The BEACON use case under the GDPR

Regina Becker

ELIXIR-LU

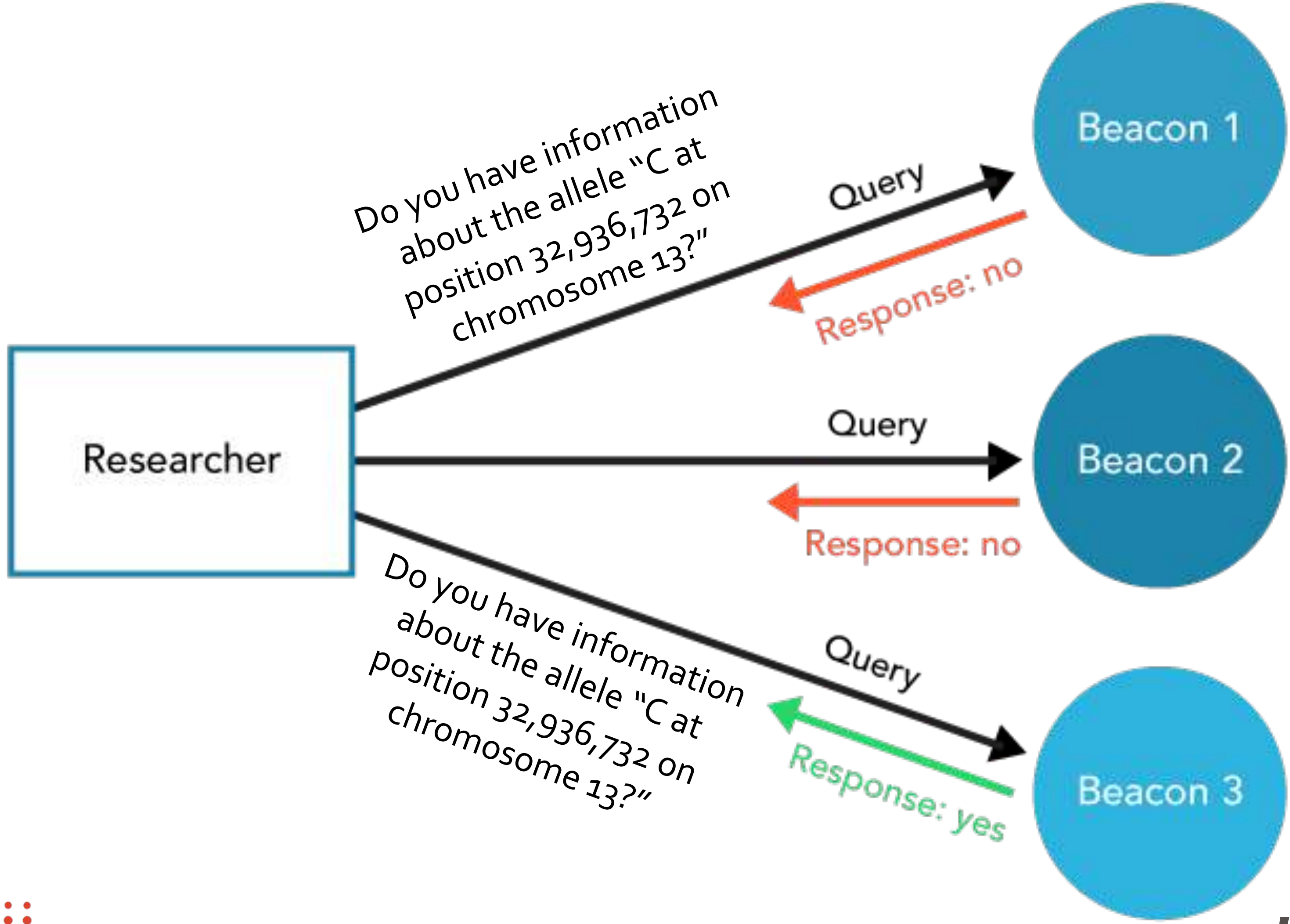
ELIXIR AllHands Workshop
7. June 2018

elixir LUXEMBOURG

Luxembourg Centre for Systems Biomedicine

The BEACON tool

— Processing genetic data to make it “Findable”



Do you have information about the allele "C at position 32,936,732 on chromosome 13?"

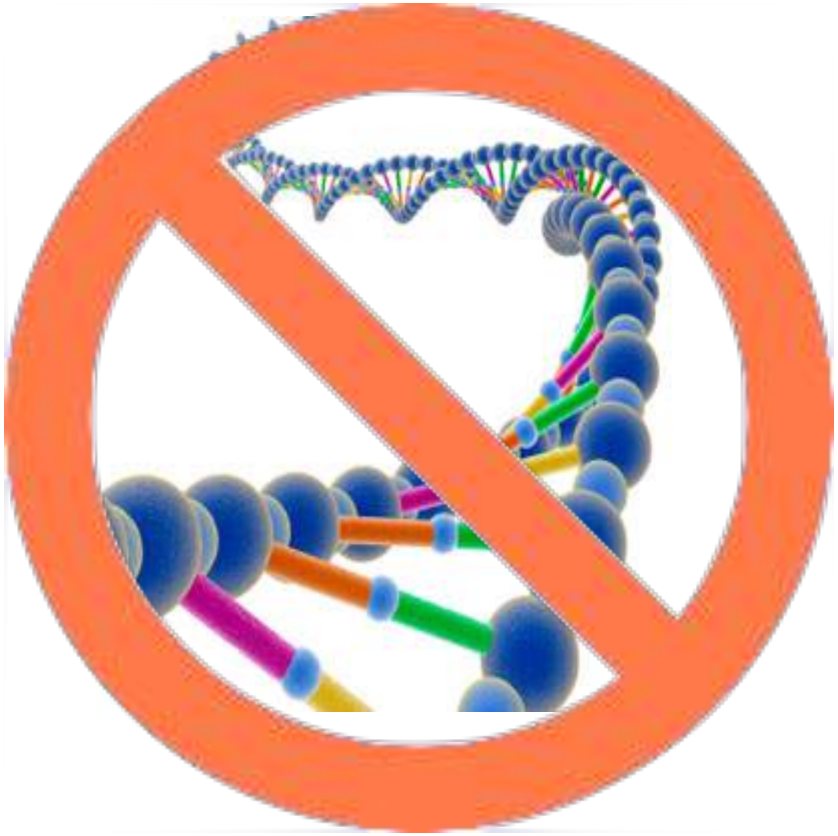
Do you have information about the allele "C at position 32,936,732 on chromosome 13?"

Processing genetic data to make it "Findable"

— What does the GDPR say?

GDPR Article 9.1

- […] the **processing of genetic data**, […] **shall be prohibited**.



Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

Processing genetic data to make it “Findable”

— When is it possible?

Opening clause GDPR Article 9.2

- Paragraph 1 shall not apply if one of the following applies:
  - (a) the data subject has **given explicit consent** to the processing of those personal data for one or more specified purposes, […]

  - (j) processing is necessary for […], **scientific** or historical **research purposes** […] based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Processing based on Art. 9.2(j)

— Using the interests of research to overcome prohibition

Conditions for application

- Implementation of the paragraph into **national law**
- **Proportionality** of the aim
- High(est) requirement for measures of **safeguards**

Pitfall GDPR Article 9.4

- Member States may maintain or introduce **further conditions, including limitations**, with regard to the **processing of genetic data**, biometric data or data concerning health.

→ The GDPR failed the harmonisation of processing genome data

→ Rules for processing genetic data differ between countries

→ Check the law in your country if Art. 9.2(j) is open for you

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

Processing based on consent Art. 9.2(a) — The safe option?

Processing based on consent

- Requires to follow the GDPR rules for consent
  - Freely given
  - Specific
  - Informed
  - Unambiguous indication
  - Can be withdrawn any time

Rescue and pitfall GDPR Recital (33)

- […] data subjects should be allowed to give their consent to **certain areas of scientific research** […]

→ Recital (33) opens the possibility of broad consent

→ But keeps purpose limitation: no consent for research in general

→ Broadest possible consent*: health / biomedical research

*My experience only, not all data protection authorities agree

Consequence of consent purpose limitation

— Lighting a beacon must be compatible with purpose

Purpose compatibility (Art. 5.1)

- Personal data shall be […] **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes
- **further processing** for […] scientific or historical research purposes […] shall, in accordance with Article 89(1), **not be considered to be incompatible** with the initial purposes

Pitfall GDPR Art. 9.4

- Member States may maintain or introduce **further conditions** […] with regard to the processing of genetic data, […] or data concerning health

→ **Possibility to limit processing of health and genetic data means further processing not possible in all countries**

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

Implementation of purpose limitation

— Measures to achieve compliance

Further processing

- Further processing requires **advance information** of the data subject according to Art. 13.3
- User must be obliged to **query for scientific research only**
- Necessity to check if further processing of genetic data is **allowed in the respective country** of the processing

Consent purpose

- Where the consent is **limited to certain disease(s), certain user types etc.,** the Beacon can only be lit within such disease requests

→ **Terms of Service must require the User to comply with (specific) research purpose**

→ **Filtering of genomes for e.g. certain diseases must be possible**

Accessibility of BEACON

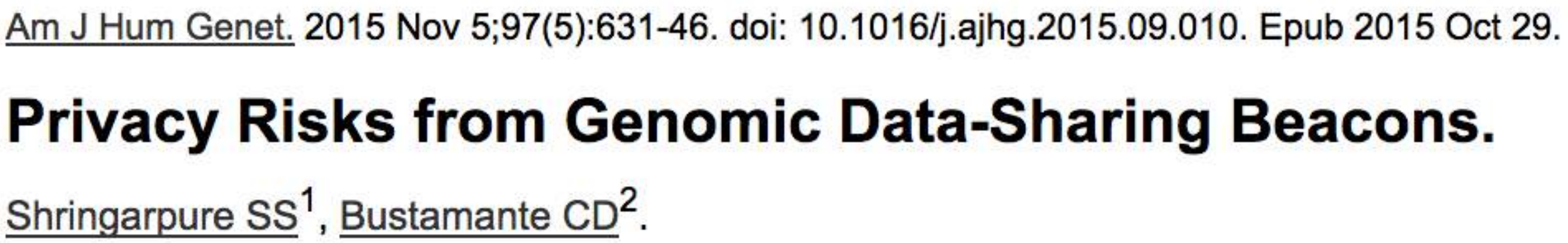
— Avoid transmission of personal data

International data transfer

- Beacon is **accessible world-wide**
- Transfer of personal data **outside the EU is prohibited** without proper safeguards / measures in place
- Information of **BEACON must never lead to personal data**

Pitfall: Shringarpure-Bustamante's Attack

- Multiple queries can **identify a person** if a set of variants is known to the attacker



Am J Hum Genet. 2015 Nov 5;97(5):631-46. doi: 10.1016/j.ajhg.2015.09.010. Epub 2015 Oct 29.

Privacy Risks from Genomic Data-Sharing Beacons.

Shringarpure SS[1], Bustamante CD[2].

→ Registered or controlled access minimises this risk

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG

Other personal data in BEACON

— Web statistics

Use of cookies

- **IP addresses are identifiers** and create personal information (Art. 4.1, Recital (30))
- Cookies overned not only by GDPR but also **ePrivacy Directive** (Directive 2002/58/EC http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1525854997759&uri=CELEX:32002L0058)
- Most cookies that are not essential for a service require **consent**
- Information on cookies and **national differences in legislation** https://termsfeed.com/blog/eu-cookies-directive/#Requirements_by_the_EU_Cookies_law

Google Analytics

- Google Analytics acts as **processor**
- Google offers **GDPR compliance tools**
- It’s the **obligation of the controller** to choose the right settings

Administrative data in BEACON

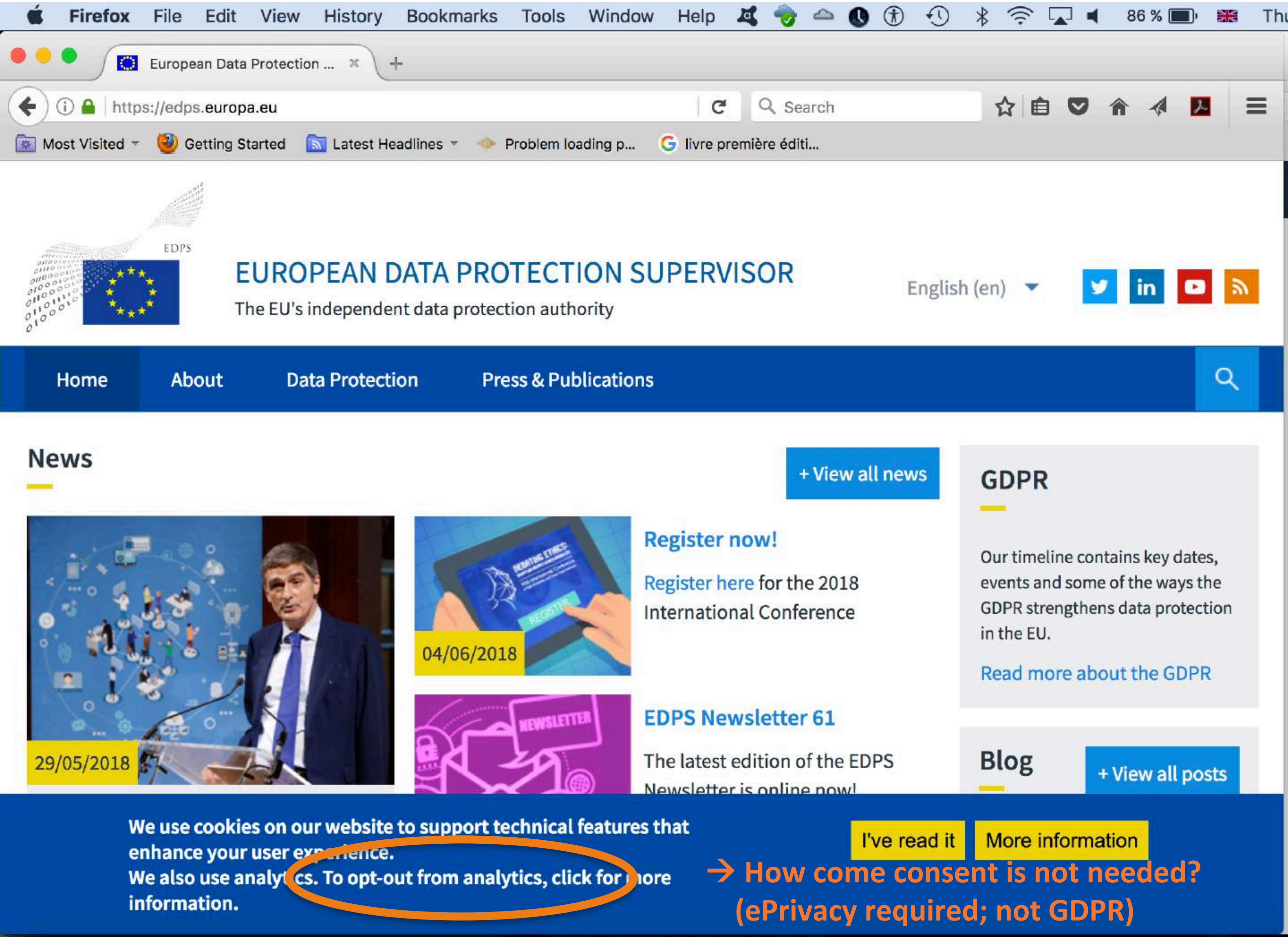
— Registration data

No consent for cookies needed for...

- **user-input cookies** (session-id) such as first-party cookies to keep track of the user's input when filling online forms, etc.
- **authentication cookies**, to identify the user once he has logged in, for the duration of a session
- **user-centric security cookies**, used to detect authentication abuses, for a limited persistent duration

No consent needed for processing registration data...

- If legal basis for processing is:
  - Art 6.1(c) necessary for **compliance with legal obligation**
    →Only possible if registration exclusively for data protection
  - Art. 6.1(b) necessary for the **performance of a contract**
    → Here, **Terms of Service** have the role of a contract
    Explicit **acceptance** will be needed
    → Only if registration is exclusively for service provision



EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

News

Register now!

Register here for the 2018 International Conference

EDPS Newsletter 61

The latest edition of the EDPS Newsletter is online now!

GDPR

Our timeline contains key dates, events and some of the ways the GDPR strengthens data protection in the EU.

Read more about the GDPR

Blog

We use cookies on our website to support technical features that enhance your user experience.
We also use analytics. To opt-out from analytics, click for more information.

→ How come consent is not needed?
(ePrivacy required; not GDPR)

Security measures – Art. 32

Proportionality

- Measures balance the
  - **Costs** of implementation
  - **Nature, scope, context** and **purposes** of processing
  - Risk of **likelihood** and **severity** for the rights and freedoms of natural person

Technical and organisational measures

- **Pseudonymisation** and **encryption**
- Ability to ensure the ongoing **confidentiality**, **integrity**, **availability** and **resilience of processing** systems and services
- Ability to **restore the availability and access** to personal data in a timely manner in the event of a physical or technical incident
- Process for **regularly testing**, assessing and evaluating the effectiveness of technical and organisational measures
- Ensure **compliance of staff**

Information obligation following Art. 13

— Privacy Policy

Need for privacy policy on webpage

- If personal data is processed
- Independent of legal basis (i.e. also outside consent)
- Easily accessible / findable

Content

- Controller
- Data protection officer
- Separately:
  Purposes of processing, legal basis, data types and recipients
- Automated decision making with logic involved and consequences
- Data protection rights of the webpage user (Art. 15-21)
- Right to withdraw consent (where previously given)
- Right to lodge a complaint with data protection authority

Nice example

http://www.kowi.de/en/system-metanavigation/privacy-policy/privacy-policy.aspx

elixir LUXEMBOURG

THANK YOU!

Luxembourg Centre for Systems Biomedicine

elixir LUXEMBOURG