GDPR Guidelines

October 2017

xeerpa

This document is disclosed in confidence and is protected by copyright. The contents and any ideas set out or reflected in it are confidential and their disclosure to any person not specifically authorised to have access to them may result in material damage to the author and other interested parties.

Should these documents come to the hands of anyone not specifically authorised in writing to have access to them, they should be returned immediately to Xeerpa.
Any unauthorised copying or other use is unlawful.

GDPR - General Data Protection Regulation

The European Union's General Data Protection Regulation (GDPR) is a regulation by the European Parliament, the Council of the European Union and the European Commission that unifies all data protection regulations within the EU, including exports of personal data outside the EU.

GDPR will be fully applicable on May 25, 2018 and any company that offers goods or services to EU residents, or processes data related to EU residents or has employees in the EU will be required to comply with it. In essence, GDPR enforces that users remain in control of the personal data they share with companies.

GDPR requires companies to establish a series of initiatives and controls with regards to the personal they store from clients and users. **Xeerpa is one of the first CIAM European companies to become GDPR-ready, implementing strategies and measures in compliance with the new regulations**, including those related with data security, hosting and data processing.

Learn more about GDPR in this link http://eur-lex.europa.eu/ and http://eugdpr.org.

Xeerpa's key strengths in relation to GDPR

- **Xeerpa already has a designated Data Protection Officer**

  Reporting directly to the CEO and the board, Xeerpa's DPO leads all of our efforts in terms of security and compliance with GDPR, providing first-hand advice to all our clients.

- **Xeerpa is ISO 27001 certified**

  ISO 27001 is the most internationally recognised certification in data security, proving the utmost importance Xeerpa gives to any matter related to personal data access and storage.

- **Xeerpa offers you flexibility and total control over your GDPR strategies**

  Xeerpa's API offers you all the functionality you require in order to securely comply with all GDPR guidelines and recommendations (see table below), not imposing any specific or rigid visual layout. This way you can implement your own strategies and visual interfaces with your users, in line with your current corporate identity and customer experience.

- **Xeerpa already implements rigorous technical measures to ensure data privacy**

  - All data is stored under password-protected encryption at an operating system level with LUKS or EFS.
  - Data access is made through encryption using the https SSL/TLS protocol.
  - Data transfers are encrypted with AES-128.
  - Drives are erased through the DoD 5220.22-M algorithm, which consists of multiple full writings of the discs with random data to prevent the information from being later restored.

- **Let us help you**

  Count on us not only to guide you on how to comply with GDPR, but also on designing personalised user interfaces that make use of our existing API and integrate with your current UX, providing all the functionality that will be required to fulfil your customers' demands and data protection rights.

How Xeerpa complies with GDPR

Differently from other solutions, Xeerpa does not have a visual interface to the end user, so you have total control over the informative screens that will need to be presented to the end user to manage the data you store about them.

Still, Xeerpa already offers GDPR-Compliant features that help our clients comply with the new regulation, including:

GDPR Requirement	What Xeerpa does about it	Success
Customer consent	Xeerpa stores the decision made by each user on whether to consent or not the sharing of their individual personal data when registering to your website, mobile app, promotion or Wi-Fi portal.	✓
Progressive permissions	Xeerpa has the capacity to prevent any processing of personal data until the user has explicitly consented to share it with you, including double-opt in techniques and progressive permission strategies.	✓
Easy data record access mechanisms	Xeerpa provides functionality so your website or app can offer the user the option to view or download all the personal data you store about them, at their request.	✓
Data correction/ Integrity mechanisms	Xeerpa provides mechanisms so the personal data stored for a user can be corrected and its integrity verified, in compliance with the rights of any user as per the new regulations.	✓
Data portability	Xeerpa provides functionality so you can provide a user with all the personal social data stored from them.	✓
Data deletion and rectification	Xeerpa provides functionality to permanently delete all or part of the personal data stored for each user, both manually and automatically.	✓
Data pseudonymization	Xeerpa offers the necessary functionality to transform personal data into anonymous information.	✓
Age gating	Xeerpa provides functionality to prevent the storage of data from users of a certain age.	✓
Proof of Consent	Xeerpa can store metadata associated to the registration process or interactions of a user with your website or app, including the specific terms and conditions that the user accepted at the time of registration or sign up.	✓
Data Location & Data Transfer	Xeerpa offers the option of several hosting locations for the personal data, including servers in the EU and America. International data transfers are also under your control, in compliance with the new regulation.	✓
Facebook Data deletion	Automatic Account Deletion, in the case a user revokes data access permission from your site's Facebook app.	✓
Facebook Data Updates	Automatic Account Updates, in the case a user updates her/ his Facebook profile after registering to your website or app.	✓