General Data Protection Regulation (GDPR)

Last Edited: April 30, 2018

Smooth Fusion is committed to be your trusted, 3rd party GDPR co-processor. To that end, we wish to act as a resource to help you meet GDPR compliance.

You, our business client, own the relationship with your end customers. For the purpose of complying with GDPR, you are therefore the "controller." Because you own the software* and use it to process EU data subject PII, you are also the "processor."

**Smooth Fusion creates custom software for our business clients. The software we create is fully owned by the business client except in cases where software or components may be licensed to our clients.*

Ultimately, successful GDPR compliance is a team effort, with your Data Protection Officer (DPO) acting as the lead. The table below identifies GDPR obligations, what they mean, and how Smooth Fusion can help you meet the obligations.

GDPR is a large and sweeping regulation. Best practices for GDPR are emerging as organizations work to become compliant. Therefore, this list should not be viewed as a comprehensive guide to compliance. This list simply provides a sampling of the kinds of services you can expect from Smooth Fusion.

	What it means	**How we can help**
Lawful basis of processing	You need to have a legal reason to collect and use any PII (personally identifiable information) from your data subjects. You also need to track this “lawful basis.”	Smooth Fusion can verify the PII being collected on your website and work with your DPO to ensure that all PII has a lawful basis. Smooth Fusion can customize your database to track the lawful basis.
Consent	One type of lawful basis is consent. For consent to be compliant, it needs to meet certain criteria like: - “Notice”: The data subject must be told what they’re opting into. - “Opt-in”: The data subject must affirmatively opt-in. They can’t be forced to uncheck a box (opt-out), for example. - “Granular”: Consent must be given for each unique way the data will be used. For example, if the data subject provides consent for “email marketing”, you cannot use that consent to make sales calls to the	Smooth Fusion can help with consent in the following ways: - Work with your DPO to verify that consent meets the criteria spelled out in GDPR. - Implement custom consent forms for your website or application. - Customize your database to ensure that consent is captured correctly. - Review processes and customize integrations to ensure that consent is honored.

	user. Separate consent must be given. - “Clear language”: Consent must be given in clear, non-legal language.	
Withdrawal of consent (or opt out)	Data subjects need to see what they’ve signed up for and withdraw consent.	Smooth Fusion can customize your website or application to allow the data subject to see their consent and remove that consent (opt out). We can also create custom APIs to ensure that withdrawal is honored throughout your organization.
Cookies	Data subjects need to be given notice that the website is using cookies for tracking. The data subject should consent to being tracked by cookies.	Smooth Fusion can implement a cookie notice with a lawful opt-in.
Access / Portability	Data subjects have the right to request access to all PII that you have collected. In the event of a request, you (as the controller) must provide the data in a machine-readable format (e.g. CSV or XLS). Data subjects may also request to see and verify lawful basis of processing.	Smooth Fusion can customize your website or application to programmatically verify the identity of the data subject, gather all PII for the data subject, and deliver the PII in a CSV or any other format. Smooth Fusion can also customize the website to log the request and fulfillment.
Deletion	Data subjects have the right to request that you, the controller, delete all PII belonging to the data subject. GDPR requires this information to be permanently removed from your database or anywhere else it may reside in your organization. The deletion must be completed, and the data subject notified within 30 days. The right to deletion is not absolute. There are exceptions to this right, but the data subject should still be notified.	Smooth Fusion can customize your website to allow a data subject to delete their PII within the website’s database. Many websites share data with other services (“processors”). For example, a website may share data with Google Analytics. Smooth Fusion can help ensure that data is not shared with processors that cannot comply with the deletion right. Smooth Fusion can also build software to programmatically delete the right PII from those processors that can support it.
Modification	Data subjects can request that the you modify their personal data in the event it is inaccurate or incomplete.	Smooth Fusion can customize your website or application to allow data subjects to authenticate and modify their data. Or, Smooth Fusion can customize your website to allow the appropriate employee to make those modifications.
Retention Period	When PII is no longer being used for the reason it was originally collected, it should be deleted. The deletion period should be clearly stated in the privacy policy.	Smooth Fusion can customize your website or application to programmatically delete the data when certain criteria are met. For example, data could be deleted 30 days after

		the data subject unsubscribes from the email newsletter.
Privacy Policy	GDPR requires a privacy policy which makes clear, in non-legal language, what PII is being collected and how it is being used. The privacy policy should state which other processors are involved and how the data subject may go about accessing their rights around the data (access, deletion, modification, etc.)	While Smooth Fusion does not offer policy writing as a service, we can review your privacy policy to ensure that it is accurate within the scope of our involvement. Smooth Fusion can also build a webpage for the privacy policy and link to the policy from any website or application.
Data Breach Policy	GDPR requires controllers to document and execute a reporting policy in the event of data breach.	Smooth Fusion can help analyze suspected data breaches to determine the scope of the breach. We will also be available to work with the DPO to identify and patch any vulnerabilities in technology.
Documentation	GDPR calls for documentation of processing activities, privacy reviews, technical reviews, codes of conduct, impact assessment, etc.	Smooth Fusion will work with the DPO to review the controller's documentation and ensure that the technology meets the stated requirements.
Security Measures		
GDPR does not contain a technical guide to securing PII. GDPR requires "appropriate technical and organizational measures to ensure a level of security appropriate to the risk." Smooth Fusion depends on the controller (you, the client) to define the risk level. Smooth Fusion is your partner to implement security measures to meet the level of risk you have defined. Listed below are some, but not all, of security options we make available to our clients.		
Data Encryption	Smooth Fusion can ensure that website data is encrypted when it is sent and retrieved (transport) and when it is stored (at rest).	
Appropriate Access	Smooth Fusion can customize your website or application to use role-based authorization for employees who are using it. Roles can be created which appropriately limit access to PII to the employees who need it.	
Access Log	Smooth Fusion can customize your website or application to record access to PII. This will allow your company to see who accesses PII and when.	
Pseudonymization and Anonymization	Pseudonymization is a technique which replaces identifying data with pseudonyms. Pseudonymization changes the data such that more information would be required to identify the data subject. Anonymization irreversibly destroys any way of identifying the data subject. Smooth Fusion can implement both of these techniques on data to allow for analytics or other processing.	