LogSentinel

Mapping Between PSD2 Requirements and LogSentinel Functionalities

#	Source of Requirement	Requirement	LogSentinel Functionality
1.	**PSD2, Article 65** – Confirmation on the availability of funds, paragraph 2	A requirement for multiple processes is the explicit consent of the payer. The PSP should demonstrate that this consent has been given and ideally should not be able to back-date or modify consent records.	**Ability to log consent** (and consent withdrawal) in an immutable way so that the PSP can clearly demonstrate that once consent was given, it was not tampered with.
2.	**PSD2, Article 70** - Obligations of the payment service provider in relation to payment instruments	1. The payment service provider issuing a payment instrument shall: (a) make sure that the personalised security credentials are not accessible to parties other than the payment service user that is entitled to use the payment instrument, without prejudice to the obligations on the payment service user set out in Article 69;	Logging access to the security credential storage or **mechanism to be able to demonstrate that no other party has used the credentials.**
3.	**PSD2, Article 70** - Obligations of the payment service provider in relation to payment instruments	1. The payment service provider issuing a payment instrument shall: (d) provide the payment service user with an option to make a notification pursuant to point (b) of Article 69(1) free of charge and to charge, if at all, only replacement costs directly attributed to the payment instrument;	Securely logging the exact moment the user notifies the **PSP loss, theft, misappropriation or unauthorised use of the payment instrument**.
4	**PSD2, Article 72** - Evidence on authentication and execution of payment transactions	1. Member States shall require that, where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider. If the payment transaction is initiated through a payment initiation service provider, the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical	Ability to prove with legal certainty that if a transaction has been logged and chain verification passes successfully, there has been no modifications to the logged data, therefore **proving that the transaction was accurately recorded.**

#	Source of Requirement	Requirement	LogSentinel Functionality
		breakdown or other deficiency linked to the payment service of which it is in charge.	
5	**PSD2, Article 97** - Authentication	Member States shall ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials.	Logging (a hash) of the security credentials will help ensure their integrity, i.e. that **no actor, internal or external, has tampered them**. Regular comparison of actual credentials (e.g. OTP secret keys) to the logged ones can be used to detect tampering.
6	**Commission Delegated Regulation (EU) 2018/389, Article 2** - General authentication requirements, Paragraph 1	Payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions for the purpose of the implementation of the security measures referred to in points (a) and (b) of Article 1.	LogSentinel supports **fraud detection based on the logged information** which can be used to supplement other fraud detection solutions for improved results.
7	**Commission Delegated Regulation (EU) 2018/389, Article 21** – Monitoring, Paragraph 1	In order to make use of the exemptions set out in Articles 10 to 18, payment service providers shall record and monitor the following data for each type of payment transactions, with a breakdown for both remote and non-remote payment transactions, at least on a quarterly basis:	Every transaction can be logged together with the required metadata to ensure that **no modifications have occurred and to prove compliance.**
8	**Commission Delegated Regulation (EU) 2018/389, Article 21 –** Monitoring, Paragraph 2	Payment service providers shall make the results of the monitoring in accordance with paragraph 1 available to competent authorities and to EBA, with prior notification to the relevant competent authority(ies), upon their request.	LogSentinel support "**auditor access**" so that competent authorities are given access to the dashboard to **search through the logged events without additional effort.**

Mapping Between EBA's Guidelines for PSD2 and LogSentinel Functionalities

#	Source of Requirement	Requirement	LogSentinel Functionality
1.	**European Banking Authority** Guidelines on the security measures for operational and security risks of payment services under **Directive (EU) 2015/2366 (PSD2), Guideline 2**: Governance	2.2 The risk management framework should: d) establish the necessary procedures and systems to identify, measure, monitor and manage the range of risks stemming from the payment-related activities of the PSP and to which the PSP is exposed, including business continuity arrangements.	Ability to **log every user or system event**, display them in dashboard and easily retrieve them for measuring and monitoring risk. **Fraud detection capabilities for risk management**.
2.	**European Banking Authority** Guidelines on the security measures for operational and security risks of payment services under **Directive (EU) 2015/2366 (PSD2), Guideline 2:** Governance	2.6 The security measures set out in these Guidelines should be audited by auditors with expertise in IT security and payments and operationally independent within or from the PSP. The frequency and focus of such audits should take the corresponding security risks into consideration	LogSentinel provides **auditor access to the logs and dashboard** to enable IT security audits.
3.	**European Banking Authority** Guidelines on the security measures for operational and security risks of payment services under **Directive (EU) 2015/2366 (PSD2), Guideline 4**: Protection	4.2 PSPs should establish and implement a 'defence-in-depth' approach by instituting multi-layered controls covering people, processes and technology, with each layer serving as a safety net for preceding layers. Defence-in-depth should be understood as having defined more than one control covering the same risk, such as the four-eyes principle, two-factor authentication, network segmentation and multiple firewalls	LogSentinel can serve as an additional/alternative product to the following: • **Existing system logs,** comprising another storage location, and ensuring **log integrity** • **System risk monitoring** through the management dashboard of all connected systems (incl. per system, per database table, per event type, etc.) • **Fraud detection and notification capabilities** for improved risk management
4.	**European Banking Authority** Guidelines on the security measures for operational and security risks of payment services under **Directive (EU) 2015/2366 (PSD2), Guideline 4:** Protection	4.3 PSPs should ensure the confidentiality, integrity and availability of their critical logical and physical assets, resources and sensitive payment data of their PSUs whether at rest, in transit or in use. If the data include personal data, such measures should be implemented in compliance with Regulation (EU) 2016/6796 or, if applicable, Regulation (EC) 45/2001.	LogSentinel provides **complete data integrity** for all information stored within the solution, leveraging a permissioned **blockchain technology**. In case of personal data LogSentinel provides data protection and compliance features, including a **built-in Register under article 30 of the GDPR.**

#	Source of Requirement	Requirement	LogSentinel Functionality
5.	**European Banking Authority** Guidelines on the security measures for operational and security risks of payment services under **Directive (EU) 2015/2366 (PSD2), Guideline 4**: Protection	4.7 […] PSPs should ensure that integrity-checking mechanisms are in place in order to verify the integrity of software, firmware and information on their payment services.	LogSentinel provides **complete data integrity for all information stored** within the solution, leveraging blockchain technology. The chain is subject to complete **verification every 12 hours**, or at other configurable intervals. Internal verification mechanisms also exist, as follows: • Pushing hashes, representing the complete state of all data to external stakeholders via **e-mails** or t**ext message**. • Pushing hashes, representing the complete state of all data to a **public blockchain** (e.g. Bitcoin, Ethereum or any other). • Pushing hashes, representing the complete state of all data to a publicly verifiable source such as **Twitter**. **LogSentinel ensures that it is technically impossible to breach data integrity without detection.**
6.	**European Banking Authority** Guidelines on the security measures for operational and security risks of payment services under **Directive (EU) 2015/2366 (PSD2), Guideline 4:** Protection	4.10 PSPs should institute strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements. Controls such as roles-based access, logging and reviewing of the systems activities of privileged users, strong authentication and monitoring for anomalies should be implemented. […]	LogSentinel provides functionalities **for storing logs of all events or activity in the IT systems**. Particular focus can be given to privileged users with elevated system access or critical systems. **Fraud detection functionalities can be used to comprehensively monitor for anomalies in system activity.**
7.	**European Banking Authority** Guidelines on the security measures for operational and security risks of payment services under **Directive (EU) 2015/2366 (PSD2), Guideline 4:** Protection	4.11 Access logs should be retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in accordance with GL 3.1 and GL 3.2, without prejudice to the retention requirements set out in EU and national law. PSPs should use this information to facilitate identification and investigation	LogSentinel **securely stores logs and allows interactive search across many dimensions** that can facilitate the identification and investigation of anomalous activities. Furthermore, parts of the chain older than a **pre-specified period (e.g. 12 months) can be discarded without compromising verification.**

#	Source of Requirement	Requirement	LogSentinel Functionality
		of anomalous activities that have been detected in the provision of payment services.	
8.	**European Banking Authority** Guidelines on the security measures for operational and security risks of payment services under **Directive (EU) 2015/2366 (PSD2), Guideline 4:** Protection	4.13 The operation of products, tools and procedures related to access control processes should protect the access control processes from being compromised or circumvented. This includes enrolment, delivery, revocation and withdrawal of corresponding products, tools and procedures.	Access control processes critically includes logs of all accesses. LogSentinel **provides complete integrity of those logs, leveraging blockchain technology.**
9.	**European Banking Authority** Guidelines on the security measures for operational and security risks of payment services under **Directive (EU) 2015/2366 (PSD2), Guideline 5**: Detection	5.1 PSPs should establish and implement processes and capabilities to continuously monitor business functions, supporting processes and information assets in order to detect anomalous activities in the provision of payment services. As part of this continuous monitoring, PSPs should have in place appropriate and effective capabilities for detecting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets used in the provision of payment services.	LogSentinel provides functionalities **for real-time monitoring of logging** (i.e. system and user activity) and allowing for rapid visual inspection. In addition to that it leverages fraud detection capabilities that detect anomalous behavior, symptomatic of information security breaches. Regular chain verification ensures quick detection of integrity breaches.
10.	**European Banking Authority** Guidelines on the security measures for operational and security risks of payment services under **Directive (EU) 2015/2366 (PSD2), Guideline 5**: Detection	5.4 PSPs should determine appropriate criteria and thresholds for classifying an event as an operational or security incident, as set out in the 'Definitions' section of these Guidelines, as well as early warning indicators that should serve as an alert for the PSP to enable early detection of operational or security incidents.	LogSentinel **detects anomalous activity** in critical systems or **by users with high privileges** and those signals can serve as an alert to enable **early detection of operational or security incidents.**
11.	**European Banking Authority** Guidelines on the security measures for operational and security risks of payment services under **Directive (EU) 2015/2366 (PSD2), Guideline 8**: Situational awareness and continuous learning	8.2 PSPs should analyse operational or security incidents that have been identified or have occurred within and/or outside the organisation. PSPs should consider key lessons learned from these analyses and update the security measures accordingly.	LogSentinel securely stores logs and allows interactive search across many dimensions that **can facilitate the identification and investigation of security incidents**.

LogSentinel

Review our enterprise solutions:
https://logsentinel.com/pricing/