GDPR: Keeping Your Personal Data Secure

General Data Protection Regulation

Given regulation status in May 2018, what was once a directive became enforceable by creating a set of legislative acts that are applicable in entirety in every EU country. All data moving through the EU must meet the requirements.

I've heard the term, but what does it mean?

GDPR is an EU-wide regulation which enforces every citizen's fundamental right to be able to protect their personal data.

Sounds good, but why do I need it?

Tech companies are constantly dealing with some of your most important private data.

Regulating the use of that data keeps companies from selling your personal information for profit without your consent.

It also protects against data breaches and cyberattacks by keeping exchanged information anonymous.

Overall, users have the lawful right to be in control of their data.

Ok. What exactly is this personal data?

The term you need to know is PII: Personal Information Identifiers.

PII can only be processed with legal basis:

- to fulfill contractual obligations
- due to official authority
- with consent

- Sensitive PII can include full name, driver's liscense, passport information, medical records and financial information.
- Non-sensitive PII is easily accessible from public sources, ex. race, gender, date of birth

What about my rights according to my PII?

You have four to remember:

- Right of access: you have the right to access your data and know how it is processed.
- Right to be forgotten: you have the right to request erasure of any personal data related to you
- DPO (Data Protection Officer): public authorities and some businesses must have someone in charge of ensuring compliance.
- Pseudonymisation: PII should be stored in an unidentifiable way.

These rights legally must be addressed by allowing the user to choose which information they give access to with clear, easy to understand cookie banners.

Sounds great! Are there any additional protections that are Germany specific?

There is still an EU directive waiting to be set in to regulation, covering additional privacy concerns called the ePrivacy Directive.

This directive covers data concerns regarding data retention, unsolicited communication and browser storage.

Currently, it is enforced on the national level; each is responsible for creating and enforcing the directive.

- Data Retention: companies must delete or anonymise PII when not needed, unless given informed consent for longer retention.
- Unsolicited Communication: use of email for marketing purposes is prohibited without user consent.
- Browser Storage: user must consent before cookies data is stored in the browser.

Consent is the key here. Users must always have the opportunity to give consent to any use of their personal data.

★ ★