



The Galaxy use case under the GDPR

Regina Becker
ELIXIR-LU



ELIXIR AllHands Workshop
7. June 2018

The Galaxy service

— What GDPR rules apply?



The Galaxy service

— Acting as a processor under the GDPR

Definition Art. 4.8

- ‘processor’ means a natural or legal person, public authority, agency or other body **which processes personal data on behalf of the controller;**

Definition Art. 4.2

- ‘processing’ means **any operation** [...], such as collection, recording, **organisation**, structuring, **storage**, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;[...]

→ **By offering a service that includes the processing of personal data, the Galaxy host becomes processor**

Obligation as processor – Art. 28

— Processing must be governed by contract

Content

- **Subject-matter and duration** of the processing, **nature and purpose** of the processing, **type of personal data** and **categories of data subjects** and obligations and **rights** of the controller.
- **Obligations** of processor
 - Process the personal data **only on documented instructions** from the controller
 - Ensure authorised persons committed to **confidentiality**
 - Take all **(security) measures** required pursuant to Article 32
 - Engage another **(sub-)processor** only with approval of controller
 - Assist the controller in compliance with **data subject requests**
 - **Assist controller in legal obligations** pursuant to Articles 32 to 36
 - **Delete or return** all the personal data after the end of services
 - Allow for and contribute to **audits**
 - **Existing contracts will probably need revision**
 - **Mention participating clouds in the contract**

Obligation as processor – Art. 28

— Example clause for sub-processors

5.2 Subprocessing

LCSB-UL may use providers and **subprocessors** (the “**Subprocessors**”) whilst delivering Services to the Data Provider. Subprocessors include the entities listed in Annex B. Other Subprocessors may take part in the Data processing, subject to,

- informing the Data Provider beforehand in writing (email accepted),
- the Data Provider’s not objecting against such appointment (on reasonable grounds) within fourteen (14) days of such information.

LCSB-UL’s and each Subprocessor must enter into a written processing agreement compliant with Data Protection Law requirements.

The Data Provider hereby authorises and instructs LCSB-UL to transfer Data to Subprocessors, and the latter to process the Data. Where Subprocessors are located outside the EU/EEA, the Data Provider will cooperate with LCSB-UL (including by entering into standard contractual clauses with the concerned Subprocessors or by executing power of attorney to LCSB-UL to this end) to secure the transfers against Data Protection Law transfer restrictions, unless the Data Provider has reasonable grounds for objecting to the transfer.

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**

→ **Confidentiality biggest concern**

→ **No “one size fits all” required but choice needs justification**

Support the controller – Art. 33-36

— Information obligations

Data Breach

- **Inform the controller** without undue delay after becoming aware
 - Nature of the breach,
 - Categories and approximate numbers of data subjects concerned,
 - Categories and approximate number of personal data records concerned
 - Contact point where more information can be obtained
 - Where appropriate: measures taken

Data protection impact assessment

- Provide **information on technical and organisational safeguards** to maintain privacy and integrity of the personal data
 - **You are responsible and accountable for the processing on your side**

Processor's Documentation obligation – Art. 30

— Records of categories of processing

Content

- Name and contact details **processor**
- Name and contact details of each **controller** including where applicable: representative and data protection officer
- **Categories of processing** carried out on behalf of each controller
- **Transfers** of personal data to a third country or an international organisation (where applicable) including safeguards
- **General description** of the technical and organisational **security** measures

Form of records

- In **writing** (including electronic form)

→ You will have to update your book-keeping for DPOs

The Galaxy server

— Acting as data controller for data about users



<http://www.abtasociates.com>

The Galaxy server

— Acting as controller under the GDPR: lawful processing

Legal basis for processing registration data

- Consent is **not appropriate**
 - As required for service → **not freely given**
- Art. 6.1(b) necessary for the **performance of a contract**
 - Processing agreement is required
 - Even **Terms of Service** count as contract
 - But: explicit **acceptance** will be needed
 - Data needs to be required **for service only**,
no other purposes should be hidden
 - if **additional purposes** are envisage:
ask for **dedicated consent**

Transparent processing

— Web statistics

Use of cookies

- **IP addresses are identifiers** and create personal information (Art. 4.1, Recital (30))
- Cookies governed not only by GDPR but also **ePrivacy Directive** (Directive 2002/58/EC <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1525854999759&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](https://termsfeed.com/blog/eu-cookies-directive/#Requirements%20by%20the%20EU%20Cookies%20law)

Google Analytics

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



EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

English (en)



News

+ View all 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

+ View all posts

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.

I've read it More information

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

Transparent processing

— Cookies without consent

Criteria

- The cookie is used “for the sole purpose of carrying out the transmission of a **communication** over an electronic communications network”.
- The cookie is “strictly necessary in order for the provider of an **information society service** explicitly requested by the subscriber or user to provide the service”.

WP29 – 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

Transparent processing

— Information obligation following Art. 13

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-metavigation/privacy-policy/privacy-policy.aspx>

Transparent processing

— Record keeping following Art. 30

Content of processing records

- Name and contact details of **controller** and, where applicable: joint controller, representative and data protection officer
- **Purposes** of the processing
- **Categories of data subjects** and categories of **personal data**
- **Categories of recipients** to whom data have been or will be disclosed including recipients in third countries or international organisations
- **Transfers** of personal data to a third country or an international organisation (where applicable) including safeguards
- Envisaged **time limits** for erasure of different categories of data
- General description of the technical and organisational **security measures**

Fair processing

— Responsibilities of controller

Implementation of technical and organisational measures

- Data protection **policies**
- **Data minimisation** – collect only data needed for purpose!
- Keep data only **as long as necessary**
- **Access restriction** – access only to personnel needed
- Secure **storage** and **transfer**
- **Security measures** (in accordance with Art. 32)

Sharing data

- Only with **prior information** of data subject
- Joint controllers:
determine transparently the **respective responsibilities** for compliance with the obligations of the GDPR
- Processor: only based on **contract** following Art. 28

Fair processing

— Rights of data subject

- Article 13** • **Information** to be provided where personal data are collected from the data subject
- Article 15** • Right of **access** by the data subject
- Article 17** • Right to **erasure** ('right to be forgotten')
- Article 18** • Right to **restriction** of processing
- Article 21** • Right to **object** (where no consent was given)
- Article 16** • Right to **rectification**
- Article 19** • **Notification obligation** regarding rectification or erasure of personal data or restriction of processing to other recipients
- Article 20** • Right to data **portability**

The Galaxy use case

— What else is needed?

Data protection officer??

- **YES**, most likely
- Independent of role as controller or processor when
 - **Public bodies**
 - Processing on a large scale of **special categories of data** pursuant to Article 9

Data protection impact assessment??

- **No**
- **Processor** only needs to assist
- Processing of **administrative data** and web statistics not likely to result in high risk to rights and freedom of natural person



THANK YOU!

