GDPR - What do I need to know

The General Data Protection Regulation will become effective as of May 25, 2018. Any entities processing the personal data of EU citizens need to comply with this regulation. Even though that your business might be based outside the EU itself, most certainly you will and already have provided your services to EU citizens. Therefore you are subject to this regulation and we recommend to you to treat the GDPR regulation as the new must-have standard on how to handle all personal data, regardless of where the customer is from. In the following article we would like to highlight the key points you need to be aware of. This shall not be seen as a conclusive list or legal advice. Keep in mind that you have to be compliant yourself, act accordingly and not just rely on the fact that Palisis is.

Key concepts and things to know

Privacy by design and privacy by default

Privacy by design and privacy by default has become firm legal requirement. This means there's a requirement on data controllers to minimize processing of personal data, limiting activity to only what's necessary for a specific purpose, carrying out privacy impact assessments (PIA)[1] and maintaining up-to-date records to prove out their compliance[2]. A conclusive list of what personal data is, can be found here[3].

Consent-forms

On consent forms, such as your checkout pages, make sure to only offer an unselected box to subscribe to email, clearly outlines channels you will reach out to them, what kind of content it will be and offer a frequency expectation. Keep a link to mailing consent terms and conditions, kept separate to this under any circumstances separated from purchase Terms & Conditions[4].

- All your forms collecting personal data of a customer should use easy and clear language. Remember: Consent must be unambiguous.
- Always let your customers actively opt-in into any choice. This means if you use a checkbox, avoid having it pre-ticked. (All standard Palisis products do not offer the possibility to have Terms & Conditions pre-ticked. So this this is especially important for companies building their websites booking process over API).
- Let customers freely choose content, channel and frequency and gain consent on each and do not tie consent to other agreements or incentives.
- Explain clearly how customers can withdraw consent (unsubscribe).

Customer rights, including the right to be forgotten

Under GDPR, customer having consented to their personal data being processed at the same time receive rights — including

- the right to access data held about them
- the right to request rectification of incomplete or inaccurate personal data
- the right to have their data deleted
- the right to restrict processing
- the right to data portability

All these rights make it essential for organizations that process personal data to have systems in place which enable them to identify, access, edit and delete individual user data — and be able to perform these operations quickly, with a general 30 day time-limit for responding to individual rights requests.[5]

[1] https://www.smashingmagazine.com/2018/02/gdpr-for-web-developers/
[2] https://techcrunch.com/2018/01/20/wtf-is-gdpr/
[3] https://gdpr-info.eu/art-4-gdpr/
[4] http://www.gf4b.co.uk/wp-content/uploads/2017/10/GDPR-Whitepaper-Forms.pdf
[5] https://techcrunch.com/2018/01/20/wtf-is-gdpr/

Palisis will offer on all its products by the date GDPR becomes effective a customer data scrambler and or permanent deletion mechanism, which will either override all customer sensitive information with random data or delete them entirely. You will be informed about it through the next release notes.

Data breach disclosure

GDPR requires that data controllers report any security incidents where personal data has been lost, stolen or otherwise accessed by unauthorized third parties to their DPA within 72 hours of them becoming aware of it.

What does Palisis do

Data Protection and privacy by design

Palisis fully embraces the privacy by design concept and already did this previous to this regulation. We know and have always clearly communicated that the customer data, your data, is the most sensitive asset we store and we proactively take all steps available to safeguard it.

Hosting and certification

Our Palisis system is constantly reviewed, externally checked and certified PCI compliant. The hosting providers we use are all fully compliant to ISO 27001, 27017 und 27018. Data stored on the Palisis core system is stored within the borders of the European Union and/or in Switzerland. Our TourCMS product data is distributed also to hosting partners in the United States but clearly limited to data stored in TourCMS. No Palisis core data is stored in the US. Reason for storing data in US datacenters is - among others - the technical response times of our infrastructure towards major US-based distribution partners.

Review and adaptations of agreements

We are finalizing our review on our terms of service, privacy policy. We will share with you our latest updated version once it has been finalized, to make sure that we are as precise as possible on subjects affected by GDPR.

Compliance and Data Protection Officer (DPO)

We have appointed a Data Protection Officer and have therefore a staff member dedicated to questions of data privacy, data protection, GDPR and compliance. In case you want to get in contact you can reach the data protection officer using compliance@palisis.com