ODESSO Cookie Policy

This Cookie Policy describes how ODESSO uses cookies and similar technologies to provide, customize, evaluate, improve, promote and protect our Services. Cookies are small pieces of data stored on a site visitor's browser. They are typically used to keep track of the settings users have selected and actions they have taken on a site. We use cookies on the website and associated domains of www.odesso.com for the following purposes:

1) Authentication, Security, and Personalization - Cookies allow users to access their accounts, retain saved settings, and identify the account devices to prevent fraudulent access to ODESSO services.
2) Analytics and Performance - Cookies allow us to analyze how users interact with ODESSO’s processes, and to track the performance and get insights to provide higher quality service to users.
3) Third Party Access - Some third party sites that partner with ODESSO may require cookies to access their services. All policies third party cookies are used in conjunction with that third party’s separate individual policies.

We may update this Cookie Policy from time to time. When we make changes, we’ll update the “Effective Date” at the top of the Cookie Policy and post it on our sites. We encourage you to check back periodically to review this Cookie Policy for any changes since your last visit.

ODESSO GDPR Policy

The General Data Protection Regulation, or GDPR, is a European privacy law that went into effect May 25, 2018. The GDPR regulates how individuals and organizations may collect, use, and retain personal data, which affects ODESSO and applications run on our platform. If you have visitors or customers in the European Economic Area (EEA), the United Kingdom (UK), or Switzerland, this guide covers what you should know as a ODESSO application owner.

Under the GDPR, personal data is any information that can reasonably identify a specific living person, either alone or with other information. This broad definition includes traditional personal data—like dates of birth, names, physical addresses, email addresses—and location data, biometric data, financial information, and more.

For more information about what is considered personal data in the EU, please see the information pages of the European Commission and Data Protection Commission of Ireland.

In the EU, cookie laws are currently governed by the E-Privacy Directive. The cookie laws in the EU require website owners to take certain steps before dropping non-essential cookies on EU visitors. Websites that drop non-essential cookies must, through a cookie banner, take the following minimum steps:

1. Provide clear and comprehensive information regarding the website's cookie usage.
2. Display that information prominently so visitors can easily access it.
3. Obtain consent from the website visitor to drop the non-essential cookies.

The GDPR requires certain safeguards when transferring personal data from outside the EEA, the UK and Switzerland to "third countries," which are all

countries outside these protected areas, including the United States. We're committed to treating personal data received from the EEA, the UK and Switzerland (as well as personal data received from elsewhere around the world) in a secure and privacy-first way, and processing it in a way that meets the European Commission Standard Contractual Clauses.

European Commission Standard Contractual Clauses

We use Standard Contractual Clauses (also known as Model Contractual Clauses) as the legal basis for transferring personal data to third countries, including the United States. We protect your personal data and have put appropriate technical and organizational safeguards in place to meet these standards.

Other transfer requirements

Articles 45 to 50 of the GDPR set the various requirements for the lawful transfers of personal data to third countries or international organizations that provide an adequate level of protection. These include:

Adequacy

Third countries, specified sectors within third countries, or international organizations have adequacy if the EU Commission determined they provide an adequate level of data protection.

In the absence of an adequacy decision, the GDPR allows a transfer if the controller or processor has provided “appropriate safeguards,” which may include:

- Approved Codes of Conduct or Approved Certification Mechanisms
- Binding Corporate Rules
- Standard Contractual Clauses

Exceptions for specific situations

Exceptions allow transfers in specific situations, like if consent is obtained, or:

- For the performance or conclusion of a contract
- For the exercise of legal claims
- To protect the vital interests of the data subject when they can't give consent or for reasons of public interest

For more information, visit this guidance document from the European Data Protection Board.

We may use other transfer mechanisms to ensure adequate data protection and we'll provide more information, as appropriate, if other transfer mechanisms are used for the lawful transfers of personal data to third countries.

ODESSO asks you to provide your own legal terms or privacy policies to be governed underneath ODESSO’s existing platform-wide policies.

More Information

Regulators within the EU provide specific guidance on the GDPR and Cookies. You can view their documentation here:

- The European Data Protection Board (EDPB)
- Official EU GDPR website
- Bundesministerium des Innern (Germany)
- Commission Nationale de l'Informatique et des Libertés (France)
- Data Protection Commission (Ireland)
- Information Commissioner's Office (UK)
- Agencia Española de Protección de Datos (Spain)
- Full text of the GDPR