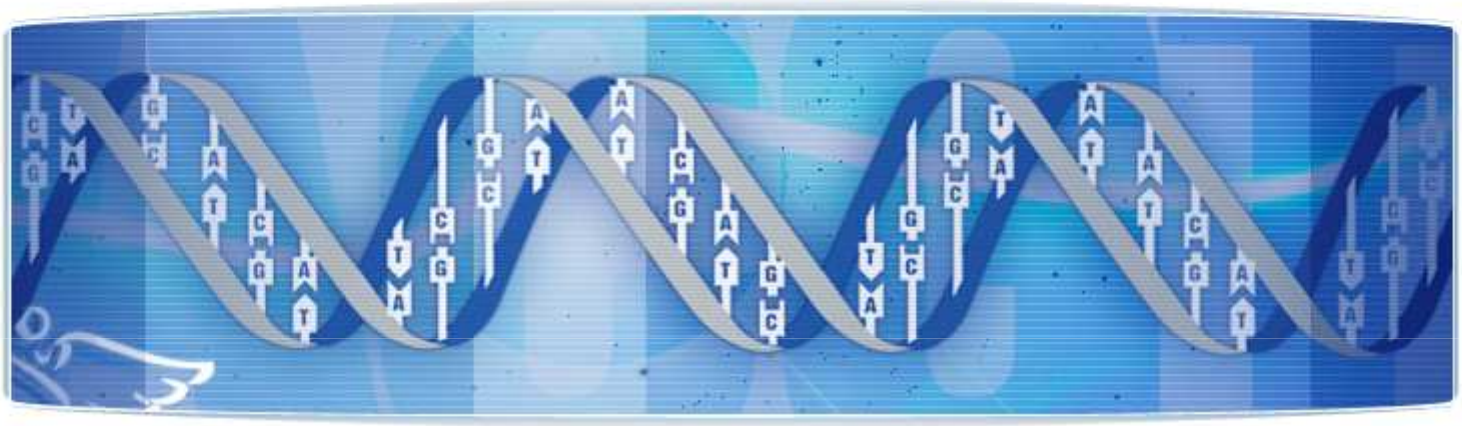
ACGT
Advancing Clinico Genomic Trials on Cancer



Laws, ethics and security for networked medical data

Tina Krügel
Institute for Legal informatics, Germany

Sapporo, 14. September 2009

http://www.eu-acgt.org

Information Society and Media

The ACGT project (FP6-2005-IST-026996) is funded by the European Commission Information Society and Media DG under the 6th Framework Programme.

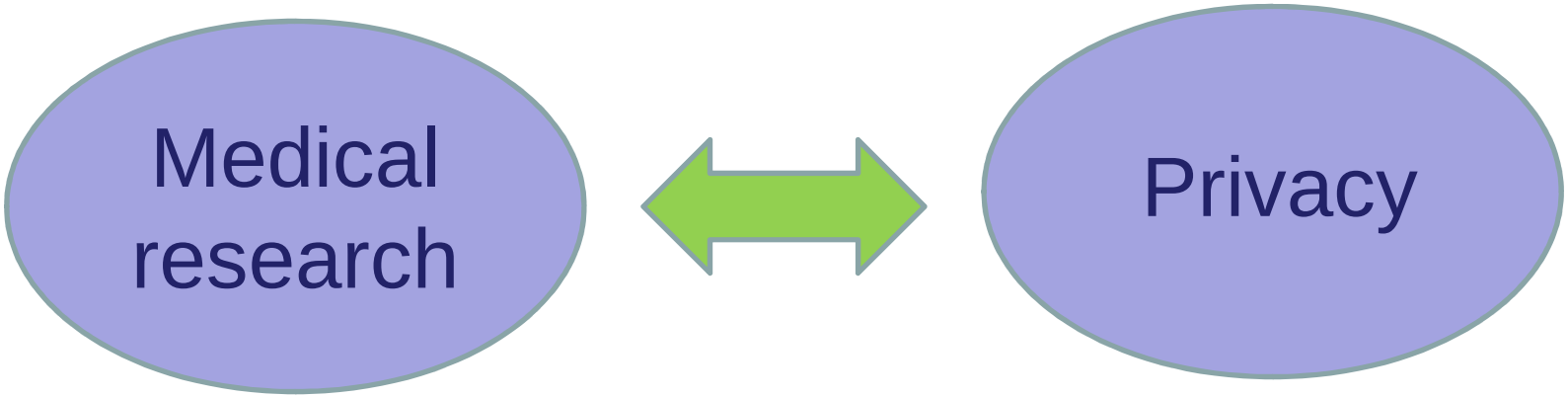
Data protection regarding human genetic research

- Institute for Legal Informatics
- Motivated by ACGT
- WP-leader Ethical, Legal and QA-issues
- Building up of a *Data Protection Framework*

The problem about genetic data

- Unique
- Provides information about
  - descent
  - ethnical origin
  - future diseases and their healing chances
  - …
- Relevance for blood relatives (even unborn)
- Sensitive data (Art. 8 (1) Directive 95/46/EC)

Value conflicts



Balance

→ Need for a

Data Protection/Data Security Framework

Principles of the proposed Data Protection Framework

- Processing of anonymous data
- Data Protection Authority
- Binding contracts
- Informed consents as first fall-back-scenario and for ethical reasons (patient autonomy)
- Allowing re-identification

Processing of anonymous data

- It is essential to work with as much anonymous data as possible within genetic research projects:
  - Patient's privacy is protected best
  - For the processing of anonymous data Data Protection Legislation is NOT applicable

But: Genetic data = personal data?

- Genetic data is unique.
- Genetic data is potentially personal data, as the identification of the data subject is always possible if the controller has additional knowledge (for example reference templates).
- Even though researchers work with data they can not refer to the data subject, this data in fact is only pseudonymized, not anonymous

Data protection regarding human genetic research

Art. 2 Dir. 95/46/EC

'Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); **an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number** or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

Data protection regarding human genetic research

Recital 26 Dir. 95/46/EC

Whereas the **principles of protection** must **apply** to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the **means likely reasonably to be used either by the controller or by any other person** to identify the said person; whereas the principles of protection shall **not apply** to data **rendered anonymous** in such a way that the data subject is no longer identifiable; …

Pseudonymous = de-facto anonymous?

- Wording of Directive: no
- Meanwhile change in opinion on the European level
- Anonymous, if the effort for identification is disproportionate with respect to the effort of time, money and manpower
- De facto anonymous data = anonymous data
  → Relevant factor: effort for identification
- For researchers (e.g. within the ACGT project) it might be disproportionate to attribute the information to a person, if he/she does not have the link → no personal data ?

Conditions:

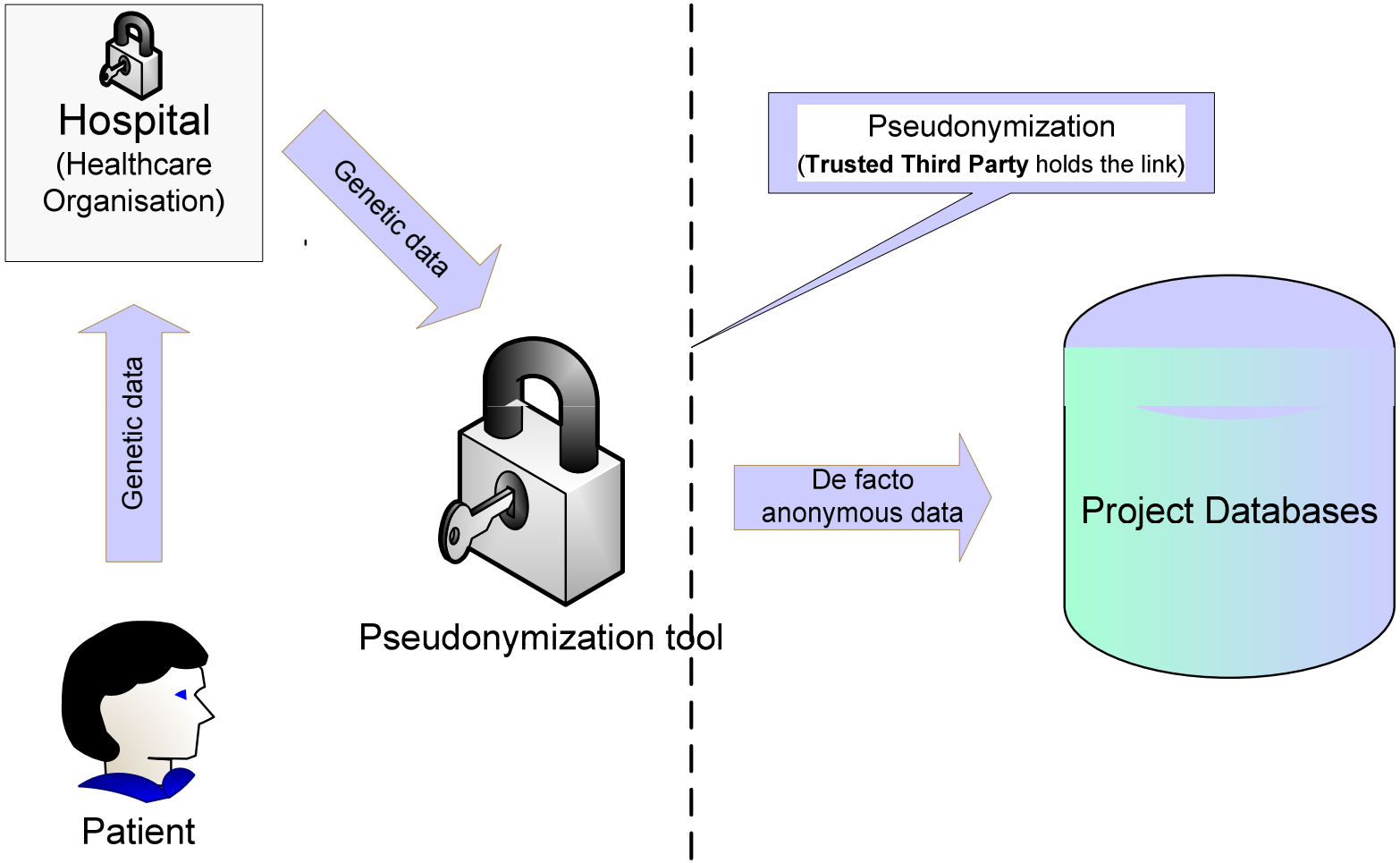
1. The researcher does not have access to the link
2. No third party has access to the genetic data

Processing of anonymous data

- If data processors work with
  - pseudonymized data
  - can't establish the link
  - do not transmit it to third parties outside of the project or disclose it

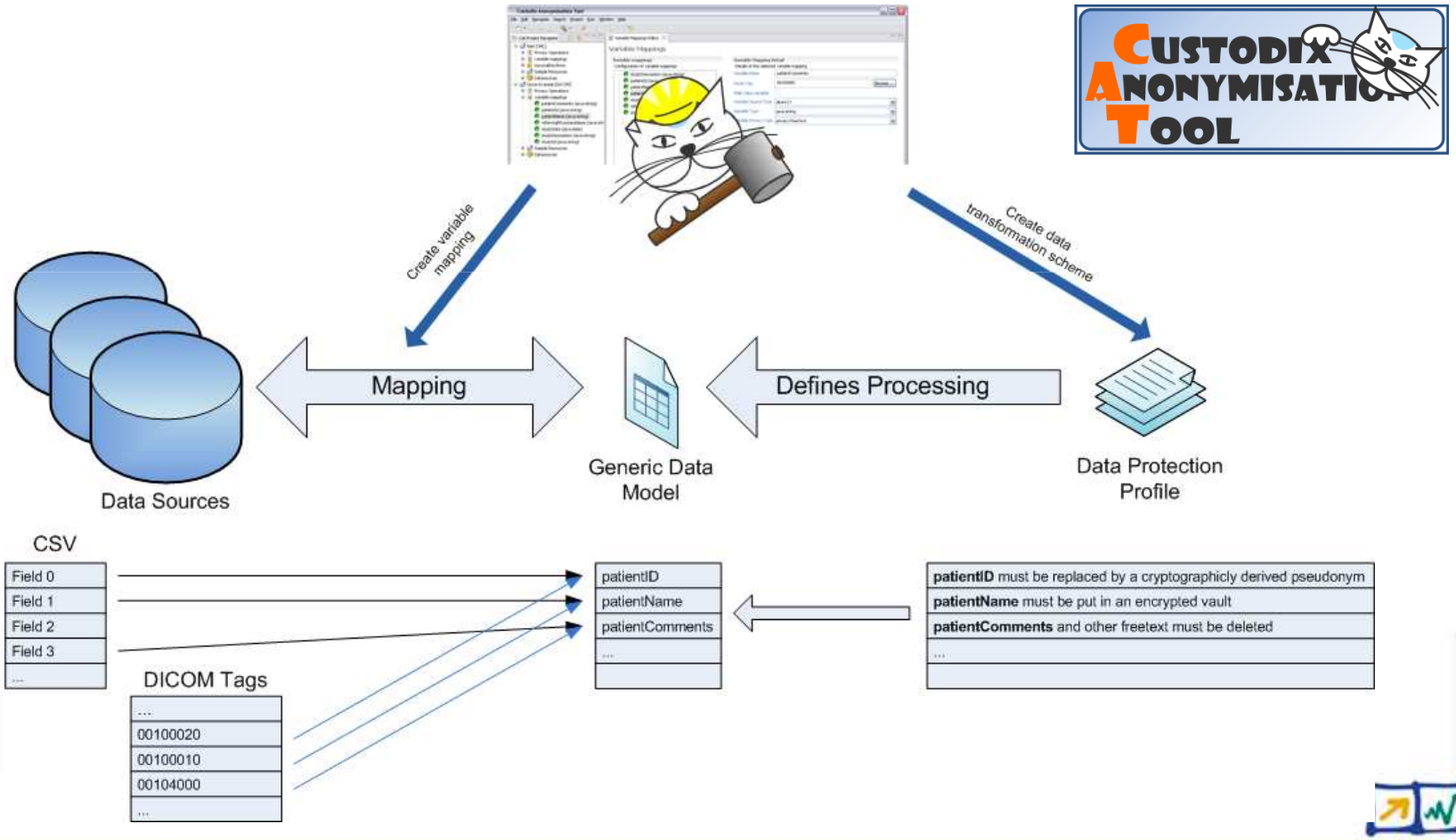
  they process de facto anonymous data
- To ensure a state-of-the-art pseudonymization we implement a procedure done by the local hospital in cooperation with a Trusted Third Party

Processing of anonymous data

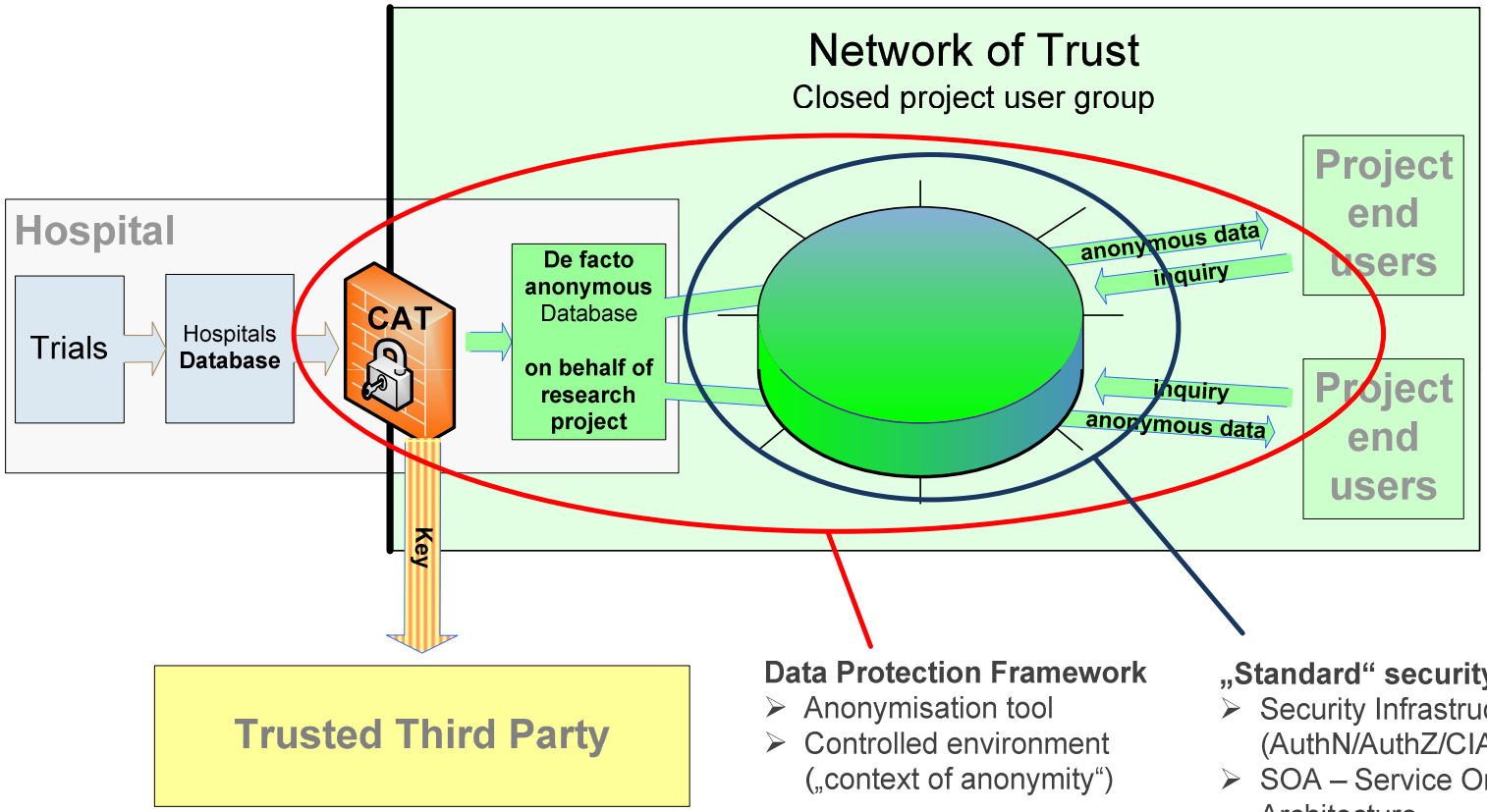


Pseudonymization tool: CAT Workbench

- Make a “data protection” configuration once… run it several times…



Data Security architecture



Data Protection Framework
- Anonymisation tool
- Controlled environment („context of anonymity“)

„Standard“ security
- Security Infrastructure (AuthN/AuthZ/CIA)
- SOA – Service Oriented Architecture
  - GLOBUS/GRIDGE
  - WS

Data Protection Framework

- Processing of anonymous data
- Data Protection Authority
- Binding contracts
- Informed consents as a fall-back-scenario and for ethical reasons (patient autonomy)
- Allowing re-identification

Center for Data Protection

CDP

www.privacypeople.org

Home Objectives Contact Us

Menu

- Home
- Objectives
- 2007 Activities
- Founders
- Contact us

Home

Welcome to the CDP

Origin of the "Centre for Data Protection" (CDP)

The Center for Data Protection (CDP) is a non-profit organization that founded in August 2007 as a spin-off from the prestigious European Research Project "Advancing Clinico-Genomic Trials on Cancer" (ACGT). The ACGT project aims at developing a Biomedical GRID infrastructure for sharing Clinical and Genomic expertise. The core activities of the project are:

- Integration of clinical history, medical imaging and genetic data
- Building a knowledge Grid
- Running Clinical Trials (initially) on breast cancer and paediatric nephroblastoma

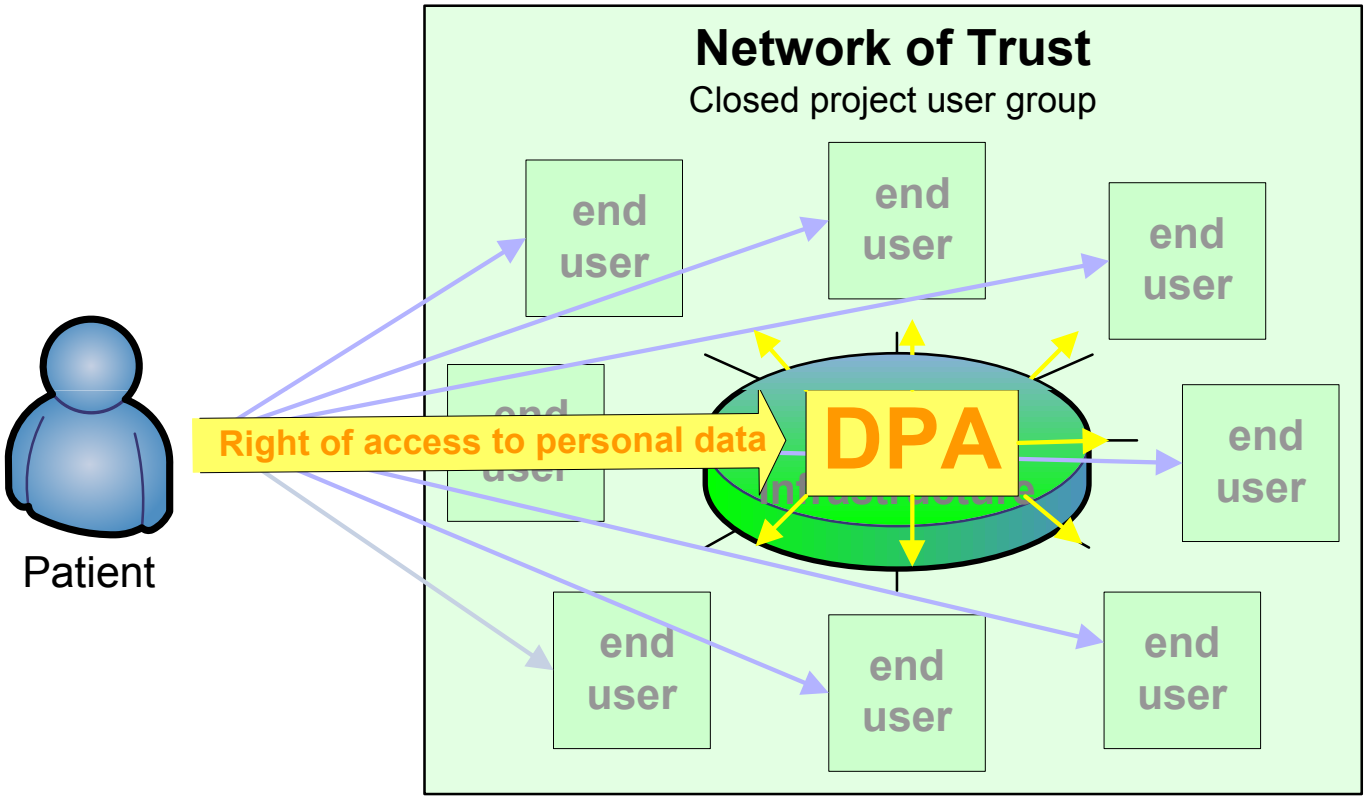
The CDP is the result of the work of two complementary workpackages in ACGT, focussing on all aspects of data protection (ethical, legal, technical): "WP 10: Ethical, Legal and QA issues" and "WP 11: Trust and Security". The Center for Data Protection is primarily founded to act as a legal body able to enforce security and privacy policies for the ACGT clinical trials (and act as Data

ACGT: Center for Data Protection

Center for Data Protection
CDP
www.privacypeople.org

- Non-profit organisation under Belgian law
- Contract Party (on behalf of ACGT)
- Data Controller
- „Home“ for the Ethical and Data Protection Issues
- Contact point for patients

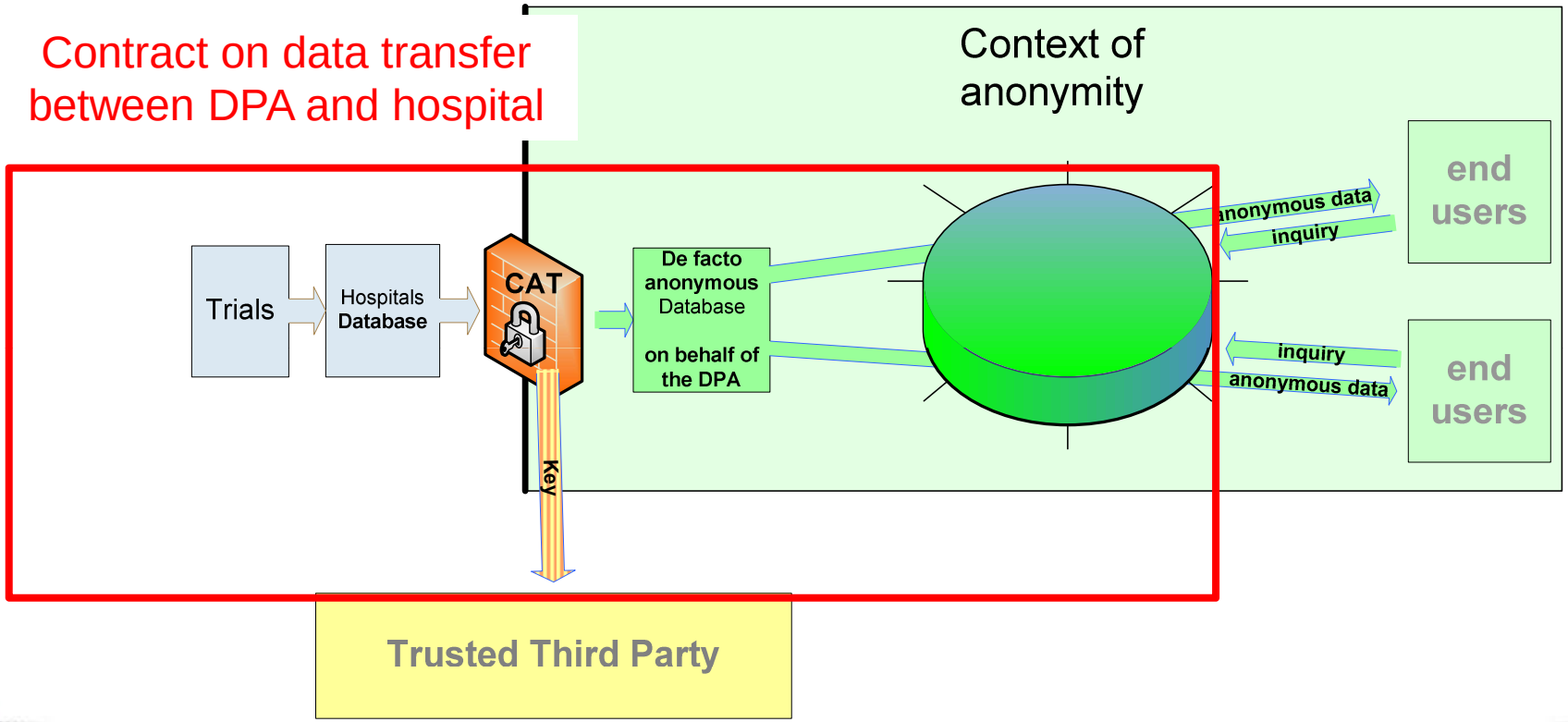
Contact point for patients



Data Protection Framework

- Processing of anonymous data
- Data Protection Authority
- Binding contracts
- Informed consents as a fall-back-scenario and for ethical reasons (autonomy)
- Allowing re-identification

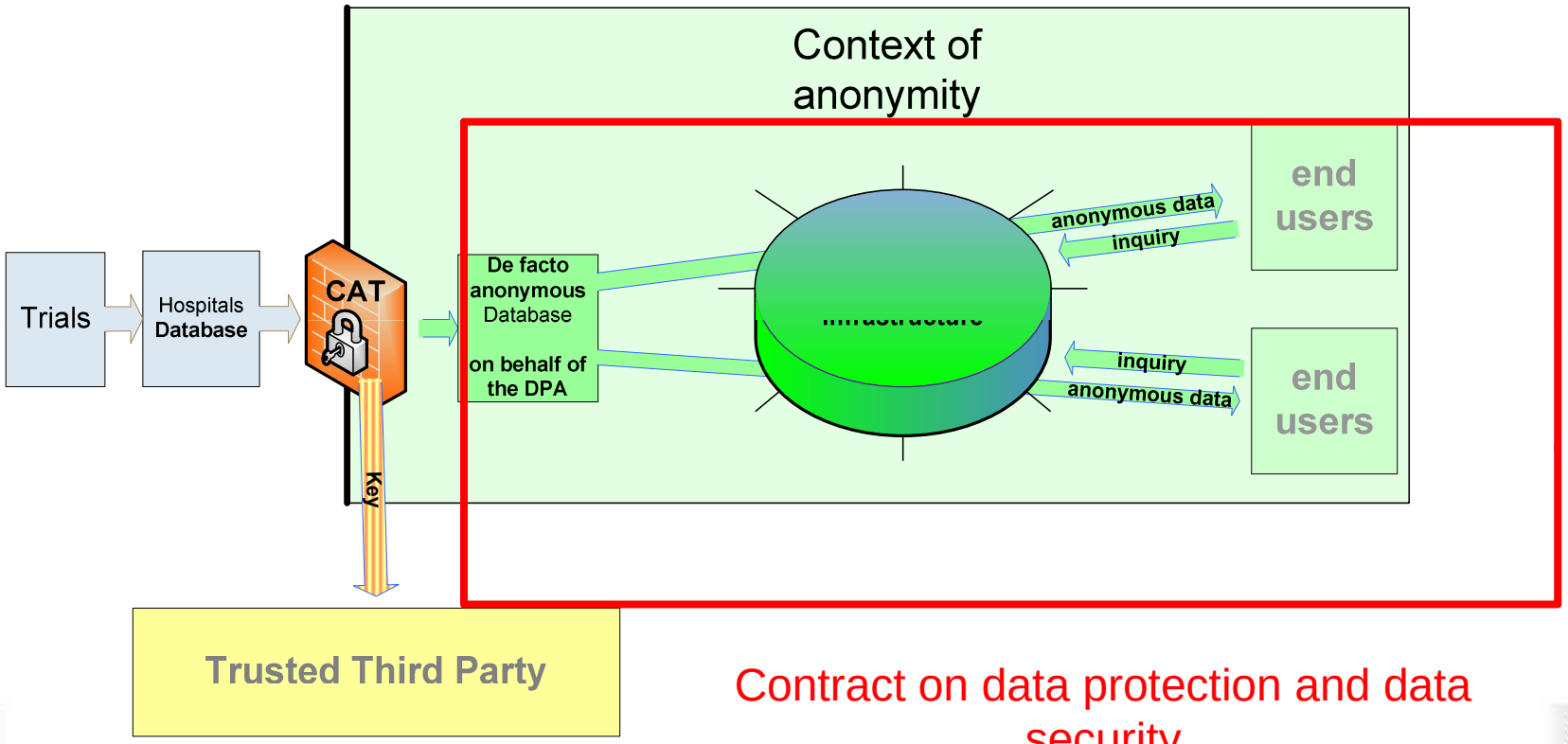
Contract on data transfer



Contract on data transfer

- Concluded between hospitals/investigators and DPA
- Guarantee of a state-of-the-art pseudonymization procedure
- Technically and organizationally separated Project Database
- No matching between the Project Database and the hospital's database
- Confidentiality

Contract on data protection/security



Contract on data protection and data security
between DPA and end user

Contract on data protection/security

- Concluded between DPA and end users
- Ensuring the context of anonymity:
  - Technically and organizationally separated database for data received via the project
  - No matching between the data received via the project and other genetic data
  - No transfer/disclosure of data received via the project to any third party
- Confidentiality
- Data subject's rights (access etc.) can be exercised via the DPA

Data Protection Framework

- Processing of anonymous data
- Data Protection Authority
- Binding contracts
- Informed consents as a fall-back-scenario and for ethical reasons (autonomy)
- Allowing re-identification

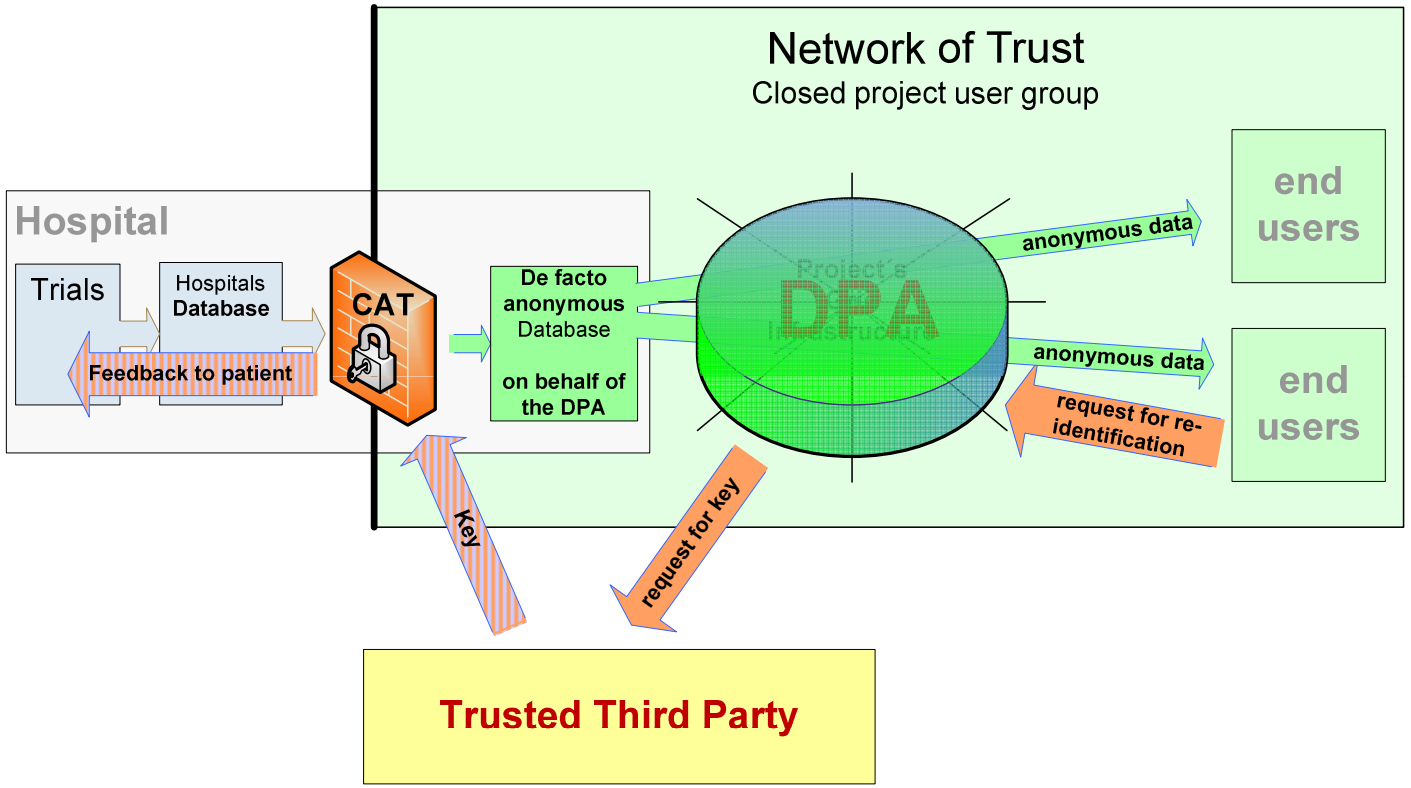
Informed consents

- Major Fallback Scenario
- If a patient or his/her representative consents to the processing of his/her sensitive data, the processing is lawful in every Member State (Art. 8 para. 2 lit. a).
- For ethical reasons needed anyway

Data Protection Framework

- Processing of anonymous data
- Data Protection Authority
- Binding contracts
- Informed consents as a fall-back-scenario and for ethical reasons (autonomy)
- Allowing re-identification

Reidentification, if needed



Side note

- Data transfer to so called "third countries"

→ Artt. 25, 26 of Dir. 95/46/EC

Data transfer to third countries?

- Art. 25 Dir. 95/46/EC
  - Transfer of personal data only if "third country in question ensures an ***adequate level of protection***"
  - Aim → hinder data controllers from avoiding the requirements of the Directive by shifting their data-processing operations to countries with more lenient requirements.

Third countries?

- Countries not belonging to
  - the European Union (EU) or
  - European Economic Area (EEA) - Norway, Liechtenstein and Iceland
- The Commission has so far recognized
  - Switzerland,
  - Canada,
  - Argentina,
  - Guernsey,
  - Isle of Man and
  - the US Department of Commerce's Safe harbour Privacy Principles

as providing adequate data protection

Data transfer to third countries? – Art. 26

- If the country in question does not ensure an adequate level of protection, transfer only if:
  - data subject has given consent unambiguously; or
  - necessary for performance of a contract between data subject and controller; or
  - necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or
  - necessary in order to protect the vital interests of the data subject; or …; or
  - a Member State authorises the proposed transfer accompanied by *appropriate contractual clauses* and notifies the Commission and the other Member States

Data transfer within ACGT?

- Closed user group under the sole control of the CDP (Data Protection Authority)

  → data processing within the network is **no transmission** in the meaning of Dir. 95/46/EC

  → if participant from third country signs all contracts provided in ACGT, the Belgian Data Protection Authority would have to approve and inform European Commission and other MS

Thank you very much
for your attention!

Contact:
Dr. Tina Krügel, LL.M.
kruegel@iri.uni-hannover.de
info@privacypeople.org