Mojaloop GDPR Scope Definition Document

This document defines the scope of Mojaloop in assisting hub operators and their participating digital financial service providers (DFSP's) to comply with the requirements of The General Data Protection Regulation (GDPR). As Mojaloop we are not required to be GDPR compliant since we do not operate a production hub which process privacy data of EU citizens.

1. GDPR Requirements Overview

The General Data Protection Regulation (GDPR), agreed upon by the European Parliament and Council in April 2016, will replace the Data Protection Directive 95/46/ec in Spring 2018 as the primary law regulating how companies protect EU citizens' personal data. Companies that fail to achieve GDPR compliance will be subject to stiff penalties and fines.

GDPR requirements apply to each member state of the European Union, aiming to create more consistent protection of consumer and personal data across EU nations. Some of the key privacy and data protection requirements of the GDPR include:

- Requiring the consent of subjects for data processing
- Anonymizing collected data to protect privacy
- Providing data breach notifications
- Safely handling the transfer of data across borders
- Requiring certain companies to appoint a data protection officer to oversee GDPR compliance

Simply put, the GDPR mandates a baseline set of standards for companies that handle EU citizens' data to better safeguard the processing and movement of citizens' personal data.

The purpose of the GDPR is to impose a uniform data security law on all EU members, so that each member state no longer needs to write its own data protection laws and laws are consistent across the entire EU. In addition to EU members, it is important to note that **any company that markets goods or services to EU residents, regardless of its location**, is subject to the regulation. As a result, GDPR will have an impact on data protection requirements **globally**.

Below Summary of the GDPR requirements:

CATEGORY	REQUIREMENT	DESCRIPTION	ACTION POINTS

Lawful basis and transparency	Conduct an information audit to determine what information you possess and who has access to it.	Organizations that have at least 250 employees or conduct higher-risk data processing are required to keep an up-to-date and detailed list of their processing activities and be prepared to show that list to regulators upon request. The best way to demonstrate GDPR compliance is using a data protection impact assessment Organizations with fewer than 250 employees should also conduct an assessment because it will make complying with the GDPR's other requirements easier. In your list, you should include: the purposes of the processing, what kind of data you process, who has access to it in your organization, any third parties (and where they are located) that have access, what you're doing to protect the data (e.g. encryption), and when you plan to erase it (if possible).	1 - Have an up to date list of our processing activities (https://gdpr.eu/article-30-records-of-processing-activities/) 2 - Conduct a Data Protection Impact Assessment..

	Have legal justification for your data processing activities	Processing of data is illegal under the GDPR unless you can justify it according to one of six conditions listed in Article 6. There are other provisions related to children and special categories of personal data in Articles 7-11. Review these provisions, choose a lawful basis for processing, and document your rationale. Note that if you choose "consent" as your lawful basis, there are extra obligations, including giving data subjects the ongoing opportunity to revoke consent. If "legitimate interests" is your lawful basis, you must be able to demonstrate you have conducted a privacy impact assessment.	1 - Six conditions of Article 6: https://gdpr.eu/article-6-how-to-process-personal-data-legally/ 2 - Provisions relating to children and special categories 3 - Review these provisions, choose a lawful basis for processing, and document your rationale. 4 - If you choose "consent" as your lawful basis, there are extra obligations (https://gdpr.eu/gdpr-consent-requirements/), including giving data subjects the ongoing opportunity to revoke consent. If "legitimate interests" is your lawful basis, you must be able to demonstrate you have conducted a privacy impact assessment.

	Provide clear information about your data processing and legal justification in your privacy policy.	You need to tell people that you're collecting their data and why (Article 12). You should explain how the data is processed, who has access to it, and how you're keeping it safe. This information should be included in your privacy policy and provided to data subjects at the time you collect their data. It must be presented "in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child."	1 - Document privacy policy 2 - Review Article 12: https://gdpr.eu/article-12-how-controllers-should-provide-personal-data-to-the-subject/

Data Security	Take data protection into account at all times, from product development to data processing.	You must follow the principles of "data protection by design and by default," including implementing "appropriate technical and organizational measures" to protect data. In other words, data protection is something you now must consider whenever you do anything with other people's personal data. You also need to make sure any processing of personal data adheres to the data protection principles outlined in Article 5. Technical measures include encryption, and organizational measures are things like limiting the amount of personal data you collect or deleting data you no longer need. The point is that it needs to be something you and your employees are always aware of.	1 - Review Data Protection by Design (https://gdpr.eu/article-25-data-protection-by-design/) 2 - Implementing "appropriate technical and organizational measures" to protect data. 3 - Ensure any processing of personal data adheres to the data protection principles outlined in Article 5 (https://gdpr.eu/article-5-how-to-process-personal-data/). Technical measures include encryption, and organizational measures are things like limiting the amount of personal data you collect or deleting data you no longer need.
	Encrypt, pseudonymize or anonymize personal data whenever possible.	Most of the productivity tools used by businesses are now available with end-to-end encryption built in, including email, messaging, notes, and cloud storage. The GDPR requires organizations to use encryption or pseudeonymization whenever feasible.	1 - Implement encryption 2 - Enforce data protection controls within data processing. (https://gdpr.eu/article-32-security-of-processing/)

	Create an internal security policy for your team members and build awareness about data protection.	Even if your technical security is strong, operational security can still be a weak link. Create a security policy that ensures your team members are knowledgeable about data security. It should include guidance about email security, passwords, two-factor authentication, device encryption, and VPNs. Employees who have access to personal data and non-technical employees should receive extra training in the requirements of the GDPR.	1 - https://gdpr.eu/recital-78-appropriate-technical-and-organisational-measures/
	Know when to conduct a data protection impact assessment and have a process in place to carry it out	A data protection impact assessment (aka privacy impact assessment) is a way to help you understand how your product or service could jeopardize your customers' data, as well as how to minimize those risks.	1 - Document a data protection impact assessment process 2 - Conduct an assessment
	Have a process in place to notify authorities and data subjects in the event of a data breach	If there's a data breach and personal data is exposed, you are required to notify the supervisory authority in your jurisdiction within 72 hours.	1 - Document data breach incident response process 2 - Identify responsible parties (data controllers, data processors e.t.c

Accountability and Governance	Designate someone responsible for ensuring GDPR compliance across the organisation.	Another part of "data protection by design and by default" is making sure someone in your organization is accountable for GDPR compliance. This person should be empowered to evaluate data protection policies and the implementation of those policies.	1 - Establish GDPR Officer role in the organisation (https://gdpr.eu/article-25-data-protection-by-design/)
	Sign a data processing agreement between your organisation and any third parties that process data on your behalf.	This includes any third-party services that handle the personal data of your data subjects, including analytics software, email services, cloud servers, etc. Most services have a standard data processing agreement available on their websites for you to review.	1 - Document listing of third parties 2 - Prepare data processing agreement. (https://gdpr.eu/data-processing-agreement/)
	If your organisation is outside the EU, appoint a representative within the EU member states.	If you process data relating to people in one-member state, you need to appoint a representative in that country who can communicate on your behalf with data protection authorities. The GDPR and its official supporting documents do not give guidance for situations where processing affects EU individuals across multiple member states.	1 - Appoint representative 2 - Document representative roles and responsibilities.

	Appoint a Data Protection Officer (If necessary)	There are three circumstances in which organizations are required to have a Data Protection Officer (DPO), but it's not a bad idea to have one even if the rule doesn't apply to you.	1 - Circumstances requiring having a data protection officer (https://gdpr.eu/data-protection-officer/) 2 - Define DPO Job Description, duties and responsibilities.
Privacy Rights	Its easy for your customers to request and receive all information you have about them.	People have the right to see what personal data you have about them and how you're using it. They also have a right to know how long you plan to store their information and the reason for keeping it that length of time. You have to send them the first copy of this information for free but can charge a reasonable fee for subsequent copies. Make sure you can verify the identity of the person requesting the data. You should be able to comply with such requests within a month.	1 - Reports on customer data 2 - Standard consumer responses on what information we have.
	Its easy for customers to correct or update inaccurate information	Do your best to keep data up to date by putting a data quality process in place and make it easy for your customers to view (Article 15) and update their personal information for accuracy and completeness. Make sure you can verify the identity of the person requesting the data.	1 - Document processes and procedures for customers to request information correction 2 - Document processes for verifying customer information : https://gdpr.eu/article-16-right-to-rectification/

	It is easy for your customers to request to have their personal data deleted.	People generally have the right to ask you to delete all the personal data you have about them, and you have to honor their request within about a month. There are a five grounds on which you can deny the request, such as the exercise of freedom of speech or compliance with a legal obligation. You must also try to verify the identity of the person making the request.	1 - Document what constitutes personal data 2 - Document processes and procedures for deleting personal data.
	It is easy for your customers to ask you to stop processing their data.	Your data subjects can request to restrict or stop processing of their data if certain grounds apply, mainly if there's some dispute about the lawfulness of the processing or the accuracy of the data. You are required to honor their request within about a month. While processing is restricted, you're still allowed to keep storing their data. You must notify the data subject before you begin processing their data again.	1 - Document process for customers to make requests 2 - Implement processes for stopping to process customer data.

	Its easy for your customers to receive a copy of their personal data in a format that can be easily transferred to another company.	This means that you should be able to send their personal data in a commonly readable format (e.g. a spreadsheet) either to them or to a third party they designate. This may seem unfair from a business standpoint in that you may have to turn over your customers' data to a competitor. But from privacy standpoint, the idea is that people own their data, not you.	1 - Create reports to extract customer personal data 2 - Document processes to mark data as "extracted" hence not to be processes any more. 3 - What happens if a request is made to a customer who has asked for no more processing of their data?
	Its easy for customers to object to us processing their data.	If you're processing their data for the purposes of direct marketing, you must stop processing it immediately for that purpose.	1 - Document consent process 2 - Implement methods of effecting consent. 3 - implement methods for revoking / deleting customer data upon their request
	If you make decisions about people based on an automated process, you have a procedure to protect their rights.	Some types of organizations use automated processes to help them make decisions about people that have legal or "similarly significant" effects. If you think that applies to you, you'll need to set up a procedure to ensure you are protecting their rights, freedoms, and legitimate interests. You need to make it easy for people to request human intervention, to weigh in on decisions, and to challenge decisions you've already made.	1 - Review automated and individual decision making (https://gdpr.eu/article-22-automated-individual-decision-making/) 2 - Document appropriate protections employed on data. 3 - Document process for customers to interact with us on matters relating to their interacting and understanding decision processes around their data.

2. Majaloop GDPR Scope

Upon detailed analysis on all the GDPR requirements above, we have identified the following requirements below under data security section to be addressed at Mojaloop level:
Data Security Requirements:

a) Review Data Protection by Design (https://gdpr.eu/article-25-data-protection-by-design/)
b) Implementing "appropriate technical and organizational measures" to protect data.
c) Ensure any processing of personal data adheres to the data protection principles outlined in Article 5 (https://gdpr.eu/article-5-how-to-process-personal-data/).
d) Devise technical measures include encryption, and organizational measures are things like limiting the amount of personal data you collect or deleting data you no longer need.
e) Implement encryption – at rest and at motion
f) Enforce data protection controls within data processing. (https://gdpr.eu/article-32-security-of-processing/)

All the above data security requirements form the core part of the overall GDPR data protection regulation so tackling early in the platform design and development phase of Mojaloop will provide implementers with the much-needed baseline and flexibility to address the rest of the requirements. See summary in the figure below: