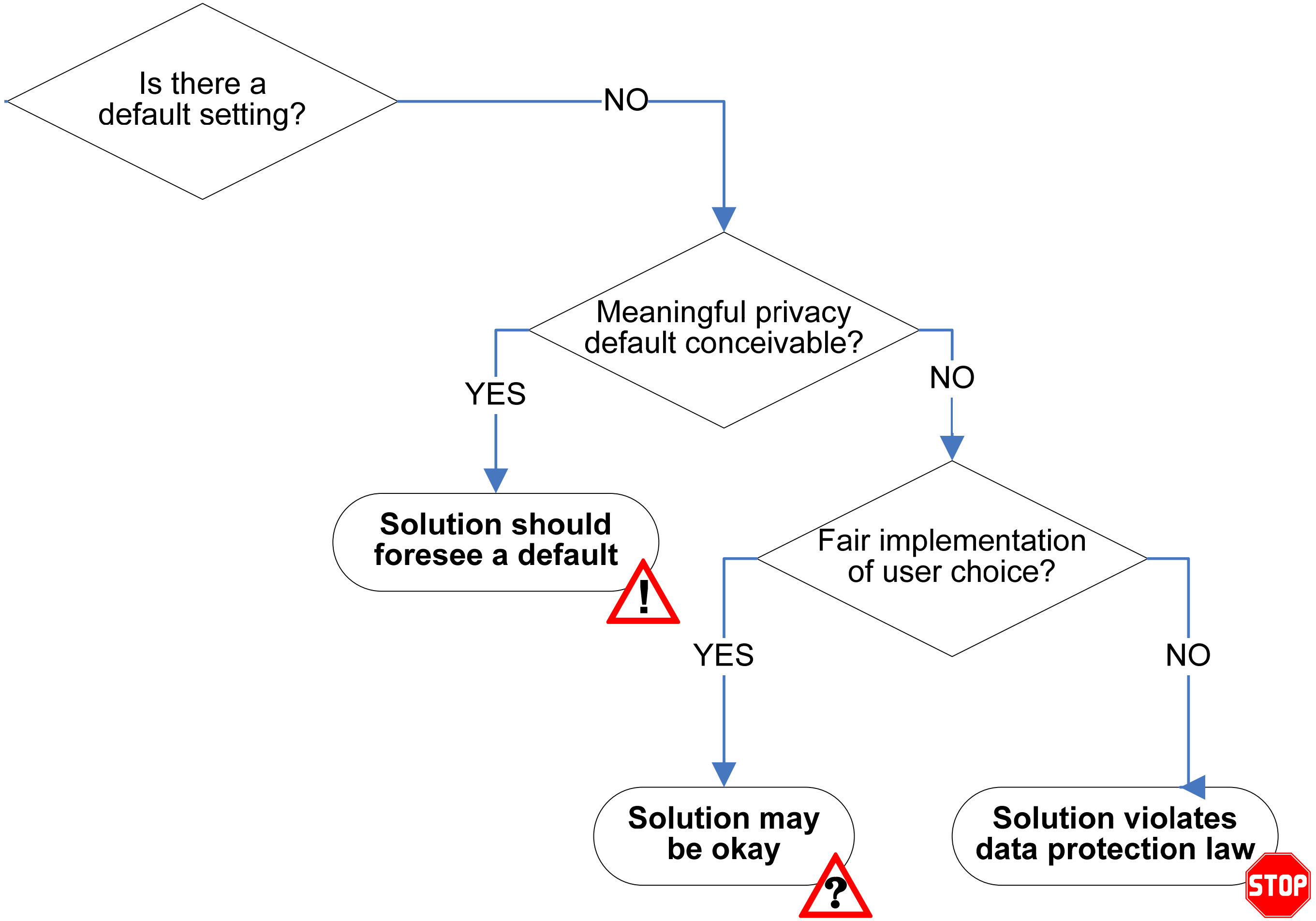
Solution may be okay if risks are tolerable and users are sufficiently made aware (of data processing, risks, potential opt-out possibilities) ⚠?

NO

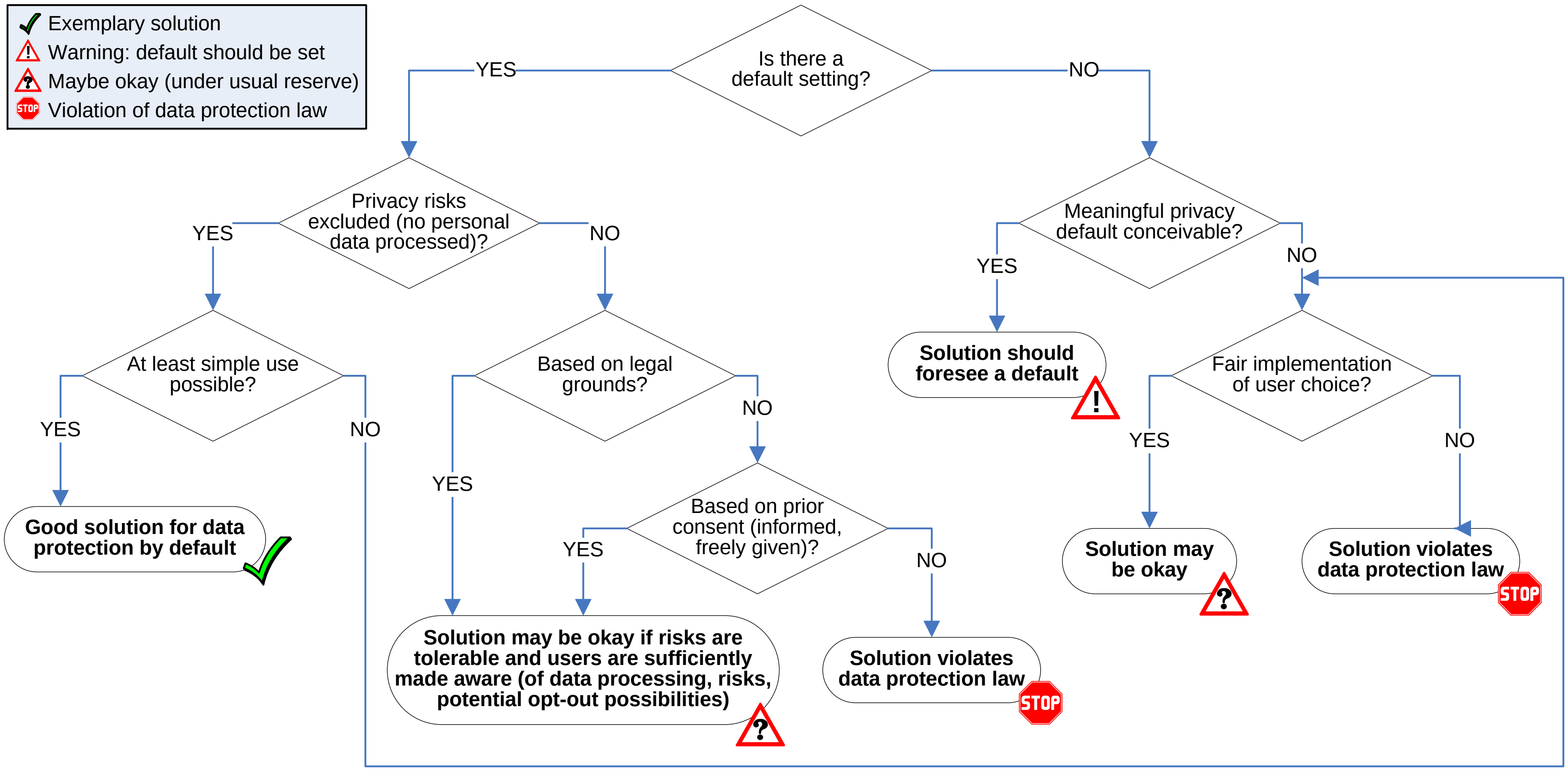
Solution violates data protection law STOP

- ✓ Exemplary solution
- ⚠ Warning: default should be set
- ⚠? Maybe okay (under usual reserve)
- STOP Violation of data protection law

Assessment: 3) No default


Is there a default setting?
NO
Meaningful privacy default conceivable?
YES
NO
Solution should foresee a default
!
Fair implementation of user choice?
YES
NO
Solution may be okay
?
Solution violates data protection law
STOP

The full picture: assessing potential default settings



✓ Exemplary solution
⚠ Warning: default should be set
⚠? Maybe okay (under usual reserve)
🛑 Violation of data protection law

Is there a default setting?

YES

Privacy risks excluded (no personal data processed)?

YES

At least simple use possible?

YES

Good solution for data protection by default ✓

NO

NO

Based on legal grounds?

YES

NO

Based on prior consent (informed, freely given)?

YES

Solution may be okay if risks are tolerable and users are sufficiently made aware (of data processing, risks, potential opt-out possibilities) ⚠?

NO

Solution violates data protection law 🛑

NO

Meaningful privacy default conceivable?

YES

Solution should foresee a default ⚠

NO

Fair implementation of user choice?

YES

Solution may be okay ⚠?

NO

Solution violates data protection law 🛑

“Data Protection by Default”

in practice

DP by Default for Social Networks

Starting from firewall rule “deny all”

- No personal data unless entered by user herself
  - Including: no biometric analysis of photos as default
- Entries only visible for oneself unless changed by user
  - Next level: only friends (not friends-of-friends …)

Usually discussion only covers relation “user – other users”, NOT “user – service provider(s)”

Check:

- Is simple use possible?
- Is setting easily changeable without giving up all protection?
- Stricter settings for children?

DP by Default for user tracking

W3C Standardization on "Do Not Track"

- 3 values expressed by user browser:
  - 1: user does not want to be tracked
  - 0: user consents to being tracked
  - "null": user has not expressed a preference
- What if a browser is rolled out with "1"? – MS IE 10
  - "1" is appropriate default from privacy perspective
  - Threat of ad industry to ignore all "no tracking" values sent from the browser
  - Now: users are asked to set value at install

DP by Default for user-controlled IdM

- Focus on self-determination,
  i.e. user should be able to control her system

- Baseline: no personal data disclosure
  - Requires additional “privacy by design” functionality

- Working with personas (partial identities, pseudonyms)
  - Maximum privacy: no re-use of personas
  - But: mostly not in line with user expectations,
    i.e. by default new persona with every new contact

Conclusion

- “DP by Default” not well defined
- Distinguish configuration of
  - options for necessary functionality and
  - add-on functionality (default = “NO”)
- No overall accepted privacy metrics to determine best default – localized defaults?
- Check:
  - User expectations (in general / individual)?
  - User’s awareness / interaction required?
  - Fair user information and choice?

Outlook

- Clarification is needed:
  - Should “DP by Default” mean “best privacy” or rather “legal compliance”?
  - Related: privileges for pseudonymous data?

- Open issues:
  - How can “configuration providers” step in?
  - How to prevent “take it or leave it” effect for devices with constraints concerning displays and user interaction (e.g. tablets, Smart TV, ubiquitous computing)?
  - How to guide and educate users (understanding and self-determination instead of blind trust)?

Thank you for your attention!

Marit Hansen
marit.hansen@privacyresearch.eu

ABC4TRUST

FutureID

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein