PrimeLife / IFIP Summer School

Necessary processing of personal data

The need-to-know principle and processing data from the new German identity card

Harald Zwingelberg

PrimeLife

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

The new German eID: Neuer Personalausweis (nPA)

Picture: *Bundesministerium des Innern - BMI*

specific sensitivity of governmentally verified personal data

- data are proven and confirmed by governmental body

- upside:
  more trust for business and other transactions,
  safeguard against identity fraud

- downside:
  potential new privacy threat as it may become hard or impossible to remain anonymous, use self chosen pseudonyms or other means of identity management

some privacy properties of the nPA

- reciprocal identification: identification of both parties
- user control: user client will display data that will be transferred and allows opting out by data category
- pseudonyms (service and card specific pseudonym)
- accessing data requires an access certificate and allows access only to **data necessary** for a given purpose

attaining an access certificate

two-step process

1. authorisation by the federal public authority Bundesverwaltungsamt (BVA) checking:
   - legally allowed purpose
   - purpose is not businesslike trade with personal data
   - necessary data processing for purpose
   - data security requirements met
   - no indication for abusive deployment of the certificate
2. with authorisation an access certificate can be attained with one of the accredited trust centres

necessary data processing

requirement in European privacy legislation

- only the minimum of personal data that are required for a stated purpose may be processed

problems of this definition

⇒ law allows for wide definition of purposes

⇒ purposes often require legal interpretation

⇒ purpose is central point to test the necessity

examples:

⇒ purpose "insurance contracts"

⇒ "negotiation and conclusion of a travel (luggage) insurance online"

defining purposes

- applicants must define and sketch the purpose for attaining an access certificate for the nPA

- issues of too wide definitions
  - would allow too much processing
  - "buying and selling goods and providing services to individuals"
- issues of too narrow definitions
  - may restrict processing too much
  - for nPA: multiple certificates necessary for what would naturally be understood to be a single occurrence

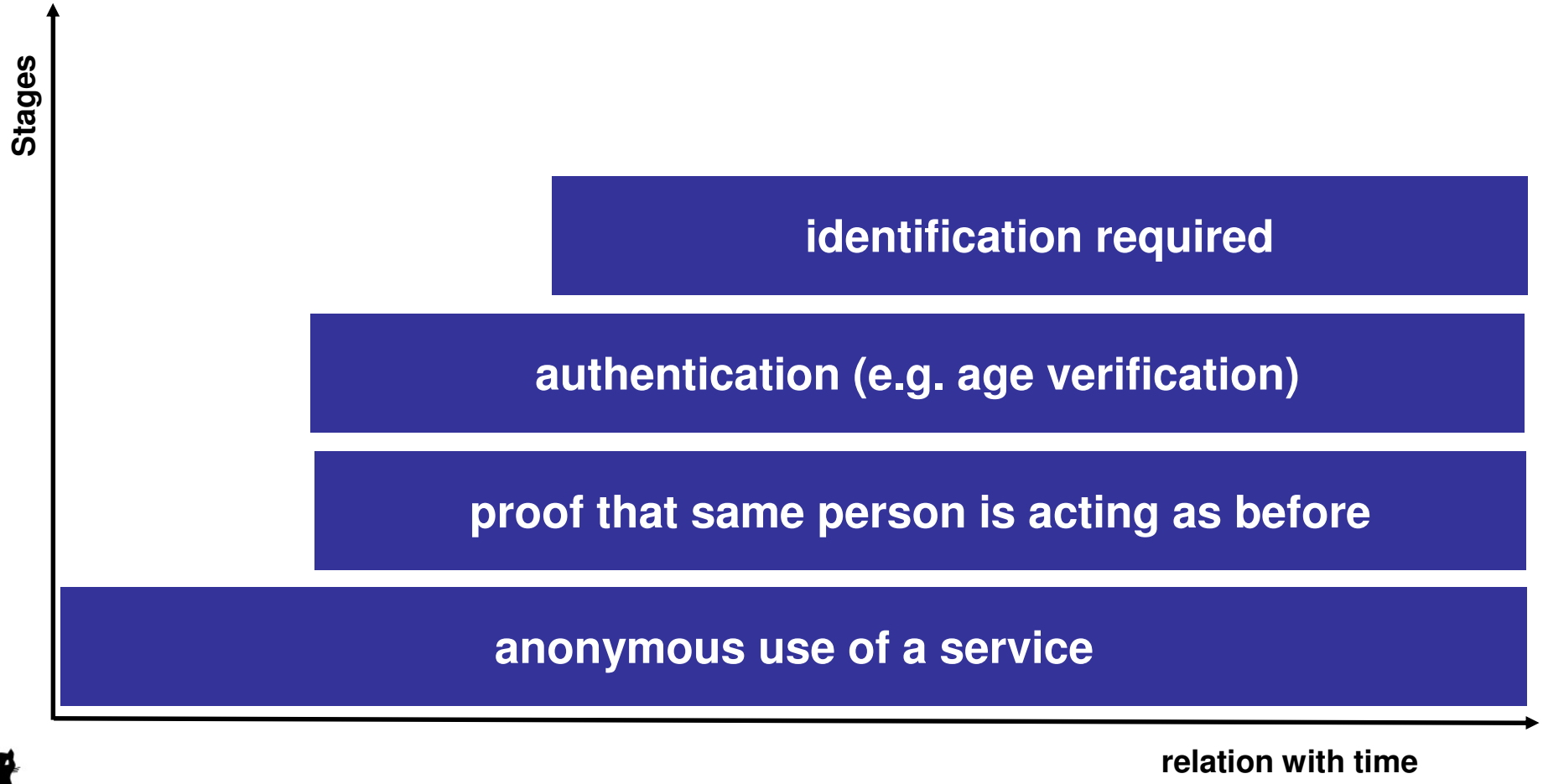
differences to 'normal' necessary processing

- for processing of personal data stored on a nPA the necessity must be proven towards the authority issuing the authorisation
- an informed consent of the holder does not suffice – it is required by the client software anyway for each transaction
- legal interpretation: it is OK when identification is eventually necessary at a later time, e.g. for a lawsuit

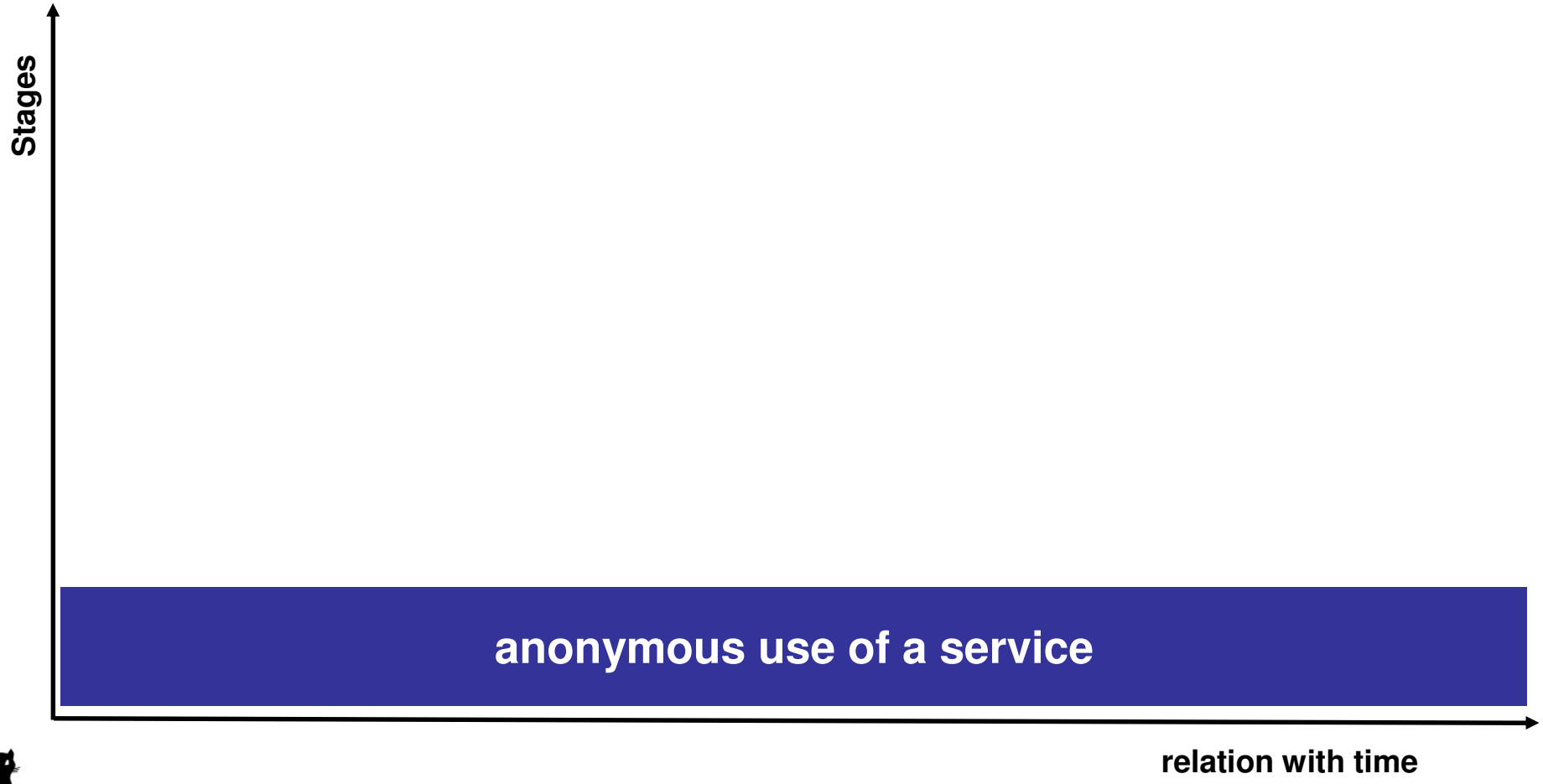
consequence

- it is not sufficient when data is merely required for setting up a user profile – here the holder may use pseudonyms

assessing necessity: staged approach



anonymous use of services



anonymous use of services

setting

- surfing websites
- holder only seeks information about goods or a service or consumes free services

consequences / solutions

⇒ no collection of verified data from the nPA

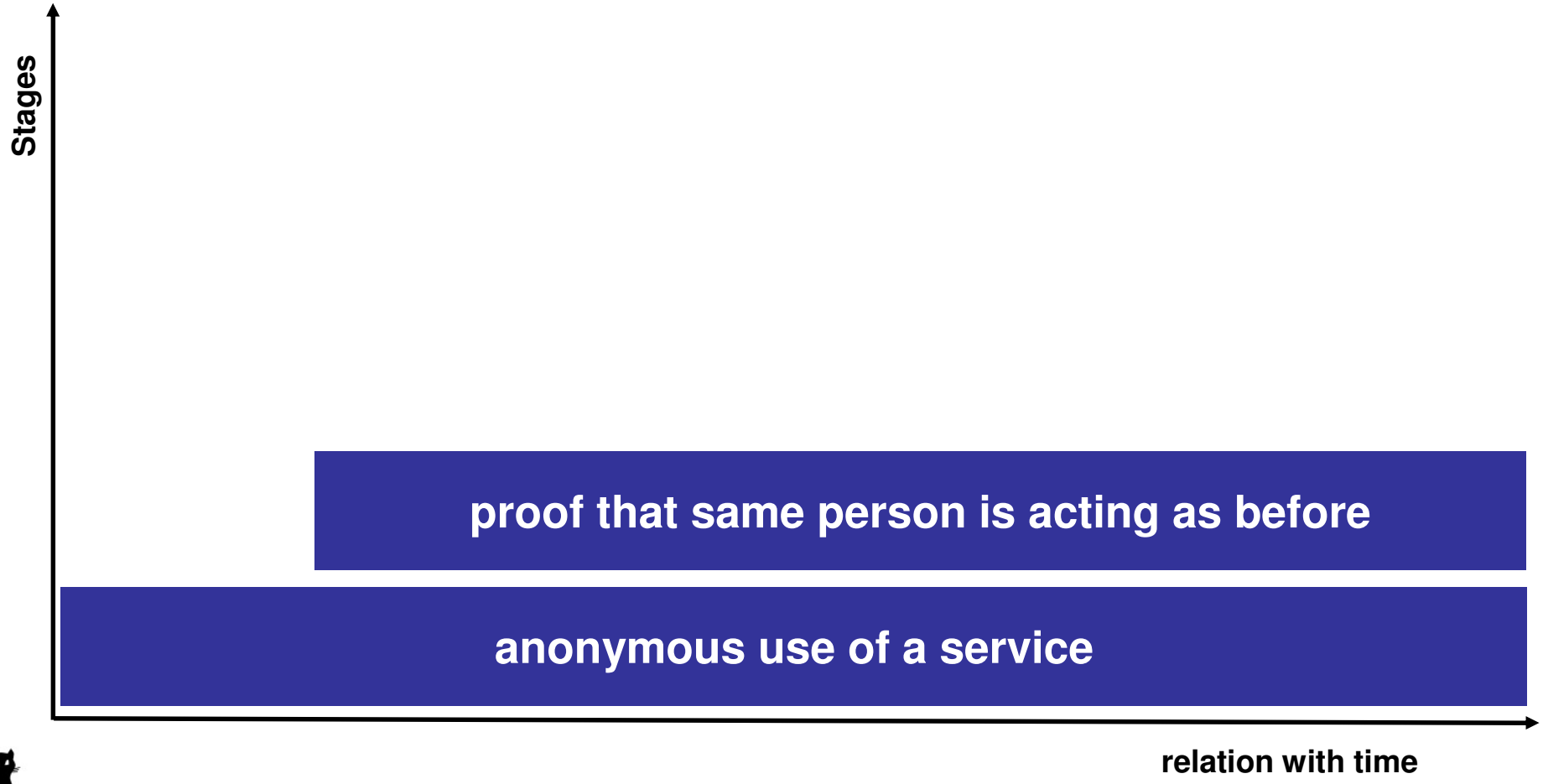
⇒ no identification of the user / holder allowed *

⇒ no tracking services (e.g. Google Analytics) *

⇒ identifying persons requires their prior (!) consent *

* European / German law applicable & DPA's understanding of these rules

same person acting



same person acting

setting

- proof is required that same person is acting
- e.g. applying for an insurance contract being calculated based on data provided
- resuming negotiations, transactions

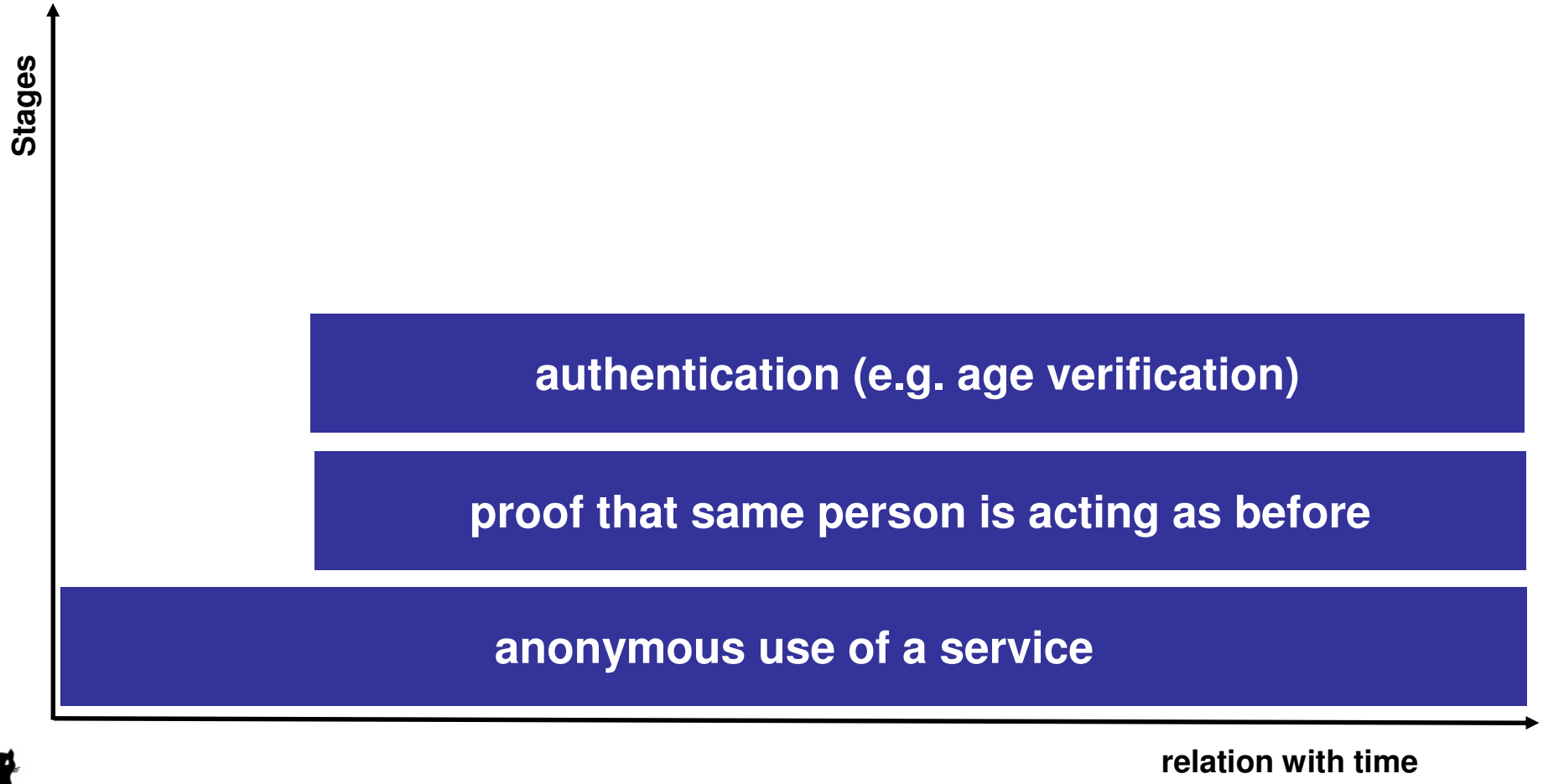
consequences / solutions

⇒ nPA: use of pseudonym function is sufficient

⇒ web: use of cookies, username/password

⇒ collection of name, address is <u>not</u> yet necessary

authentication required



authentication

setting

- authentication required to access a service or goods
- e.g. accessing free but age-restricted videos or previews
- proof of being domiciled in a certain municipality to access service reserved for its citizens

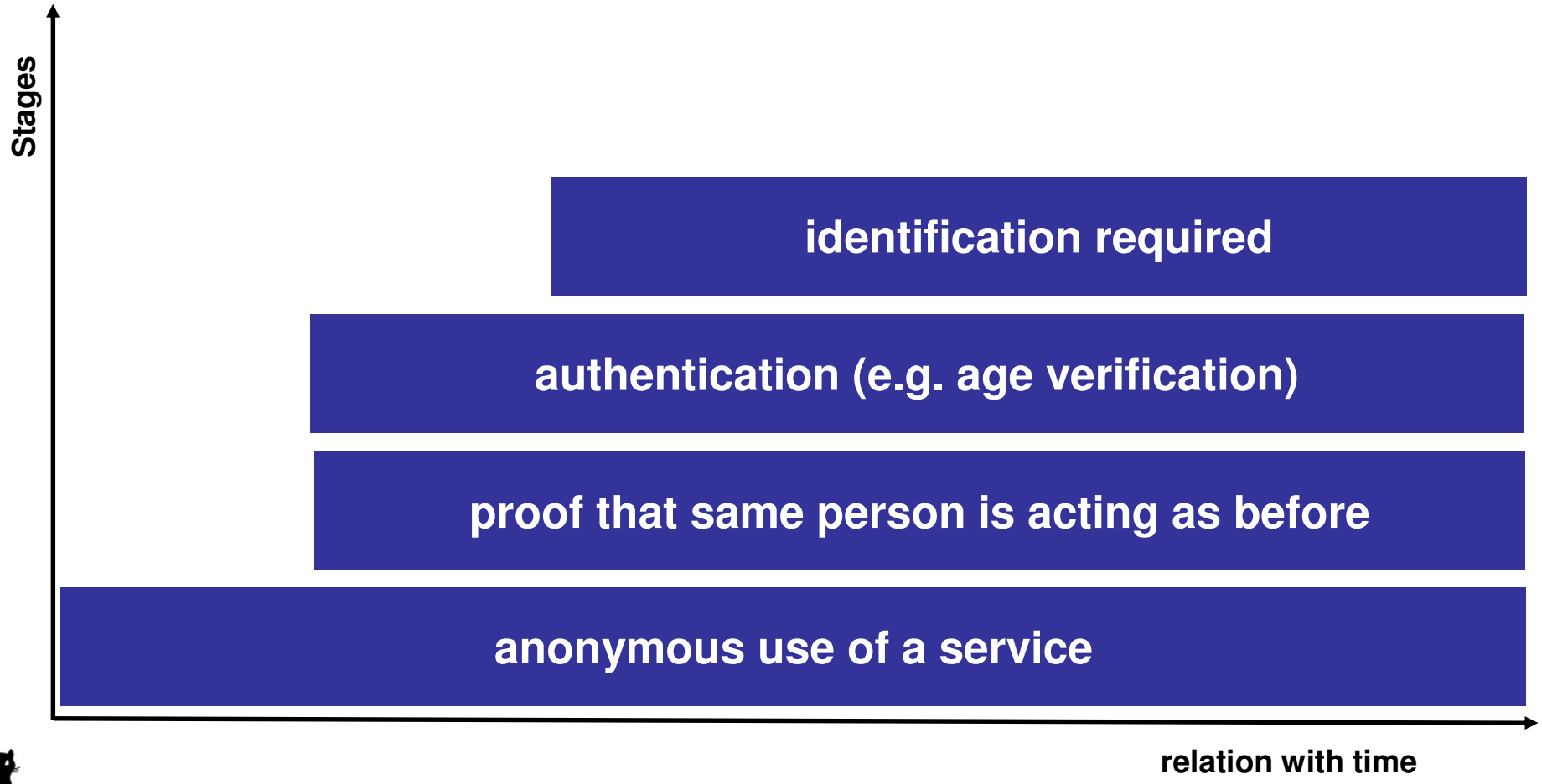
consequences / solutions

⇒ nPA: use of anonymous credentials for age & domicile

⇒ offline: use full identity, e.g. ID card

⇒ third parties checking and attesting the correctness of the claim (Postident, adultcheck)

identification required



identification required

setting

- risk of financial loss requires the collection of information for filing a lawsuit and enforcement thereof
- legal requirement to identify a person (money laundering)

consequences / solutions

⇒ nPA: collection of name, address, date of birth, place of birth is allowed (depends on civil procedural law)

⇒ nPA: collection of data required by law

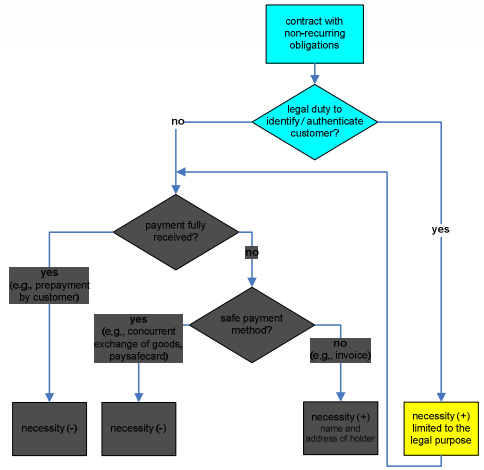
possible privacy preserving development

⇒ identification only when really needed (revocation of anonymity), e.g. for civil process

use cases

- The model with the staged approach has been applied to several use cases
  - legal requirement for authentication / identification
  - credit risk at contracts with non-recurring obligations
  - credit risk at a contract with recurring obligations or contracts that last over a time span
  - right of access to personal data

contract with non-recurring obligations



contract with non-recurring obligations

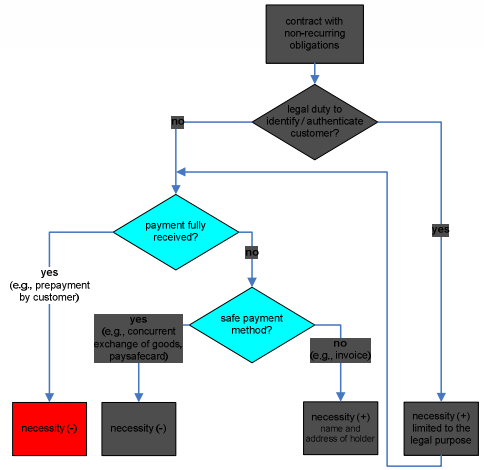
legal duty to identify / authenticate customer?

no

payment fully received?

yes
(child protection, telecommunication, money laundering)

necessity (+) limited to the specific legal purpose



no legal duty to identify / authenticate a user or requirement fulfilled

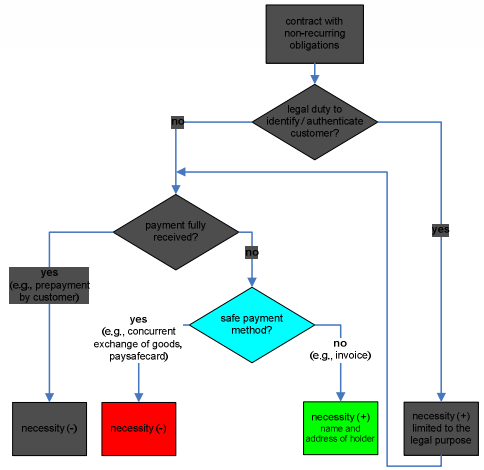
payment fully received?

yes (e.g. prepayment by customer)

necessity (-)

no

safe payment method?



payment not fully received

safe payment method?

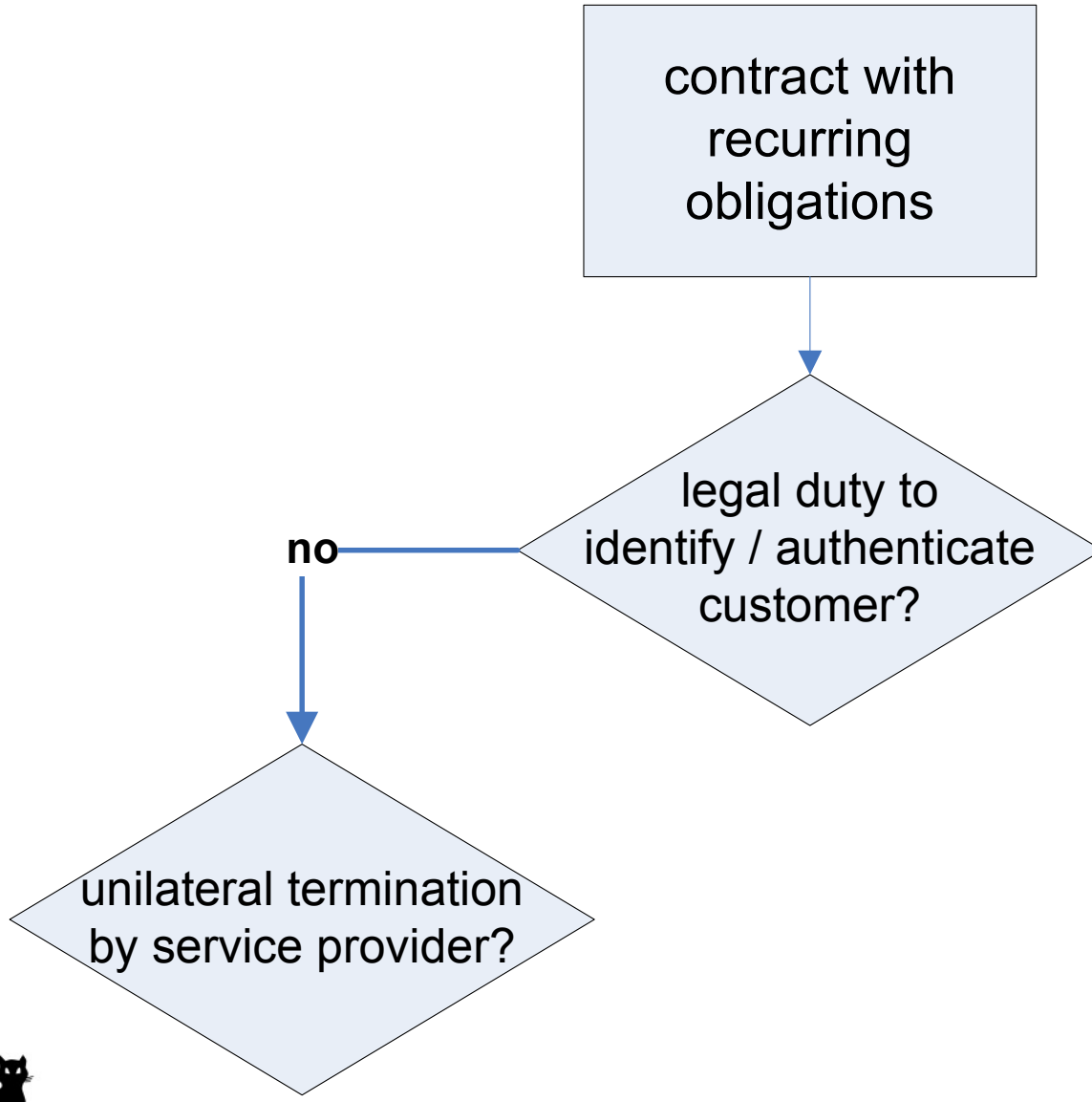
yes
(e.g. concurrent exchange of goods, paysafecard, guaranteed by third party)

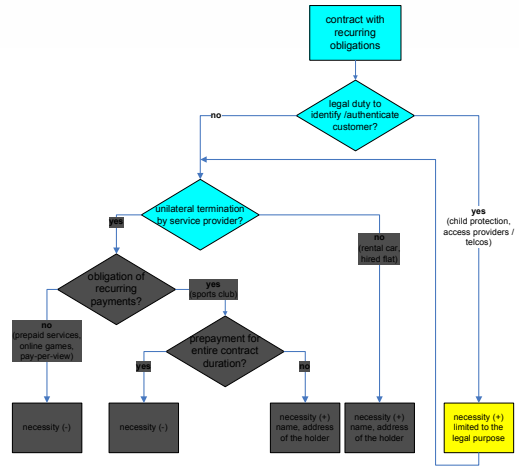
necessity (-)

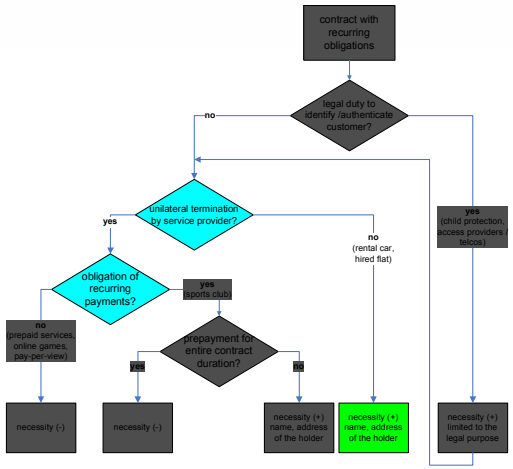
no
(e.g. invoice, possibility to claim back payment)

nPA-access (+) name and address of bearer

contract with recurring obligations


contract with recurring obligations
legal duty to identify / authenticate customer?
no
yes
(child protection, telecommunication, money laundering)
unilateral termination by service provider?
necessity (+) limited to the legal purpose


contract with recurring obligations
legal duty to identify /authenticate customer?
no
yes
(child protection, access providers / telcos)
unilateral termination by service provider?
yes
no
(rental car, hired flat)
obligation of recurring payments?
yes
(sports club)
no
(prepaid services, online games, pay-per-view)
prepayment for entire contract duration?
yes
no
necessity (-)
necessity (-)
necessity (+) name, address of the holder
necessity (+) name, address of the holder
necessity (+) limited to the legal purpose



no legal duty to identify / authenticate a user or requirement fulfilled

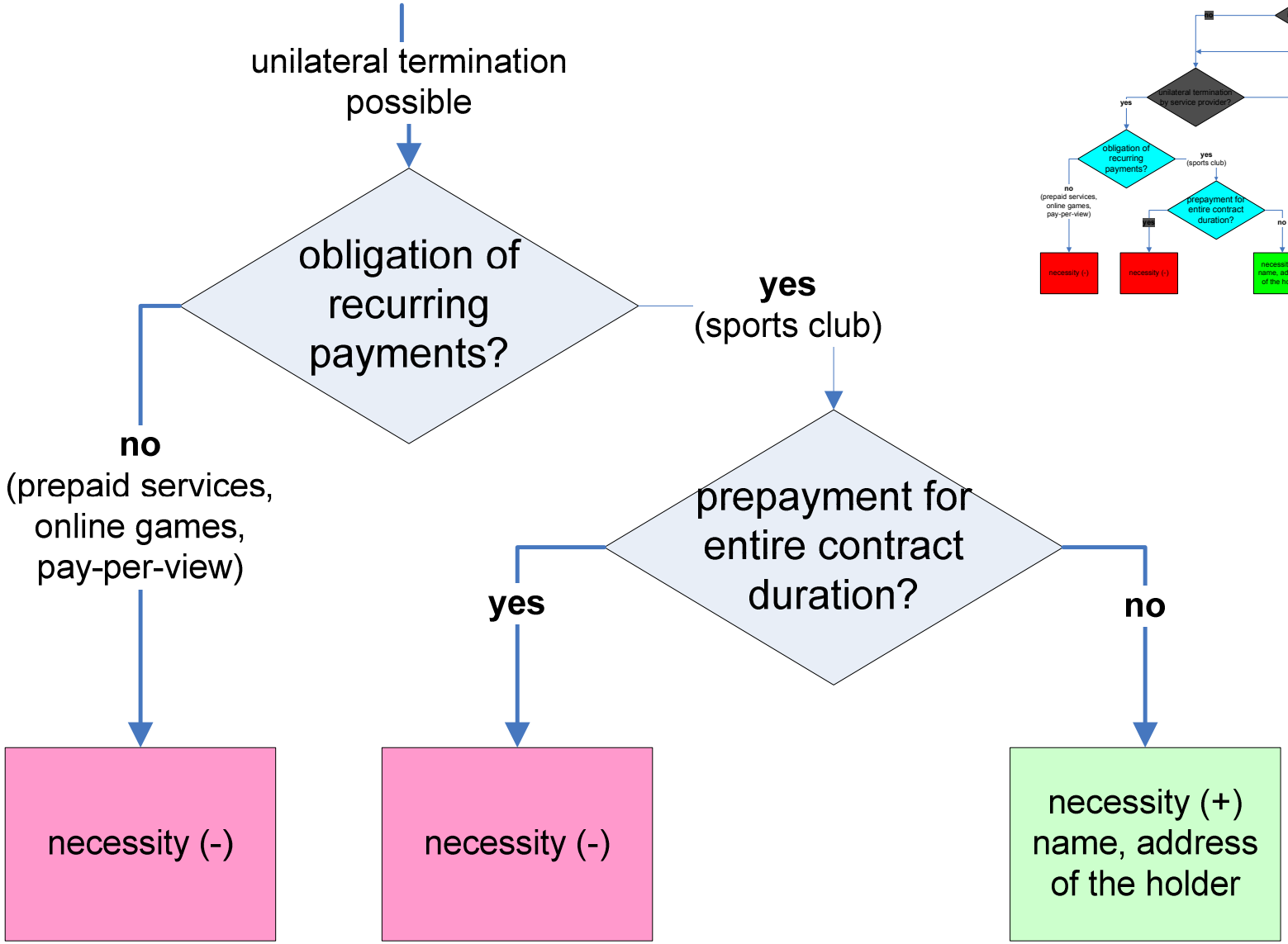
unilateral termination by service provider?

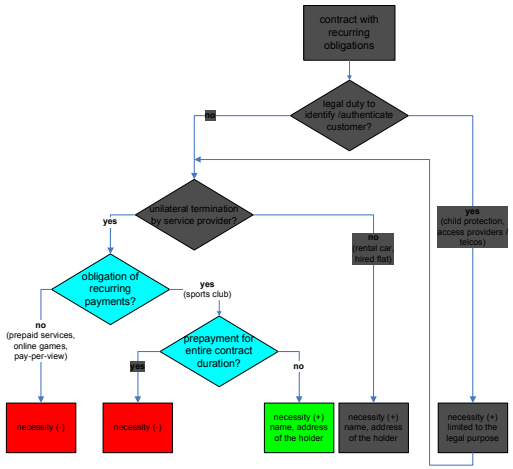
yes (blocking customer is possible)

obligation of recurring payments?

no (rental car, hired flat)

necessity (+) name, address of the holder


unilateral termination possible
obligation of recurring payments?
no
(prepaid services, online games, pay-per-view)
yes
(sports club)
prepayment for entire contract duration?
yes
no
necessity (-)
necessity (-)
necessity (+) name, address of the holder


contract with recurring obligations
legal duty to identify /authenticate customer?
unilateral termination by service provider?
yes
no
(rental car, hired flat)
yes
(child protection, access providers / telcos)
obligation of recurring payments?
yes
(sports club)
no
(prepaid services, online games, pay-per-view)
prepayment for entire contract duration?
yes
no
necessity (-)
necessity (-)
necessity (+) name, address of the holder
necessity (+) name, address of the holder
necessity (+) limited to the legal purpose

usefulness of considerations

What is the value of these considerations?

- the Bundesverwaltungsamt (BVA) issuing the access credentials will base decision upon this work
- first analysis of the necessity of data processing on a broader basis (at least in German legal literature)
- first analysis referring to specialities of the nPA
- may be useful for other areas – also within PrimeLife

"Vacation in Wolf Land"

Questions, comments, suggestions?

contact:
Harald Zwingelberg
ULD65@datenschutzzentrum.de
www.datenschutzzentrum.de
+49 (0)431 / 988-1228

PrimeLife

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein