GDPR
a practical guide to comply

Sigrid Gramlinger-Moser
Certified GDPR Consultant

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 - AVG
- 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
- **Record of processing activities** – Processing index
- **Processor** – verwerkersovereenkomst
- **Data Protection Officer** – if necessary
- **Data Protection Authority** – Autoriteit Persoonsgegevens

What is personal data

- all data of an identifiable natural person

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

- name, contact details, birthdate, geo position, IP-address, photo, video, hobbies, license plate, time sheets, educational data, family status, wage, …

Personal data - Special categories

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data,
- data concerning health or
- a natural person's sex life or
- sexual orientation
- Social Security Number - Burger Service Nummer (NL!)

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)

Concerned people

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

- Obligation to inform
- Right to get the data corrected
- Right to cancellation ("right to be forgotten")
- Right to restriction of processing
- Right to data portability
- Right to contradiction

How can I comply

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

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: verwerkersovereenkomst

You **are** 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: verwerkersovereenkomst

Newsletters

- Legal basis: consent, legitimate interest of the contoller
- if you store IP-address inform people
- check in your DB
- inform people how they can sign off again
- check if your form is transmitted through SSL
- use double opt-in if available
- sending and importing NL recipients – use encryption → no email!

Webshop

- Legal basis: for legal obigations (invoices) and to fullfill your contract (the order).
- use SSL for your website so that all communication is transported through a secured line
- inform your visitors and customers about cookies
- only collect necessary data
- check for payment providers
- inform what data is stored and how long
- if you store IP-address inform people
- are you using a currency convertor? Is it an external JavaScript?

Tracking

- For marketing purposes and optimizing websites, a good insight in your visitors is essential.
- However, you'll collect (and store) a lot of personal information about your visitors.
  - make contract with provider
  - use IP anonymize
  - provide Opt-Out
  - 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
- CLI script for RS Form Pro by Peter Martin

Paper Documents

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

Other

- Services like Watchfulli & 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

Some more terms

- Privacy by design
- Privacy by default
- Data breach

GDPR - it is a chance!

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

Twitter: sgramlinger

Twitter: data2eu