

GDPR Data Protection Impact Assessment for Lumen Pay B.V. Buy-Now-Pay-Later Service

October 2026

Contents

- 1 Description of Processing Activities and Context
- 2 Necessity and Proportionality Assessment
- 3 Lawful Basis and Consent Mechanism Validation
- 4 Data Flows, Controllers, and Processor Inventory
- 5 International Data Transfers and Transfer Safeguards
- 6 Risk Register: Likelihood, Severity, and Initial Risk Level
- 7 Technical and Organisational Measures to Reduce Risks
- 8 Residual Risk Evaluation and Acceptance Statement
- 9 Data Protection Officer Advice and Formal Sign-Off

Description of Processing Activities and Context

Lumen Pay B.V., established in Amsterdam, operates a buy-now-pay-later (BNPL) application that facilitates short-term consumer credit. The core processing activity involves collecting and analyzing open-banking transaction data to perform real-time affordability checks. This assessment covers the end-to-end lifecycle of personal data from user initiation through the mobile application to the final credit decision and subsequent repayment monitoring.

The primary data subjects are retail consumers residing in the European Economic Area (EEA). Lumen Pay B.V. acts as the data controller for the credit assessment and customer management processes. Third-party Account Information Service Providers (AISPs), regulated under PSD2, act as processors or independent controllers depending on the specific contractual arrangement, facilitating the secure retrieval of transaction history from users' bank accounts. Core banking partners and cloud infrastructure providers also process data under strict Article 28 GDPR agreements.

Data Category	Specific Elements	Source	Purpose
Identity Data	Name, date of birth, address, national ID number	User Input / KYC Provider	Identity verification and fraud prevention
Financial Transaction Data	Incoming/outgoing transfers, merchant names, balances, recurring payments	Open Banking API (via AISP)	Affordability assessment and credit scoring
Device and Usage Data	IP address, device ID, app interaction logs	Mobile Application	Security, fraud detection, and service improvement

Technical Architecture Note. The system utilizes a microservices architecture hosted within an EEA-compliant cloud environment. Data ingestion from AISPs is performed via encrypted APIs. Raw transaction data is parsed and normalized before being stored in a segregated database for analysis. Access to raw financial data is restricted to automated algorithms for scoring, with human review limited to anonymized or pseudonymized risk flags unless explicit consent for manual review is granted during dispute resolution.

Necessity and Proportionality Assessment

Processing open-banking transaction data is strictly necessary for Lumen Pay B.V. to perform the real-time affordability assessments required for its buy-now-pay-later (BNPL) service. Traditional credit bureau data often lacks the granularity required to assess short-term cash flow volatility for thin-file customers. By analyzing income regularity and essential expenditure patterns directly from bank accounts, Lumen Pay can prevent over-indebtedness more effectively than static credit scores. This direct assessment constitutes the least intrusive means to achieve the dual purpose of responsible lending and fraud prevention, as alternative

methods such as manual payslip verification introduce significant friction and higher risks of document forgery.

Data Minimisation Protocol. Lumen Pay applies strict filtering at the ingestion layer. Only transaction metadata relevant to affordability (date, amount, counterparty category) is retained. Merchant names are categorised immediately, and raw merchant details are discarded unless required for fraud investigation. Account balances are snapshot only at the time of assessment and not stored historically.

Proportionality is enforced through rigid retention policies aligned with the Dutch Autoriteit Persoonsgegevens guidance on financial data. Affordability assessment results are retained for the duration of the active credit facility plus a statutory limitation period for dispute resolution, currently estimated at five years. Raw transaction data used for the initial check is deleted within 30 days of the decision, unless the user explicitly consents to longer storage for personalised financial insights. This ensures that the privacy impact remains proportional to the commercial benefit and risk mitigation achieved. The system architecture supports automated deletion triggers to ensure compliance without manual intervention.

Data Category	Purpose	Retention Period	Deletion Method
Raw Transaction Data	Initial Affordability Check	30 days post-decision	Automated cryptographic erasure
Affordability Score	Credit Risk Management	Duration of contract + 5 years	Secure archive then deletion
User Consent Logs	Regulatory Compliance	7 years	Secure archive then deletion

Lawful Basis and Consent Mechanism Validation

Lumen Pay B.V. processes open-banking transaction data for affordability checks based on explicit consent under Article 6(1)(a) GDPR. To meet EDPB Guidelines on consent, the mechanism ensures consent is freely given, specific, informed, and unambiguous. Users must actively opt in via a granular interface that separates consent for AIS access from general terms of service. Pre-ticked boxes or bundled consent are strictly prohibited. The system records the timestamp, IP address, and version of the privacy notice presented to ensure auditability.

EDPB Compliance Note. Consent for AIS access must be distinct from other contractual consents. Withdrawal of consent must be as easy as giving it, triggering immediate cessation of data collection and initiation of deletion protocols.

For internal risk scoring and fraud prevention, Lumen Pay relies on legitimate interest under Article 6(1)(f) GDPR. A Legitimate Interest Assessment (LIA) has been conducted to balance business needs against user rights. The processing is necessary for creditworthiness evaluation where no less intrusive alternative exists.

Data minimization is enforced by limiting analysis to transaction metadata and amounts, excluding sensitive category details unless explicitly required for affordability logic. Users retain the right to object to this processing, which will be evaluated on a case-by-case basis.

Processing Activity	Lawful Basis	GDPR Article	Verification Status
AIS Data Collection	Explicit Consent	Art. 6(1)(a)	Validated
Affordability Scoring	Legitimate Interest	Art. 6(1)(f)	LIA Completed
Fraud Detection	Legitimate Interest	Art. 6(1)(f)	LIA Completed

Data Flows, Controllers, and Processor Inventory

The processing lifecycle begins when the user provides explicit consent via the Lumen Pay mobile application to access their bank account data. This consent triggers a request to the Account Information Service Provider (AISP), which acts as a processor on behalf of Lumen Pay B.V. (the Controller). The AISP retrieves transaction history from the user's bank using PSD2-compliant APIs. Lumen Pay does not store raw banking credentials because authentication is handled entirely within the bank's secure environment or via the AISP's certified interface.

Transaction data is transmitted from the AISP to Lumen Pay's core processing engine hosted on a cloud infrastructure provider located within the European Economic Area (EEA). All data in transit is encrypted using TLS 1.3. Upon receipt, the data is pseudonymised before being stored in the affordability assessment database. The cloud provider operates under a signed Article 28 Data Processing Agreement, with specific technical safeguards detailed in Annex II of the contract.

Entity Role	Entity Name/Type	Location	Data Processed	Contractual Reference
Controller	Lumen Pay B.V.	Amsterdam, NL	User profile, credit decision	Internal Policy
Processor (AISP)	Licensed EU AISP Partner	EU/EEA	Transaction history, account balance	Article 28 DPA, Annex I
Processor (Cloud)	Cloud Infrastructure Provider	EU/EEA	Pseudonymised transaction data	Article 28 DPA, Annex II
Sub-processor	Monitoring & Logging Tool	EU/EEA	System logs, IP addresses	Article 28 DPA, Annex III

Article 28 Compliance Note. All processors listed above have signed Data Processing Agreements that strictly prohibit using personal data for their own purposes. Annexes I-III of these agreements specify the subject matter, duration, nature, and purpose of processing, as required by GDPR Article 28(3). Confirm current signed versions are on file before final submission.

Data retention is enforced through automated deletion triggers. Once the affordability check is complete and the BNPL agreement is either finalized or rejected, raw transaction data is deleted from the active processing environment within 30 days, unless required for regulatory anti-money laundering (AML) compliance. Aggregated, anonymized statistical data may be retained for model improvement, but this data no longer constitutes personal data under GDPR.

International Data Transfers and Transfer Safeguards

Lumen Pay B.V. operates primarily within the Netherlands and the broader European Economic Area (EEA). The core architecture for the buy-now-pay-later affordability assessment is designed to keep all personal data, including open-banking transaction records and credit scoring inputs, within EEA borders. Data is processed on cloud infrastructure provided by EU-based regions of major providers, ensuring that primary storage and computation do not trigger international transfer mechanisms under Article 44 GDPR.

Schrems II Compliance Note. Following the Court of Justice of the European Union's decision in Schrems II, Lumen Pay conducts regular assessments of any third-country laws that might impinge on the effectiveness of transfer safeguards. No data is transferred to jurisdictions without an adequacy decision unless supplementary measures are strictly enforced.

Certain specialized subprocessors, such as specific fraud detection analytics engines or backup disaster recovery sites, may be located outside the EEA. In these instances, Lumen Pay ensures that transfers are governed by the European Commission's Standard Contractual Clauses (SCCs) adopted in June 2021 (Decision 2021/914). These clauses are integrated into Article 28 Data Processing Agreements with all relevant vendors. Where SCCs are used, a Transfer Impact Assessment (TIA) is conducted to evaluate the legal environment of the destination country.

Recipient Category	Location	Transfer Mechanism	Supplementary Measures
Cloud Infrastructure Provider (Primary)	EU (Netherlands/Ireland)	No transfer required (EEA)	ISO 27001 Certification
Fraud Analytics Subprocessor	United States	EU-US Data Privacy Framework / SCCs	Encryption in transit; Pseudonymisation of direct identifiers
Backup Disaster Recovery	Switzerland	Adequacy Decision	Contractual audit rights; Access logging

To mitigate risks associated with non-EEA transfers, Lumen Pay implements technical supplementary measures including end-to-end encryption for data in transit and strict pseudonymisation of customer identifiers before any data is accessible to non-EEA support personnel. Organizational measures include contractual obligations granting Lumen Pay the right to audit subprocessor compliance and immediate

notification requirements for any government access requests. These measures align with EDPB Recommendations 01/2020 on supplementary measures.

Ongoing Monitoring Requirement. The validity of adequacy decisions and the legal landscape of third countries are subject to change. Lumen Pay commits to reviewing the status of all international transfer mechanisms annually or upon significant legal changes in the destination country.

Risk Register: Likelihood, Severity, and Initial Risk Level

This section catalogs identified data protection risks associated with the processing of open-banking transaction data for affordability checks. Risks are assessed using a standardised 5x5 matrix evaluating likelihood and severity, aligned with EDPB Guidelines 04/2020 Annex I. The initial risk levels determine the priority for mitigation measures.

Risk ID	Description	Likelihood (1-5)	Severity (1-5)	Initial Risk Level
R01	Unauthorised access to open-banking transaction data via API vulnerability	3	5	High
R02	Inaccurate affordability assessment leading to unfair credit denial	2	4	Medium
R03	Failure to obtain valid consent for AIS access per EDPB standards	2	5	High
R04	Data retention beyond necessary period for credit decisioning	3	3	Medium
R05	International transfer of data to non-EEA subprocessor without adequate safeguards	1	5	Medium

Severity (1-5)



Figure 1. Severity (1-5)

Assessment Methodology Note. Likelihood and severity scores are indicative estimates based on current architecture. Confirm specific threat intelligence findings and vendor security posture before final submission to the Dutch Autoriteit Persoonsgegevens.

Technical and Organisational Measures to Reduce Risks

Lumen Pay B.V. has implemented a layered security framework to protect personal data throughout its lifecycle, from acquisition via Account Information Service Providers (AISPs) to final deletion. The following measures address the risks identified in the preceding risk register to ensure that data processing remains secure, confidential, and integral. These controls are subject to regular review and update to reflect evolving threats and regulatory guidance from the Dutch Autoriteit Persoonsgegevens and the European Data Protection Board.

Encryption and Access Control Mechanisms

All personal data, including open-banking transaction records and user identity information, is encrypted in transit using TLS 1.3 or higher and at rest using AES-256 encryption. Key management is handled via a dedicated Hardware Security Module (HSM) service, ensuring that decryption keys are never stored in plain text alongside the data. Access to production databases is strictly limited to authorised personnel through role-based access control (RBAC) and multi-factor authentication (MFA). All access logs are immutable and retained for audit purposes for a period of twelve months.

Dynamic Consent Management. A dynamic consent dashboard allows users to view exactly which data points have been accessed by Lumen Pay, revoke consent for future accesses instantly, and request immediate deletion of their historical data. This interface ensures that consent remains specific, informed, and unambiguous, aligning with EDPB guidelines on valid consent mechanisms.

Data Minimisation and Automated Retention

To adhere to the principle of storage limitation, Lumen Pay employs automated data deletion triggers. Raw transaction data used for affordability checks is pseudonymised immediately after the credit decision is rendered. Full personal identifiers are separated from financial behaviour data. If a user does not proceed with a loan application, their data is automatically deleted within thirty days. For active customers, data is retained only for the duration of the contract plus the statutory limitation period for financial claims, after which it is securely erased. This process is verified through quarterly internal audits.

Risk Category	Control Measure	Frequency/ Trigger	ISO 27001 Alignment
Unauthorised Access	Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC)	Continuous enforcement	A.9.2 User Access Management
Data Breach/Leakage	AES-256 Encryption at Rest and TLS 1.3 in Transit	Continuous enforcement	A.8.24 Cryptography
Excessive Data	Automated Deletion Scripts and	Daily batch	A.8.10 Information Deletion

Risk Category	Control Measure	Frequency/ Trigger	ISO 27001 Alignment
Retention	Pseudonymisation	processing	
System Vulnerability	Quarterly Penetration Testing and API Rate Limiting	Quarterly / Real-time	A.8.8 Technical Vulnerability Management

Lumen Pay conducts quarterly penetration testing performed by an independent third-party security firm to identify and remediate vulnerabilities in the application and infrastructure layers. API rate limiting is enforced to prevent scraping or excessive data requests that could indicate malicious activity or system abuse. Incident response procedures are tested biannually through tabletop exercises to ensure rapid detection, reporting, and mitigation of any potential data breaches, complying with the 72-hour notification requirement under Article 33 GDPR.

Residual Risk Evaluation and Acceptance Statement

Following the application of the technical and organisational measures detailed in the mitigation plan, all previously identified critical and high risks have been reduced to medium or low levels. The residual risk profile is now aligned with Lumen Pay B.V.'s risk appetite and the requirements of Article 32 GDPR. No critical risks remain open. Two medium-level residual risks regarding potential API latency affecting user experience and minor discrepancies in third-party AISP data formatting have been accepted. These are monitored via continuous automated logging and quarterly review cycles. The Chief Information Security Officer and the Data Protection Officer confirm that the remaining risks are proportionate to the benefits of the service and do not pose a high risk to the rights and freedoms of data subjects.

Formal Acceptance. The residual risks documented herein are formally accepted by the CISO and DPO as of October 14, 2026. This acceptance is contingent upon the continued adherence to the monitoring schedule and the immediate escalation of any new threats identified during operational use.

Risk ID	Description	Initial Level	Mitigation Applied	Residual Level	Status
R-01	Unauthorised access to transaction data	Critical	End-to-end encryption, MFA, strict IAM	Low	Closed
R-02	Excessive data retention	High	Automated deletion scripts, 13-month limit	Low	Closed
R-03	AISP API latency	Medium	Caching strategy, fallback providers	Medium	Accepted
R-04	Data formatting inconsistencies	Medium	Standardisation layer, manual review queue	Medium	Accepted

Risk ID	Description	Initial Level	Mitigation Applied	Residual Level	Status
					ed

Data Protection Officer Advice and Formal Sign-Off

The Data Protection Officer has conducted an independent review of this Data Protection Impact Assessment regarding the processing of open-banking transaction data for affordability checks. The assessment confirms that the processing activities described herein comply with the requirements of Articles 35 and 36 of the General Data Protection Regulation. The methodology aligns with guidance issued by the European Data Protection Board and the Dutch Autoriteit Persoonsgegevens regarding high-risk processing in financial services.

DPO Opinion. The DPO advises that the residual risks identified in this assessment are acceptable provided the technical and organisational measures are implemented as specified. No prior consultation with the supervisory authority is required at this stage, as all high risks have been mitigated to an acceptable level.

This sign-off is valid from October 14, 2026. Any material change to the processing architecture, data categories, or third-party processors requires a fresh review of this DPIA. The CISO and Product Owner must confirm that all mitigation controls are operational before full market launch.

Role	Name	Status	Date
Data Protection Officer	To be confirmed	Approved	October 14, 2026
Chief Information Security Officer	To be confirmed	Accepted	October 14, 2026
Managing Director, Lumen Pay B.V.	To be confirmed	Authorized	October 14, 2026