

LatentView Analytics

Response to RFP for

ProSiebenSat.1 Media SE

**DevOps – AWS Analytics Platform**

April 12, 2019

LATENTVIEW ANALYTICS GMBH & AFFLIATES  
Karlstr. 35 80333 München Germany

| [Sales@LatentView.com](mailto:Sales@LatentView.com) | www.LatentView.com

This page is left blank intentionally.

Contents

[1.0 Executive Summary 2](#_Toc5972720)

[2.0 LatentView Overview 3](#_Toc5972721)

[2.1 About LatentView 3](#_Toc5972722)

[2.2 Key Differentiating factors 3](#_Toc5972723)

[2.3 Our Achievements 4](#_Toc5972724)

[2.4 LatentView’s Key Capabilities in Data Engineering 4](#_Toc5972725)

[2.5 Data Engineering - Case Studies 5](#_Toc5972726)

[3.0 Project Objectives & Scope 6](#_Toc5972727)

[3.1 Objective 6](#_Toc5972728)

[3.2 Scope 6](#_Toc5972729)

[4.0 Proposed Solution 7](#_Toc5972730)

[4.1 Solution Architecture 7](#_Toc5972731)

[4.2 Tools and technologies 8](#_Toc5972732)

[4.3 Schedule & Planning 8](#_Toc5972733)

[4.4 Sprint activities 9](#_Toc5972734)

[4.5 Sprint schedule 9](#_Toc5972735)

[5.0 LatentView Solution Approach to implement Dev-Ops 10](#_Toc5972736)

[5.1 DevOps Activities 10](#_Toc5972737)

[5.2 DevOps Workflow 11](#_Toc5972738)

[5.3 LatentView’s suggested Best practices for Dev-Ops 11](#_Toc5972739)

[6.0 Pricing and Payment terms 12](#_Toc5972740)

[6.1 PRICING: 12](#_Toc5972741)

[6.2 Payment Terms 12](#_Toc5972742)

[7.0 Operations 13](#_Toc5972743)

[7.1 Proposed team structure 13](#_Toc5972744)

[7.2 Roles and Responsibilities 13](#_Toc5972745)

[7.3 Time Zone Management 14](#_Toc5972746)

[7.4 Service level agreements 15](#_Toc5972747)

[7.5 Assumptions and prerequisites 17](#_Toc5972748)

[7.6 Progress Meetings 18](#_Toc5972749)

[7.7 Escalation Mechanism 18](#_Toc5972750)

[8.0 Risk Management 19](#_Toc5972751)

[8.1 Identified major risks 19](#_Toc5972752)

[8.2 Business Continuity and Disaster Recovery 20](#_Toc5972753)

[8.3 Quality Assurance 20](#_Toc5972754)

[8.4 Data Security & GDPR 21](#_Toc5972755)

# Executive Summary

LatentView is glad to participate in the ProSiebenSat’s RFP process for identifying a partner for DevOps for AWS Analytics Platform. Based on our detailed review of the RFP, LatentView strongly believes that it is uniquely positioned to meet and exceed the expectations of ProSiebenSat. LatentView seeks to highlight the following credentials for being considered as ProSiebenSat’s vendor of choice:

**Experienced Analytics Player:** LatentView is one of the fastest growing pure play analytics services firms. We have extensive experience in **setting up Analytics Centers of Excellence** for many Fortune 500 firms and delivering a complete range of analytics solutions. Our analytics offerings include **Data Engineering,** **Business Intelligence**, **Data Insights** and **Advanced Analytics**.

**Data engineeting expertise:** Data engineering is a priority focus for us and we are currently supporting multiple global clients in this domain. Collectively **30%+ of our workforce** is involved in supporting clients in this field. Our clientele includes one of the **largest automobile manufacturer in Germany**, a **US based food distribution company**, multiple US based **large technology and e-commerce companies**.

Among these firms we have worked across the **value chain** in areas such as **setting up cloud infrastrucutre**, **building data pipelines**, **Big data migration**, **on-premise hadoop cluster management**, etc. We are **currently working** with the ProSiebenSat Digital data GmBH team in their **cloud migration pilot**.

**Client Focus:** LatentView’s motto is to be the “Trusted Analytics Partner of Choice” for our clients in making informed decisions with data. We have over **90% client retention** over the years since inception due to our strong focus on our clients’ business needs. We at LatentView believe in building long-standing deep relationship with our clients and scale along with their ambitions. Often, we go beyond the call of duty in exceeding the customer expectations. Our customers’ feedback stands a testimony to this fact.

**Thought Leader in Analytics:** LatentView strongly believes in fostering innovation and thought leadership at the core of its culture. Employees are constantly encouraged to explore latest technologies, research on emerging trends, publish research articles and develop innovative solutions.

**Right mix of People**: Our business model and strategy is dependent on the talent we acquire and the training we put them through. From our practice we have come to believe that successful analytics implementations require the right mix of **business acumen**, **maths** skills and **data management** skills. To have a sneak peak into our work culture kindly visit this link : <https://www.latentview.com/work-culture/>

# LatentView Overview

* 1. About LatentView

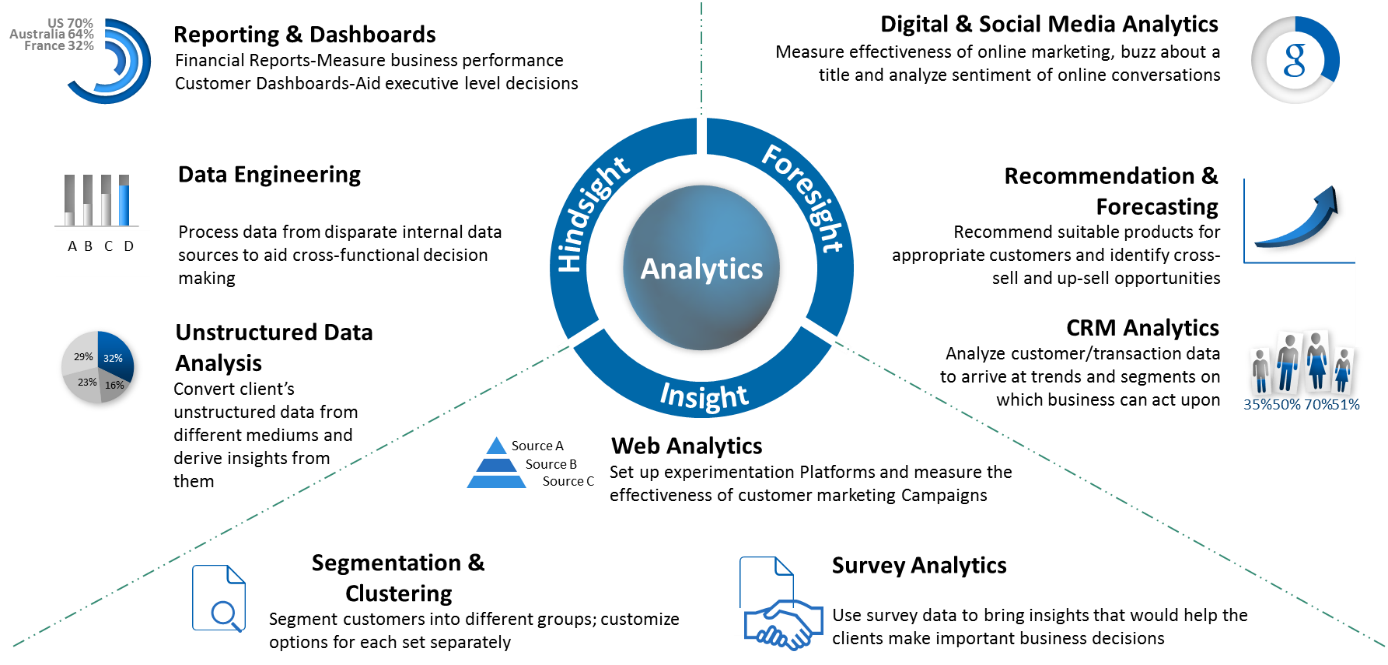
LatentView’s blend of business knowledge, expertise in quantitative methods, and data management helps us provide end to end business solution, as depicted in below figure

Figure: About Latentview

**Geographic Coverage:** LatentView is headquartered in Princeton, NJ with its global delivery center located in Chennai, India and it has multiple offices across the world including the USA, Germany, London, Singapore and the UK. LatentView has invested in getting the right combination of team members at/ near client locations to service the client’s needs. By combining its client-servicing intent, people skills and enabling investments, LatentView has successfully delivered projects in many countries such as Australia, New Zealand, Netherlands, Germany, UK, Brazil, Qatar, China, Italy, India and the USA.

* 1. Key Differentiating factors

1. **Leaders in Unstructured Data Analytics with Strong Industry Partnerships:** LatentView has helped several clients use **unstructured** data such as text, in addition to traditional structured data to derive insights across their business functions.
2. **Deep Cloud Expertise:** LatentView has advance partnership with cloud providers such as AWS, Microsoft Azure to implement Data Engineering solutions. LatentView also has strong partnerships with leaders in the industry such as Microsoft, Amazon, Tableau, and LiveRamp.
3. **Academic Collaboration:** LatentView has set up an Analytics Research Lab in IIT Madras, one of the premium technical institutes in India that allows it to partner with the academia to work and research on cutting edge analytical problems and produce the best-in-class solution frameworks relevant to its customers.
4. **IdeaLabs:** The key for generating, sustaining and profiting from innovation is have an eco-system that breeds novelty. LatentView’s IdeaLabs is such an initiative which is structured to harness the intrinsic breadth and depth of LatentView’s analytical capabilities, which are augmented by academic alliances with leading technology schools and strategic partnerships for sharing disruptive innovation with technology pioneers.
5. **AI/ML Expertise**: LatentView has developed solutions towards solving problems across NLP, Video and Image Analytics with advanced Machine Learning & Deep Learning models.
   1. Our Achievements

* LatentView is a recipient of the prestigious ‘Analytics Solutions Provider of the Year’ at the 2017 Frost & Sullivan India Digital Transformation Awards
* LatentView has been a proud winner of the Deloitte Technology Fast 50 in India for eight consecutive years (2009 - 2017), a testimony to the strong growth and engagement record with our clients
* LatentView was recognized as “Cool Vendors in Analytics” by Gartner.
* Awarded as one of the Top 20 emerging companies in the field of analytics in IE20, London
  1. LatentView’s Key Capabilities in Data Engineering

LatentView’s key capabilities in data engineering is oriented towards moving clients from traditional data architecture to new age data systems in a structured fashion. LatentView’s data engineering framework is a five-step process with business needs aligned to LatentView capabilities and a feedback mechanism for continuous evaluation and improvement. Some of the key features are:

* Ability to handle all data types (unstructured, external)
* Capabilities like Agile data discovery, real-time querying, machine learning workbench
* Timely data through real time streaming ingestion
* Rapid experimentation through sandboxes
* Accountable Infrastructure Management
  1. Data Engineering - Case Studies
     1. Case Study – I: Recommendation System To Increase Share of Wallet

|  |  |
| --- | --- |
| Client | The client is the largest food distribution company in the United States |
| Problem | In an industry where customer acquisition is fairly expensive, this company’s repeat orders were at a low 4% |
| Solution | Provided a robust scalable platform to access unified data and demonstrated the use case to improve product discoverability using an innovative recommendation engine that combined customer segmentation, user-based collaborative filtering and market basket analysis |
| Impact | 20% increase in value of new orders from existing customers.  Higher customer satisfaction due to precise recommendations |
| Technologies & Techniques | AWS Data Lake with (S3, RedShift, Lambda, Glue, Athena, Dynamo DB, Elastic Search, Cognito etc.), Distributed Processing with Spark, Hive & R, PySpark, MLLib, D3, Highcharts  Collaborative filtering & Market Basket analysis |
| Operations & Roadmap | LatentView continues to own both the operation and maintenance of the data platform and the client visualization layer. New use cases for the data platform are being evaluated and a detailed roadmap for implementation was prepared |

* + 1. Case Study – II: Market Trends from Transactional Data

|  |  |
| --- | --- |
| Client | The client is a major multi-national e-commerce market place giant |
| Problem | In a highly competitive e-commerce space it is important to keep the interestingness of the marketplace / offerings to enhance customer experience, drive user and transaction growth |
| Solution | LatentView built a real-time platform to visualize market trends, purchase trends, popular items etc. for any search/product term from 4TB of historic transaction data over 3 years with a response time lesser than 1000 ms |
| Impact | 20% of platform users (32% of searches) visited the marketplace website and contributed to a 3% uptick in transactions in select categories |
| Tools, Technologies & Techniques | Apache Hadoop, Apache Knox, Teradata, Kafka, Hive, Elastic Search, Bootstrap, NodeJS, Log Stash, AngularJS, jQuery |
| Operations & Roadmap | LatentView built this as a fully automated system requiring minimal maintenance. The focus of the ongoing engagement was to make incremental improvements, perform monthly maintenance activities, monitor the platform adoption, and ROI |

# Project Objectives & Scope

* 1. Objective

ProSiebenSat.1 Media SE (ProSieben) is a European mass media company, based in Germany. It operates free-to-air commercial TV channels, pay television channels, radio stations and related print businesses. It also has subscription-based streaming media service, which offers online streaming of a library of films and television programs. ProSiebenSat.1 is also involved in original content production which is made available through the digital platforms.

ProSieben’s digital team is working on an initiative to create a unified digital strategy to increase its presence in the digital media. This requires rapid mining & analysis of various of sources of data in the Raw Data Hub (RDH) using advanced analytics aided by enhanced computing. ProSieben aims to leverage cloud solutions to achieve a high availability data lake for this in conjunction with on premise data lake to support this strategy.

ProSieben data assets are currently stored in a centralized Hadoop cluster maintained and operated by the IT team. The Raw Data Hub (RDH) is hosted in one of the nodes in this larger cluster (Size > 600TB as of Feb’19 – double digit growth rate). Availability, space & compute constraints in the on-premise larger Hadoop cluster require the expansion into an efficient & cost-effective cloud solution.

* 1. Scope

ProSieben is currently in the process of delivering a project to extend and migrate the on premise HDFS based Raw Data Hub and its use cases into a cloud analytics platform by building the data lake and analytics environment on Amazon AWS infrastructure to improve performance through scalability while reducing the load on the on-premise cluster.

|  |  |
| --- | --- |
|  | * To support the initial data migration of 600TB of on-prem data using Snowball out based on the agreed order of priority. * Continue to design & extend the S3 based Data lake in AWS in **DevOps** mode. * Maintain the data model/schema in S3 same as the existing sources in RawDataHub * Build a scheduled, automated continuous ingestion pipeline in AWS. * Extend the existing data consumption layer for Business enablement team and data science team for quick and easy analytics. * S3 architecture shall be based on an understanding of Functional data landscape – RDH and its respective data sources. |

|  |  |
| --- | --- |
| Out of Scope Activities | |
|  | * Any reverse migration of data from AWS S3 to on-premise systems are out of scope of the current project. * Data sources other than the ones identified in the requirement gathering meetings will not be part of the current project. * Development of analytics use cases will not be part of the current project |

# Proposed Solution

* 1. Solution Architecture

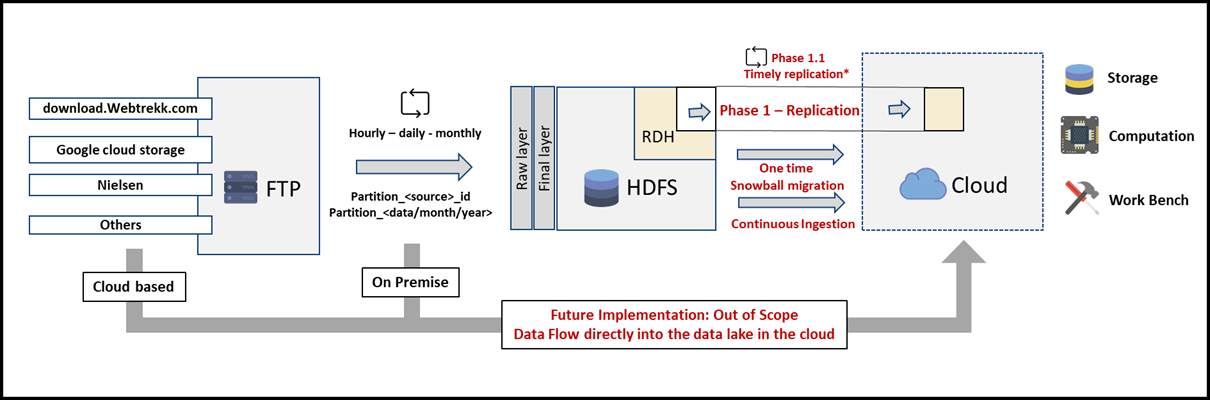


Figure: Current Migration landscape

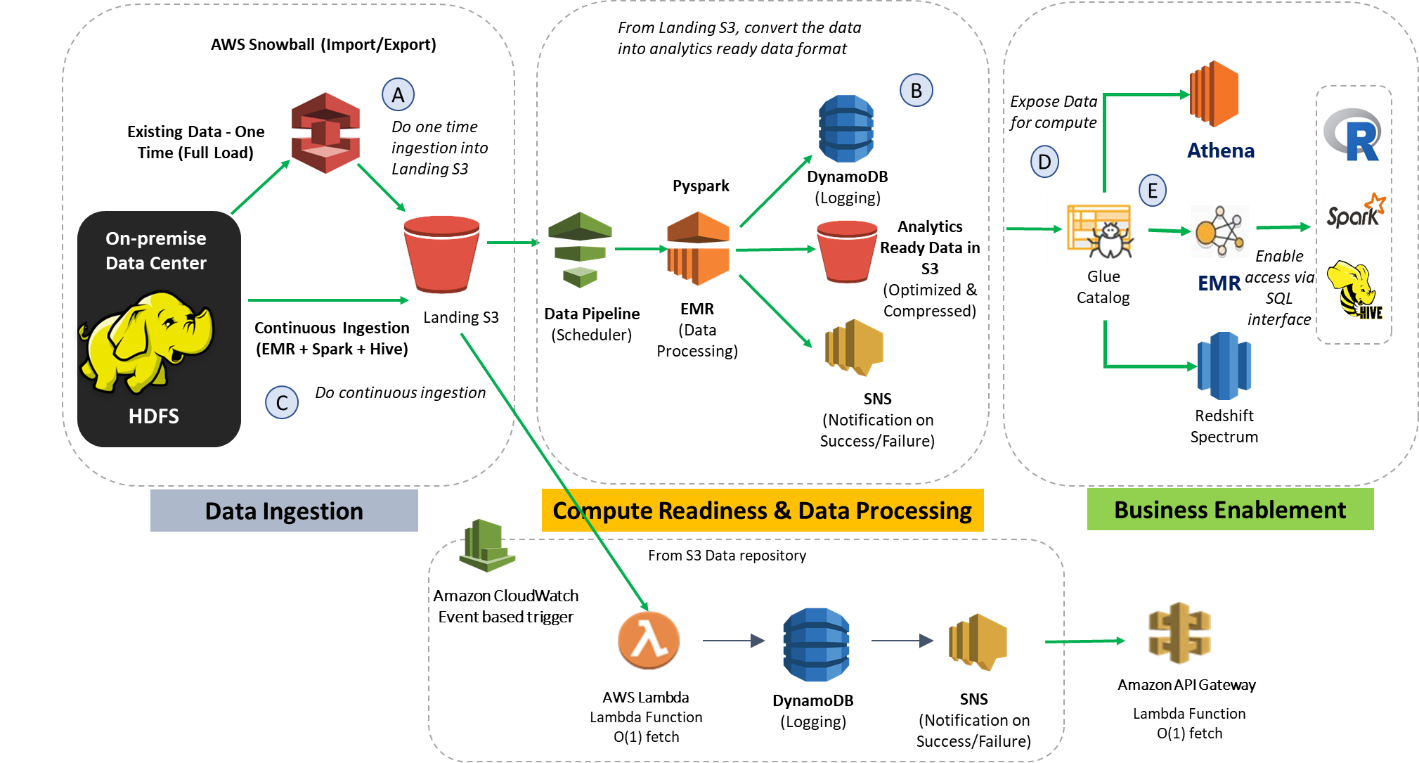
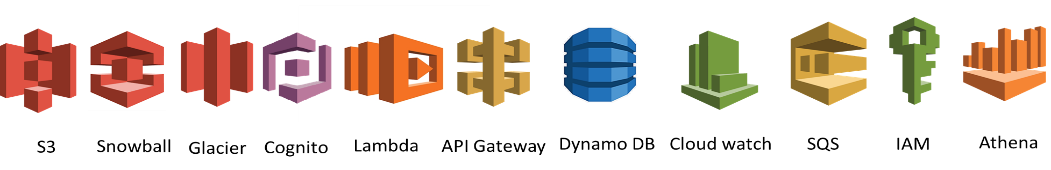
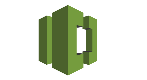


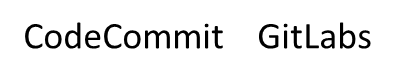
Figure : Suggested Technology architecture

* 1. Tools and technologies

LatentView plans to use the following components from Amazon AWS platform for building the solution. The choices of technology & stack have been finalized based on our understanding of the project scope and can be revised after having discussions with ProSieben.



|  |  |
| --- | --- |
| **AWS Services** | **Purpose** |
| **S3** | Storage |
| **AWS Snowball** | Data Migration |
| **AWS Glacier** | Data persistence (cold) |
| **Amazon Cognito** | Authentication |
| **AWS Lambda** | Responsive processing/logging, Microservices |
| **API Gateway** | REST endpoint for API to access data packages |
| **DynamoDB** | For Content, Storage & Data Model Metadata |
| **Cloud Watch Logs** | Audit & Monitoring |
| **SQS/SES** | Message Passing & Alerting |
| **IAM** | User Access Control |
| **Athena** | On demand analytics |
| **AWS CodeCommit** | Version control service |
| **GitLab** | Repository manager |

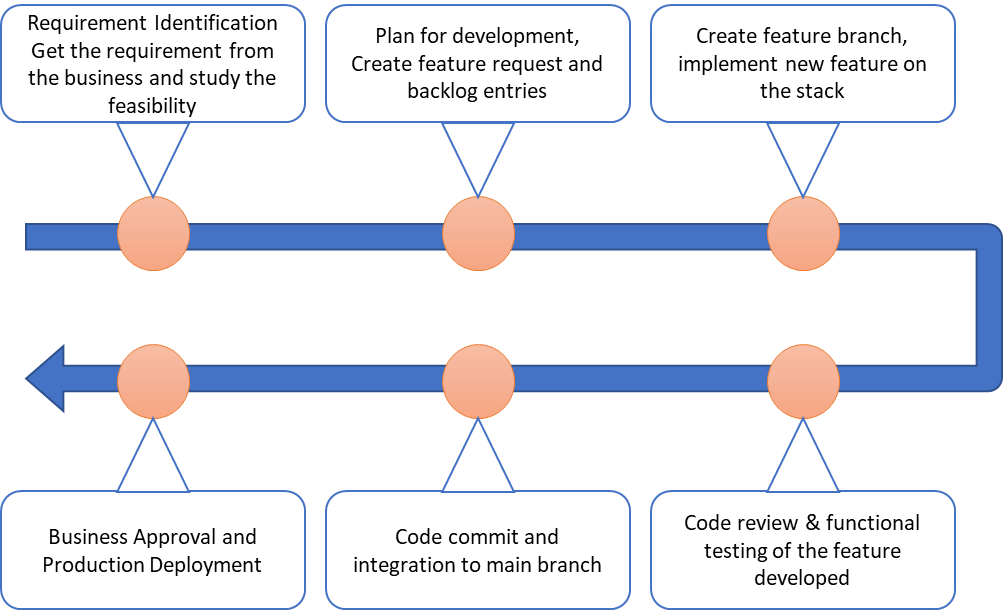


***Table: Solution Components***

* 1. Schedule & Planning

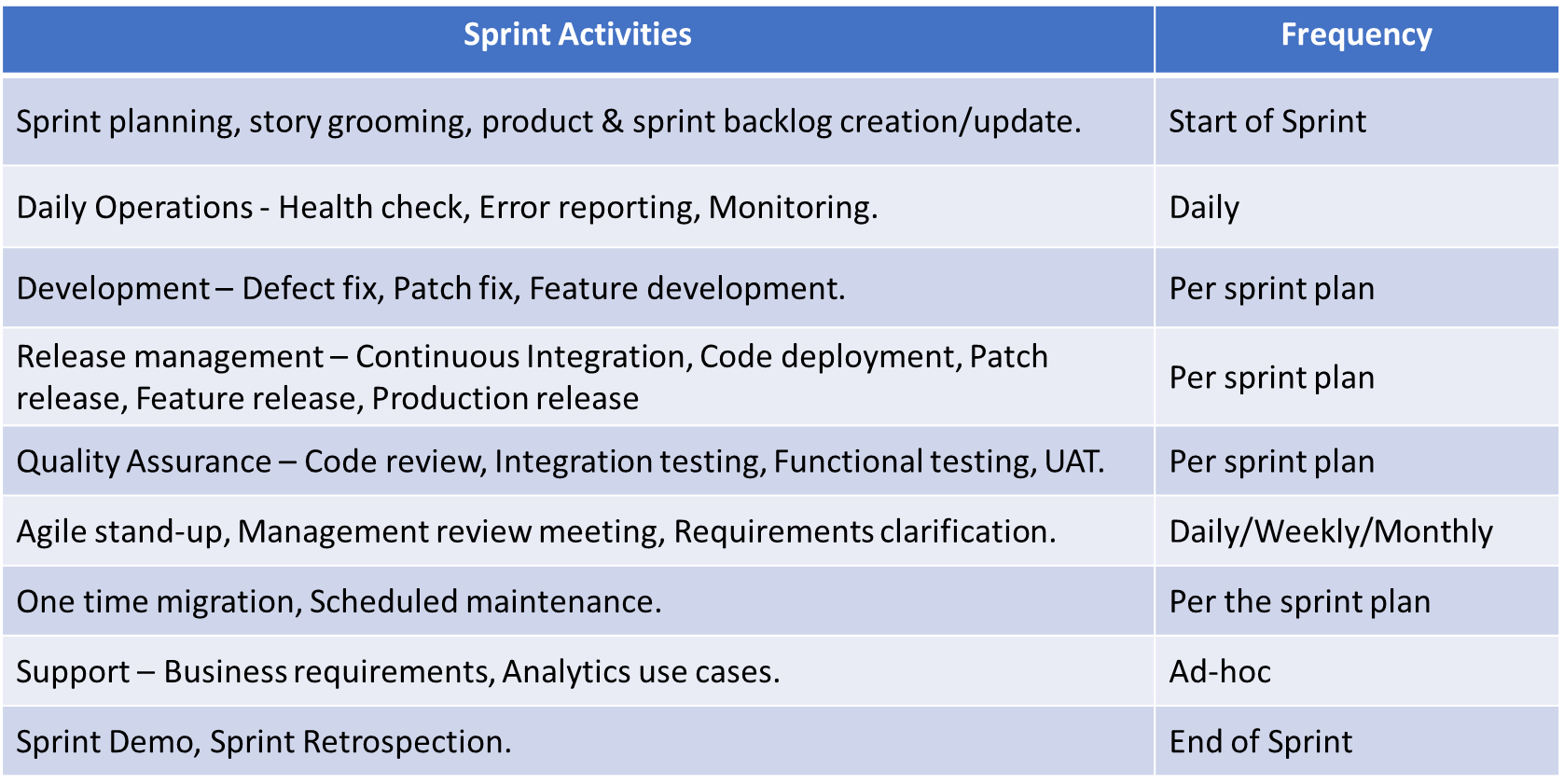
LatentView proposes to run this project in defined sprints with regular reviews and progress tracking. Jira shall be used for recording, tracking & monitoring of defects and sprint activities.

* + 1. Development plan

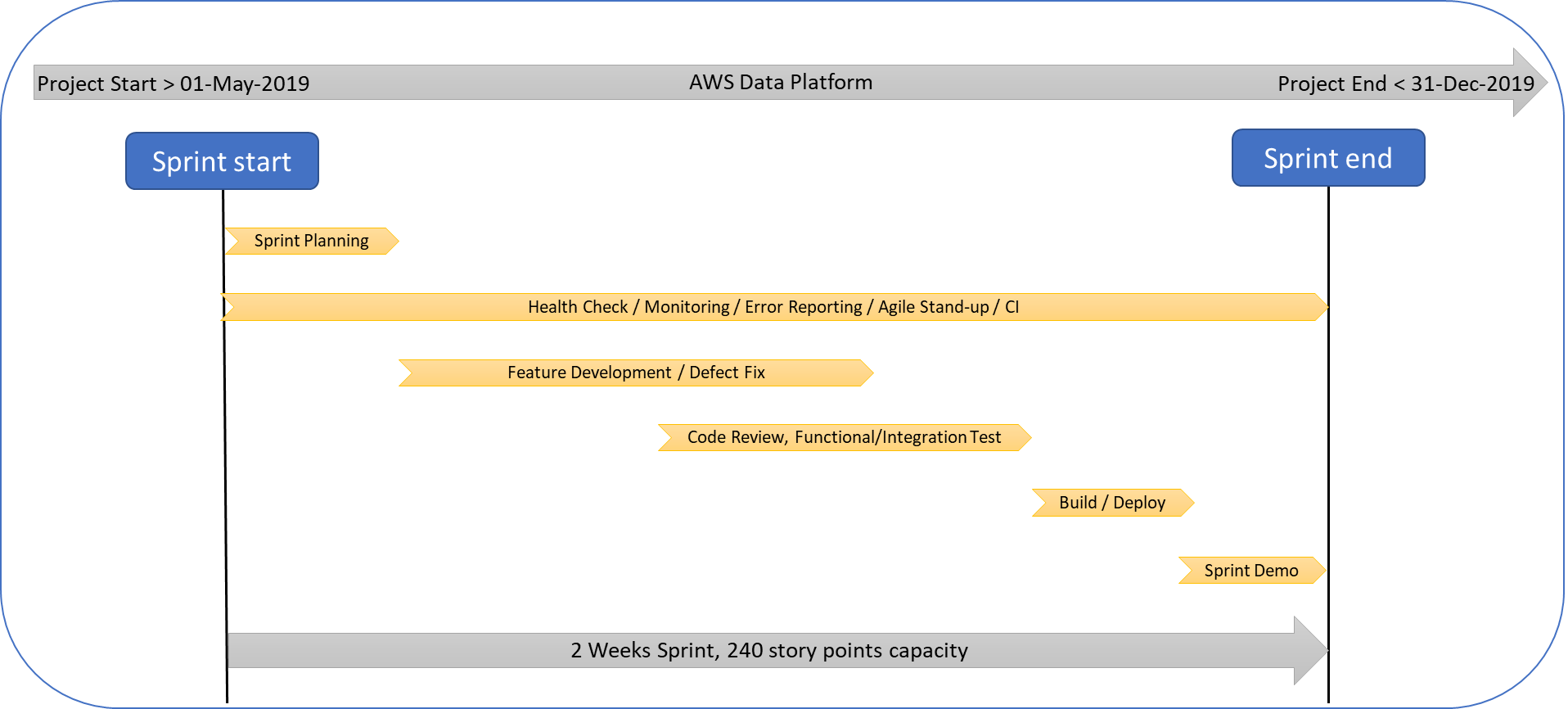


Suggested Development plan

* 1. Sprint activities



* 1. Sprint schedule



# LatentView Solution Approach to implement Dev-Ops

* 1. DevOps Activities
* **Data ingestion** with continuous pipeline, including movement and compression for periodical data update from Raw Data Hub to S3 bucket.
* **Compute readiness** of data for easy analytics including cataloguing & storage
* **Business enablement** achieved by consumable data through the following options, depending on the business requirement:

**EMR:** handles a broad set of big data use cases securely and reliably, including log analysis, web indexing, data transformations (ETL), machine learning. Ideal for Data Scientist to build machine learning models with large datasets

**Athena:** An interactive query service which automatically executes queries in parallel. Ideal for Data sampling and Dashboarding where users including Data Analysts can run queries and build their own dashboards

**Redshift Spectrum:** Built-in feature of AWS Redshift, which is primarily a warehouse service with SQL interface. Spectrum

* **Extension of sources** by additional data source migration ‘as-is’ from the on-premise Raw Data Hub to an AWS S3 buckets, located in the AWS datacenters in Frankfurt (EU). Data volume or size will determine the process of migration via Snowball or Direct Connect.
* **Platform Improvement** including performance, availability, usability and value of the platform.
* **Monitoring, Benchmarking and Documentation** for easy tracking, maintenance of the platform.

**Code management & deployment:**

* Tool: GitLab, AWS CodeCommit, Jenkins
* Process:
  + Master branch for holding the latest official released code.
  + Dedicated branch for each sprint (initially) and developers can directly develop on this branch.
  + Pull request from dedicated branch to master branch post code review process and test results.
  + Staging environment shall be maintained for development, testing while separate production environment shall be available for approved releases.
  + Deploy from master to dedicated S3 code paths as part of production deployment.
* Approach: Manual deployment process is initially recommended until the need for automation. Jenkins may be the choice for continuous integration. Additional DevOps tools shall be used as needed.
  1. DevOps Workflow

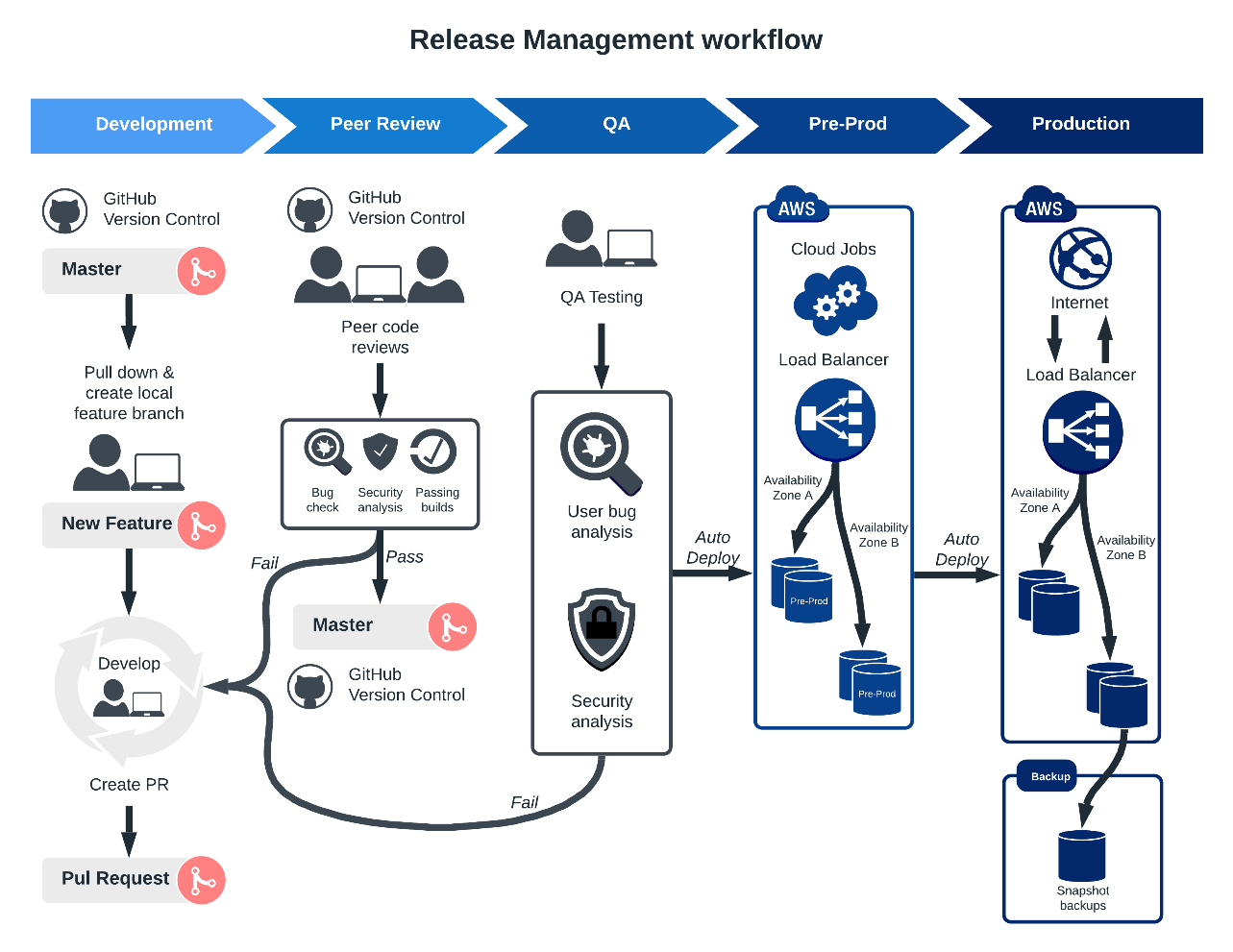


Figure: Dev-Ops workflow

* 1. LatentView’s suggested Best practices for Dev-Ops

Version control

* Versions should be maintained in a central repository
* Developers + Operations should have access to the same code
* During fault, ops can quickly rollback the deployed code and thus revert to the previous stable state.

PMML

* PMML should be the de facto standard to represent predictive solutions
* It should allows for different statistical and data mining tools to speak the same language
* It should have the flexibility to develop in one application and directly deployed on another

Integration, testing and deployment

* Capitalize different types of environment: Staging (development,testing), Production
* Canary Deployment using Load Balancing
* Deploy models in Containers – Docker
* Monitor – Retrain the model during concept drift using recent data

Security

* DevSecOps refers to the discipline and practice of safeguarding the entire DevOps environment through strategies, policies, processes, and technology
* Security should be built into every part of the DevOps lifecycle, including inception, design, build, test, release, support, maintenance, and beyond

# Pricing and Payment terms

* 1. PRICING:

**€ 34960.00/Month** (excluding of VAT, taxes & any infrastructure cost) shall be charged for the duration of the DevOps project. Emergency support services shall be charged over and above the monthly price. Please refer to attached Price matrix sheet for the detailed pricing information.

* 1. Payment Terms
     1. Additional cost payable to AWS (Not included part of LatentView service cost)

ProSieben should expect additional cost for the following items

* AWS infrastructure cost including Snowball migration & data lake components
* Software licenses that shall be deployed on the AWS cloud including Cloudera.
* Network cost incurred in the exchange of data between/across the on-prem systems & AWS data lake components.

LatentView will get preapproval for any other additional cost/expense before raising invoice for the same.

* + 1. Payment Schedule:

Invoices will be submitted for payment at the end of the month as per the work done.

LatentView shall be paid for work performed based on the rate schedule provided (submitted separately) plus expenses which have been pre-approved in writing by ProSieben.

# Operations

* 1. Proposed team structure

|  |  |  |
| --- | --- | --- |
| Role | Location | Number of resources |
| Principal AWS Consultant | Onsite | 1 |
| Offshore Manager | Offshore | 0.5 |
| Technical lead | Offshore | 1 |
| Analyst | Offshore | 2 |

* 1. Roles and Responsibilities

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Tasks and Responsibilities split between LatentView and ProSieben** | **Responsible Party** | | |
|  | **Responsibility of Deliverables** | LatentView Onsite | LatentView Offshore | ProSieben |
|  | **Service Package 1 - Coordination, OPS Manager (Agile Operation):** |  | | |
| 1 | Coordination effort for Operations Manager or Scrum Master | Y |  |  |
| 2 | Incident and problem management | Y |  |  |
| 3 | Team coordination | Y |  |  |
| 4 | Planning of micro-projects (minor update, releases.) | Y | Y |  |
| 5 | The classification of the position is at least at the advanced level | Y |  |  |
| 6 | Control of service providers and suppliers (e.g., Amazon) |  |  | Y |
| 7 | Direct contact for and regular exchange with the owner | Y |  |  |
| 8 | Create reports and corresponding dashboards (metrics, KPIs) in i.e. Jira/Confluence | Y | Y |  |
|  | **Service Package 2 - (Cloud) Infrastructure Services:** |  | | |
| 9 | Manage all basic components required for the operation of cloud-based services. |  | Y |  |
| 10 | As infrastructure services improve, they can also be retired and replaced with new tools as needed. The implementation of new infrastructure components is planned during operation and then implemented autonomously. If this is causing any impact on the running platform, a maintenance window is agreed with the owner. |  | Y | Y |
| 11 | The decision to use an infrastructure tool is the responsibility of the operations team itself. |  |  | Y |
|  | **Service Package 3 - Operating Systems and Platform Services** |  | | |
| 12 | Install, parameterize & manage cloud operating systems, components. And services on virtual HW (Amazon AWS services) |  | Y |  |
| 13 | Monitoring of systems, components and services for any defects |  | Y |  |
| 14 | Suitable and applicable for cloud architectures and services |  | Y |  |
| 15 | Supplier to handle minor and security updates |  | Y |  |
| 16 | Major upgrades must be planned and commissioned through a dedicated migration project | y |  | Y |
|  | **Other responsibilities** |  | | |
| 17 | Offshore & onsite developers shall have the necessary access to onboard them to the ProSieben system including data and documentation (Confluence, Jira, VPN, HDFS, AWS etc.) | Y |  | Y |
| 18 | One-time migration of identified the data & making it available in S3 using AWS Snowball. |  |  | Y |
| 19 | Data lake on Amazon AWS Project progress – maintain project plan, provide progress update, organize update meetings with the appropriate stakeholders | y | Y |  |
| 20 | Review the deliverables and provide feedback. |  |  | Y |
| 21 | Escalate any slippages and do root cause analysis of the slippage reasons. Manage team utilization and productivity. Maintain the development environment and resolve any issues that impact team utilization. Manage smooth transitions in case of changes in the team | Y |  |  |
| 22 | Availability of stake holders for planning and communication. | y | Y | Y |

* 1. Time Zone Management

Working with clients across Europe, UK, US & APAC, LatentView has developed mechanisms to enable effective and prompt co-ordination and collaboration across teams. LatentView’s flexible work hours policy also ensures that we can coordinate with our clients at optimal times across geographies.

With a very significant time overlap in working hours at ProSieben’s office locations and our delivery centre in Chennai, collaborative working will be effective. Our onsite person will serve as a SPOC for the ProSieben team and coordinate with the offshore resources.

Standard working hours for the team (onsite and offshore) will be **9:00 hrs to 18:00 hrs**, Monday through Friday.

* 1. Service level agreements
* LatentView shall support the initial data migration for the data sources migrated using Snowball
* LatentView shall maintain the same data model/schema on AWS S3 same as the RawDataHub sources
* LatentView shall perform data validation on an aggregated sample of the migrated data using Snowball. The sample size to be validated will be discussed & approved with ProSieben
* Automated data pipeline shall be designed & deployed on AWS for continuous ingestion for the identified data sources in the scope.
* ProSieben and LatentView shall design a quality dashboard to track data ingestion and input data quality on to S3. Data ingestion metrics depend on the following integration related activities.
* Logging of file upload process to S3 with the following details

*Name of file, File Format, Source ETL, destination bucket, destination s3 key, timestamp, time to upload, manifest file associated with the upload, file size, is\_multipart\_upload, is\_compressed, is\_columnar, tags, is\_dimension, is\_fact, business\_group, rows, columns, encoding, status*

* File upload SLA (upload time, upload schedule, upload dependencies) for different data sources
* Data integrity check for uploaded files (especially files > 100MB)
* Conforming to agreed standards with respect to file delimiter, file format, treatment of empty values, nulls.
* Consistent encoding for datasets and appropriate communication in case of any changes. The encoding information must be captured as part of metadata.
* Based on schedule & requirements, track the number of uploads & failures per key prefix
* Turnaround time for Snowball Import/Export.
  + 1. Turnaround time for issues

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Severity | Standard hours | | Emergency hours | |
| First response | Resolution target | First response | Resolution target |
| Critical | 2 hours | 6 hours | 3 hours | 8 hours |
| Urgent | 4 hours | 12 hours | 6 hours | 24 hours |
| Important | 8 hours | 24 hours | Next business day | 48 hours |
| Routine |  | Next scheduled release |  | Next scheduled release |

Critical: All errors which result in the loss of the entire service or prevents effective use of the service by a majority of all the users or more. Such an error has a major adverse impact on the business critical operations as well as users and is characterized as:

* Impacts majority of all the users or more
* Impacts the ability of majority of all users or more to continue using the system
* Supported application system is inoperable or unworkable
* Automated processes developed by RSG are inoperable or unworkable
* Error in API or Interface that may cause incorrect data processing
* Major functionality is disabled
* Causing financial loss or damages reputation of the business

Urgent: All errors which prevent a user using the service effectively. Such an error has significant impact on the business operations as well as end users and is characterized as:

* Impacts one user to minority of all users
* Impacts the ability of a user or a minority of all users to continue using the system
* Impact is that part of the functionality is being disabled
* Supported application system is, in part, inoperable or unworkable
* Impact where a workaround is unavailable or doesn’t meet business need completely

Important: All errors not categorized as Critical or Urgent. Such an error has a minor impact on the business operations as well as end users and is characterized as:

* Suggestions for enhancing applications
* Errors which are inconvenient but do not impact the usage of the application
* Supported application system is fully available and operable to most of the users
* Impact where a workaround is available but not acceptable in long-term
* User queries not linked to any change
  1. Assumptions and prerequisites

The following Project Assumptions are agreed upon by the parties as factors in determining the Scope, Objectives and assigned responsibilities.

|  |  |
| --- | --- |
| Project Assumptions | |
| 1 | ProSieben may disclose or permit access to ProSieben information or data hereunder. ProSieben data will be considered ProSieben Confidential Information. For ProSieben data refers to data in electronic form collected for or through the Services from ProSieben or ProSieben’s databases or customers or other third parties or directly from ProSieben. ProSieben data will be and remain the property of ProSieben. Supplier may not use ProSieben data for any purpose other than as required to render the Services. No ProSieben data will be sold, disclosed, assigned, leased or otherwise disposed of to third parties or commercially exploited by or on behalf of Supplier (or its subcontractors). Neither Supplier nor any of its subcontractors may possess or assert any lien or other right against or to ProSieben data. Without limiting the generality of the foregoing, Supplier may only use personal information as strictly necessary to render the Services and must restrict access to such information to Supplier personnel on a strict need-to-know basis. At the conclusion or termination of the Agreement or this Statement of Work Supplier shall return all ProSieben data to ProSieben in a useful, electronic format acceptable to ProSieben and thereafter erase the ProSieben data. “Erase” shall mean the destruction of ProSieben data, wherever located, so that no copy of the ProSieben data remains or can be accessed or restored in any way. |
| 2 | LatentView warrants it will not install any unlicensed software in any ProSieben environment or provide software Deliverables subject to any obligation or condition (including without limitation any “copyleft” or other obligation or condition under any “open source” license such as without limitation the GNU Public License, Lesser GNU Public License or Mozilla Public License) and will indemnify ProSieben from any breach of this warranty. |
| 3 | Each Deliverable that consists of software will be delivered in binary form together with source code, programming documentation enough to permit replication of the binary Deliverable, and any relevant Perficient proprietary programming tools. |
| 4 | ProSieben has necessary approvals and/or acceptances from relevant stakeholders (both internal and external) to use AWS Cloud Stack and host existing and upcoming data.  Scoping will be done at sprint planning meeting, during which size of the database will be determined. |
| 5 | Infrastructure cost might vary based on the project requirement and computational power required |
| 6 | ProSieben shall provide access to the ProSieben infrastructure including data & documentation for offshore & onsite developers by the end of week 1 from the official project kick off. |
| 7 | Private connectivity to the data tables in RDH will be provided to the LatentView team to start the project |

* 1. Progress Meetings

ProSieben and LatentView shall support and provide representation at progress review meetings that shall be planned and scheduled as needed.

* 1. Escalation Mechanism

LatentView has a well-defined organizational structure comprising of a steering committee and account management to take care of any issues. Communication with the customer involves the following:

* Communication is through email or any mode as agreed to with the customer. All emails sent and received from the customer are tracked to ensure proper responses are sent to the customer
* The weekly status report is used for recording the status of project activities with respect to the project plan
* Both internal and external escalation details are documented as part of the project plan and followed

The below table details the Escalation process and personnel involved to manage the escalation:

|  |  |
| --- | --- |
| Escalation Procedure | |
| **First Level** | **LatentView Project Manager** |
| * Provide a single point of contact for day-to-day operational issues * Establish communication protocols with client for issue resolution and reporting needs via e-mail, issue log, encounter reports. | |
| **Second Level** | **LatentView Delivery Head** |
| * Provide support to the project team throughout all project phases * Resolve escalated issues or commit other resources for issue resolution | |
| **Third Level** | **Joint Senior Management of ProSieben and LatentView** |
| * In the event of an issue being escalated to this level, the same is resolved in mutual interest and in line with our strategy of ‘Partnership’ with the clients. | |

***Table: Escalation Matrix***

# Risk Management

* 1. Identified major risks

While LatentView makes every effort to accurately replicate the HDFS system into cloud, an exact system interoperability cannot be guaranteed. Following lists major risks associated with this exercise:

**Onboarding & Access**

It is expected that the offshore & onsite developers shall have the necessary access to onboard them to the ProSieben system by the end of Week 1 from the official project kick off. 

**Snowball Migration**

ProSieben shall be responsible for the one-time migration of data from Raw data hub to AWS S3 using snowball. Any delay in this process of snowball migration shall affect the schedule of the tasks identified in Sprint 2,3,4 and will need a review of scope and timeline accordingly

**Resolving key infrastructure and application dependencies**

Infrastructure and application dependencies and associated codes in existing on premise HDFS data may not be replicated accurately due to difference in architecture between cloud and on-premise. This may result in either higher or lower performances depending on use cases

**Data Loss**

Data loss for the copy of data maintained only in the cloud due to disasters need to be managed separately. While Amazon AWS provides various disaster recovery options, complete protection of data cannot be ascertained

**Data breaches**

Particularly in multi-tenant cloud service databases, a flaw in one client’s application could give an attacker entrance to other clients’ data as well. AWS Cognito authentication services help mitigate this risk

**Network Limitation**

Moving from on premise to Cloud involves dependency on internet as opposed to internal network. Limitations on internet connectivity may limit the performance and availability of hosted applications and solutions

**System integration**

Legacy systems which may no longer be supported or have limited support by cloud architecture may not be adequately integrated with Cloud systems. The code & migration logic developed for the cloud might not be compatible with the on-premise systems.

**IT Governance**

ProSieben would lose governance and control of IT systems in cloud and may find limitations in carrying out certain tasks like auditing and regulation compliance

* 1. Business Continuity and Disaster Recovery
* LatentView has robust Business Continuity and Disaster Recovery processes to ensure continuous undisrupted analytics and data operations for its clients.
* Chennai global delivery center is the operations hub for LatentView and has world class infrastructure. LatentView’s Business Continuity Management Team (BCMT), responds in accordance with Business continuity plan and initiates specific actions for recovery in the event of a disaster.
* The primary team members of BCMT are Director IT, Delivery Manager and Director HR/Admin. Periodic back up of is carried out as a precautionary step in BCP.
* LatentView uses WINDOWS® backup application to store backed-up data in multiple server locations. The primary and secondary domain controllers for active directory are implemented to avoid single point of failure.
* LatentView also has satellite office relationships with other locations across South India (Coimbatore, Bangalore, and Kochi), where our staff could be relocated for a short duration and operations aren’t affected.
* **Highlight to the Business Continuity** was the recent floods at Chennai where multiple IT firms, BPO firms and even several client’s Indian offices experienced loss in operations and delivery. However, our client’s senior leadership commented that our business continuity processes ensure that we communicated well in advance, ensured that there was only minimal loss of productivity and that we were able to respond much better to the calamity than other teams they were associated with.
  1. Quality Assurance

LatentView uses the **DARTS** **framework** for this quality assurance. The model covers five essential criteria namely:

* **Documentation:** LatentView follows an agreed upon documentation process that helps us to follow up with the status of projects every week, to track down the number of incidents raised and enhancements identified with appropriate naming conventions. Internal audit team audits these documents monthly and measures the overall performance metrics of the projects
* **Accuracy**: LatentView documents all accuracy/error related incidents raised by different stakeholders and use the same to measure accuracy for each project
* **Responsiveness**: This is measured based on LatentView’s response to any client request within an agreed upon time mutually decided by the client and LatentView
* **Timeliness**: This is measured against the actual completion date as mentioned on SOW
* **Satisfaction**: LatentView use Quarterly survey to track the level of customer satisfaction on a scale of 1 to 10, with 1 being “Completely Dissatisfied” and 10 being “Completely Satisfied”. Combining the scores of all parameters of this satisfaction survey, a consolidated score for customer satisfaction is calculated.

Above mentioned criteria are analysed in two ways. First, LatentView conducts internal audits and second, LatentView takes surveys from clients as well. Based on these two aspects, the dimensions are specifically analysed and compared with the benchmarks defined for each criteria. Then individual scores are calculated for these criteria which help us to identify the areas of further improvement.

|  |  |  |
| --- | --- | --- |
| **Dimension** | **How is it Measured?** | **Benchmark Score  (on a scale of 10)** |
| Documentation | 1. Documents refreshed weekly 2. Audited monthly | 9 |
| Accuracy | 1. Accuracy related incidents/emails from stakeholders 2. Monthly Internal Audit + Client survey | 9.5 |
| Responsiveness | 1. Responses to client requests tracked 2. Monthly Internal Audit + Client survey | 9 |
| Timeliness | 1. Measured against actual completion date in SOW 2. Monthly Internal Audit + Client survey | 9 |
| Satisfaction | 1. Monthly Internal Audit + Client survey | 8.75 |

* 1. Data Security & GDPR

Information is an extremely valuable and important corporate asset that requires protection against risks that would threaten its confidentiality, integrity and/or availability. LatentView is engaged in delivering business critical insights by analysing customer data. In such a business, information security is an essential prerequisite for customer confidence. Suitable information security controls must therefore be selected and implemented. The security controls identified in LatentView’s policy are based on ISO standards 27001.

LatentView has a stringent data security policy to ensure clients confidentiality, the key elements of which are as follows:

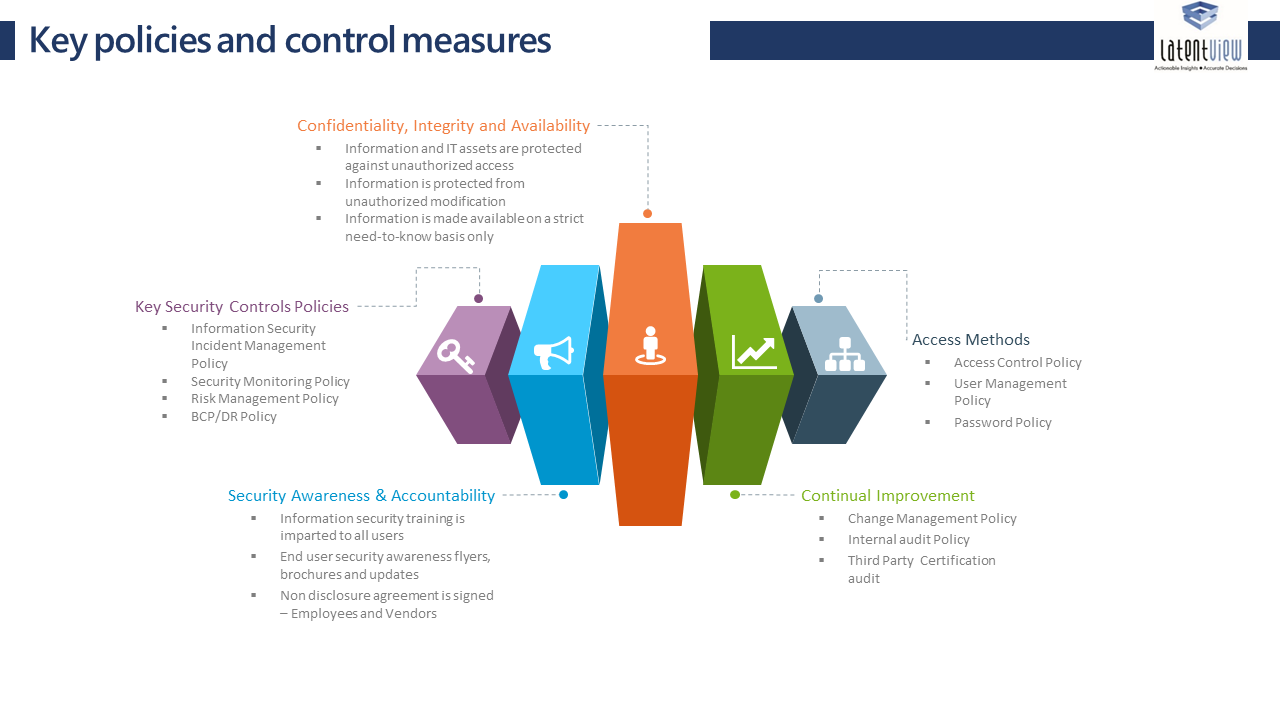


Figure: Key elements of data security policy

**The above features of data security are enabled by LatentView using the following infrastructure and processes**

**Infrastructure and Data Security:**

LatentView has a secure data center and powerful computing servers for our analytics practices. LatentView has taken extensive measures in maintaining the security standards and is certified as ISO 27001 and PCI (Payment Card Industry Standard) complaint organization.

**Centralized Cloud Infrastructure:**

LatentView uses the Amazon cloud system for computing intensive processes that require faster results.

**Physical Security Standards:**

Physical security of the site is ensured by 7x24x365 guards. Biometric finger print is used to have secure authorized entry to our premises. Cameras are placed throughout the perimeter with guards and recorded video is maintained for 30-day periods on all cameras. All access is logged and tracked. Smoke detectors are used, as is laser air sampling. Conventional smoke and heat sensors are cross-zoned throughout the ceiling and below the raised flooring.

**Data Security and Backup**: Storage Area Network (SAN) is used to store our data. Daily, incremental and complete backups are taken in disk-to-disk backup processes executed to external disks. Backup devices are stored in a secure environment and are available for immediate restore.

#### Data Security Policy - Detailed

LatentView’s policy guidelines are designed to preserve the confidentiality, integrity, availability, and value of all information assets, as well as to ensure the continued delivery of business services. They also establish the appropriate focus and standards for acceptable information security practices across the organization. This policy is based on applicable regulations and highlights Customer goals and requirements for protecting its information assets.

LatentView aims to promote and build an environment where all employees are aware of their individual information security responsibilities and are actively engaged and committed to improving standards of information security.

LatentView shall implement appropriate security controls to ensure that:

i) Information assets are identified and categorised in terms of business value.

ii) Ownership of information assets is established, responsibilities defined.

iii) Information and IT assets are protected against unauthorized access.

iv) Information is made available on a strict need-to-know basis only.

v) Information is not disclosed to unauthorized persons through deliberate or careless action.

vi) Confidentiality of information is assured in accordance with client agreements and best practices.

vii) Information is protected from unauthorized modification.

viii) Applicable regulatory and legislative requirements are met.

ix) Disaster recovery plans for IT assets are developed, maintained and tested.

x) Information security training is imparted to all users of information assets.

xi) Information security breaches are reported, investigated, resolved, and closed.

xii) A culture of compliance towards information security is advocated and promoted.

xiii) Violations of policies are dealt with disciplinary action.

xiv) The responsibility for maintaining the policy and providing advice and guidance on its implementation rests with LatentView management.

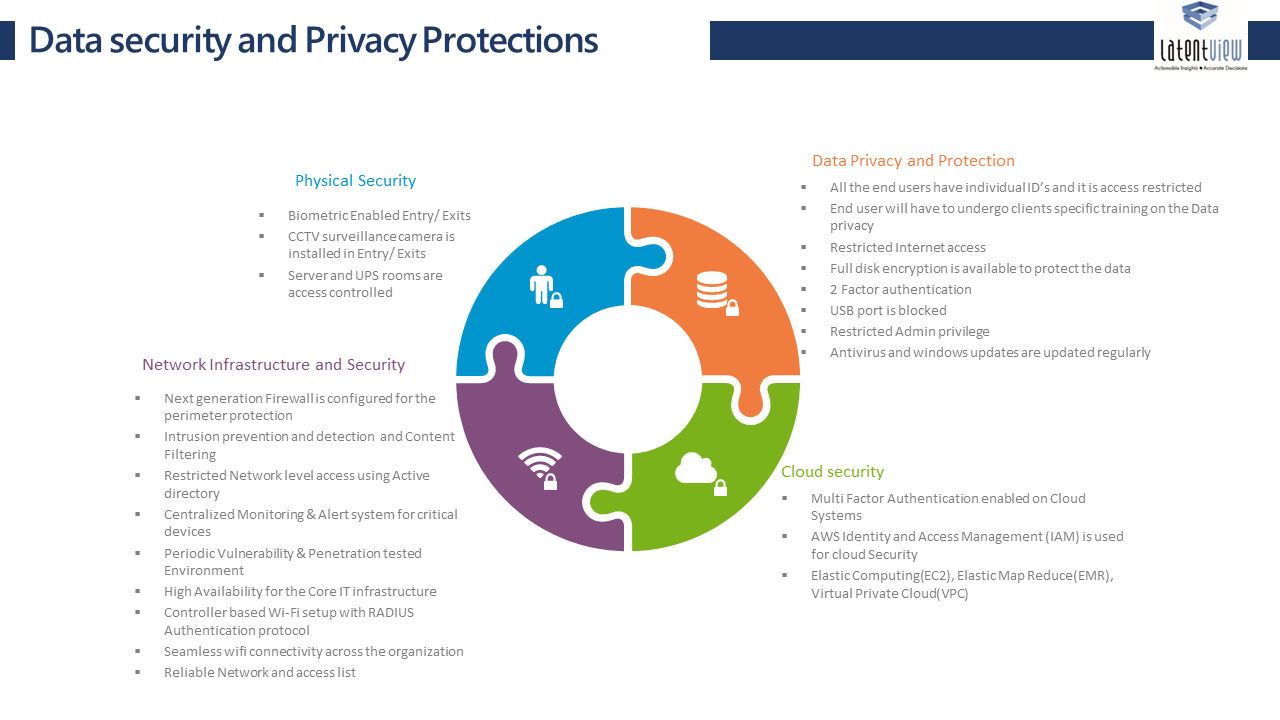


Figure: Data Security Policy Aspects

#### GDPR – Please refer to attached signed terms and conditions

#### Security Certifications

Below are the security certifications, LatentView have undergone through.



**Network Redundancy**: Networking to the analytics platform is ensured by having high speed Internet Leased Lines. Alternate carrier capabilities are also present. SonicWALL firewall secure SSL VPN is used to connect a fully meshed networking fabric to each LatentView site. Sys Logs are stored and reviewed for violations and/or suspicious activity. Port activity is carefully monitored and opened only on a needs basis. Network Security Appliances at the perimeter level enables us with many security features that are tamperproof.

**Security in Data Transfer / Access**: A dedicated FTP server in AWS is being used for file transfers and McAfee is used for encryption. All client data is maintained within the analytics infrastructure and off-shore teams log into the platform via secured VPN, authenticate to the domain and then sign into the specific server and project. Permissions are limited to the key project members and align with the functions they are performing. System logs are reviewed for access patterns, violations or suspicious activity.

**LatentView HIPAA Certification**



#### Security Training

LatentView employees are put through information security training upon their induction in to the company and at periodic instances after that. For employees working in specific client projects, they also undergo the security training and evaluation as prescribed by the client.

Employees and delivery managers working on Europe based client engagements are additionally put through GDPR training done by external agencies.

#### References

LatentView’s data security policy incorporates the following elements from global information standards

|  |
| --- |
| LV-ISMS-PO-02 Security Organization Policy |
| LV-ISMS-PO-03 Asset Management Policy |
| LV-ISMS-PO-04 Information Security Incident Management Policy |
| LV-ISMS-PO-05 Compliance Policy |
| LV-ISMS-PO-06 Acceptable Usage Policy |
| LV-ISMS-PO-07 Change Management Policy |
| LV-ISMS-PO-08 Communication Policy |
| LV-ISMS-PO-09 Clear Desk and Clear Screen Policy |
| LV-ISMS-PO-10 BCP-DR Policy |
| LV-ISMS-PO-11 Access Control Policy |
| LV-ISMS-PO-12 Password Policy |
| LV-ISMS-PO-13 Information systems Acquisition Development Policy |
| LV-ISMS-PO-14 Email Policy |
| LV-ISMS-PO-15 Malicious Code Policy |
| LV-ISMS-PO-16 Mobile Computing Devices Handling Policy |
| LV-ISMS-PO-17 Internet Policy |
| LV-ISMS-PO-18 Physical and Environmental Control Policy |
| LV-ISMS-PO-19 Data Protection and Privacy policy |
| LV-ISMS-PO-20 Backup Policy |
| LV-ISMS-PO-21 User Management Policy |
| LV-ISMS-PO-22 Measurement of Effectiveness of Control Policy |
| LV-ISMS-PO-23 Risk Management Policy |
| LV-ISMS-PO-24 Internal Audit Policy |
| LV-ISMS-PO-25 Network Policy |
| LV-ISMS-PO-26 Server Security Policy |
| LV-ISMS-PO-27 Patch Management Policy |
| LV-ISMS-PO-28 Security Monitoring Policy |
| LV-ISMS-PO-29 Cryptographic Policy |
| LV-ISMS-PO-30 Outsourcing and External Facilities Management Policy |
| LV-ISMS-PO-31 Purchasing Policy |
| LV-ISMS-PO-32 Human Resource Policy |
| LV-ISMS-PO-33 Policy For interested Parties |
| LV-ISMS-PO-34 SDLC Policy |
| LV-ISMS-PO-35 System Security Testing for Fulfilling Security Requirements of Application Policy |
| LV-ISMS-PO-36 Wi-Fi Policy |
| LV-ISMS-PO-37 Capacity Management policy |

#### Experience in Developing Systems with GDPR Compliance

One of our clients, a global financial payment gateway provider with operations in US, UK and APAC, we developed an analytics application on Hadoop platform. The client has very strict policies towards data security. Following are the set of best practices which helped us to achieve this:

* Access to client resources: Only client authorized team members can access the client data. No sharing of data without getting client approval. Off-shore teams log into the platform via secured VPN and then sign into the specific server and project. Permissions align with the functions performed by the team members.
* Security Certifications: LatentView has ISO 27001 and PCI-DSS(Payment Card Industry Standard) Certifications.
* Physical Security Standards: Physical security of the site is ensured by 7x24x365 guards with Biometric authentication and video monitored. All access is logged and tracked.
* Client Specific Security Measures: Any addition/deletion of a resource is intimated to the client immediately and all access to data is restricted immediately upon removal