Sigrid Gramlinger-Moser

GDPR a practical guide to comply

Sigrid Gramlinger-Moser

- Master in VET
- Creating websites since 2004
- webgras since 2010 exclusively Joomla
- Joomladays Austria & JUG Vienna
- Certified GDPR consultant
- GDPR compliance with data2.eu

What is GDPR

- General Data Protection Regulation
- EU regulation
- May 25, 2018

to **simplify and enhance** the transfer of personal data between organisations in different countries while **protecting personal** data in an appropriate secure way

Term Definition

- **Data subjects** – concerned persons
- **Controller** – responsible person
- **Record of processing activities** – processing index
- **Processor** – processing data “on behalf of”
- **Data Protection Officer** – if necessary
- **Data Protection Authority**

What is personal data

- all data of an identifiable natural person

- either directly about someone or it can be traced back to a person

First name, last name, title (name)

Address, city, zip code, country (address data)

Phone, mobile, email (contact data)

Time sheets, IP-address, geographic location, event registration, payment details, social media contacts, …

Personal Data - Special categories

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- union membership,
- genetic data,
- biometric data,
- data concerning health or
- a natural person's sex life or
- sexual orientation

Legal Basis

- Person has given consent (children!)
- Fulfillment of contract
- Legal obligation
- Protection of vital interests
- Task for public interest or official authority
- Legitimate interests by controller

Principles of GDPR

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability (as controller)

- Privacy by design
- Privacy by default

Concerned people

- Information (what, why, where, how long,…)

- Right to be informed
- Right to get access
- Right to get the data corrected
- Right to cancellation ("right to be forgotten")
- Right to restriction of processing
- Right to data portability
- Right to object

How can I comply

- Privacy statement
- Privacy by default/privacy by design
- Record of processing activities – processing activities incl. technical and organisational measures (TOMs)
- Make contracts with processors
- Check if DPIA (data protection impact assessment) or DPO is necessary

Provide appropriate security measures!!!

What is a processing index

- Name and contact of controller, representative, DPO
- **Processing activities**
  - Purpose of processing
  - Categories of concerned persons
  - Data categories
  - Legal basis
  - Deleting deadlines
  - Categories of recipients (3rd countries, internat. Organisations)
- TOM (technical & organisation measures)

Newsletter

- Sending emails with events, products,…
- Subscribers, clients
- Name, email, IP-address
- Consent
- Until cancellation
- Email-provider, Mailchimp (US, Privacy Shield)

You **have** processors

- Recipients of personal data
- Are they GDPR compliant?
- Where are the situated?
- Reliable!
- TOMs
- Privacy Statement

→ **Contract with processor**

You **are** a processor

Processing index as processor

- Name and contact of controller, representative, DPO
- Name and contact of processor, representative, DPO
- **Processing activities**
- Categories of recipients (3rd countries, internat. Organisations)
- TOM (technical & organisation measures)

→ Contract with your client

You **are not** a processor

You are processing data?

Is it personal data?

Who is deciding about the means?

Just fixing a problem?

Non disclosure agreement - NDA

Newsletters

- Legal basis:
  consent
  legitimate interest of the controller
- What information do you store? **How long?**
- Inform people how they can sign off again
- Check in your DB
- Use SSL for your website
- Use double opt-in if available (→ proof)
- Sending and importing NL recipients – use encryption → no email!

Webshop

- Legal basis:
  legal obligations (invoices) and
  to fulfill your contract (the order).
- Use SSL for your website
- Inform what data is stored and how long
- Inform your visitors and customers about cookies
- Only collect necessary data
- Check for payment providers
- Are you using a currency convertor? Is it an external JavaScript?

Tracking

- Legal basis:
  legitimate interest
- For marketing purposes and optimizing websites
  → a good insight in your visitors is essential.
- Make contract with provide
- Use IP anonymize
- Provide Opt-Out
- Update cookie information and privacy statement

Contact form

- Only collect necessary data.
- Use https on your website
- Email notifications - plain text!
- Check data in database
- Delete old data
- Scripts to delete data

Paper Documents

- Printers with internal disc storage
- Misprints → shredder
- Where do you store your binders?
- Destroy / Shredder

Other

- Services like Watchful.li & myJoomla
- Remove Data in Joomla
  (articles, search, versioning, users, backups,…)
- 3rd party GDPR Extensions
- Cloud services
- Social Media

Web agency

- Transparency
- Compliance
- Good reputation
- High quality support
- Help customers with GDPR

ToDo before May 25

- Update your privacy statement
- Check all external scripts
- Contact forms and all other forms
- HTTPS

Provide appropriate security measures!!!

GDPR - it is a chance!

https://data2.eu/en/gdpr-tips

Twitter: sgramlinger

Twitter: data2eu