6CS007– Project and Professionalism

Milestone 4 – Professionalism Report

University Id:	2330520
Group:	L6CG22
Supervisor:	Dipti Gyawali
Submitted by:	Shrota Ghimire
Submitted on:	19th May, 2025

Table of Contents

1. Professionalism Aspects of a Task Management System 1
   1.1 Social Impact 1
      1.1.1 Beneficial Aspects 1
      1.1.2 Detrimental Aspects 2
   1.2 Ethical Issues 2
      1.2.1 Case Study 1: User Privacy in Task Management 3
      1.2.2 Case Study 2: Bias in Task Allocation 4
      1.2.2 Possible Ethical Issues in TMS 6
   1.3 Legal Implications 6
      1.3.1 Case Study 1: GDPR Compliance in User Tracking 6
      1.3.2 Intellectual Property Rights 7
   1.4 Security Aspects 8
      1.4.1 Case Study 1: Data Breach in Task Management 8
      1.4.2 Security Features in TMS 8
2. Conclusion 10

1. Professionalism Aspects of a Task Management System

The assessment of software development professionalism includes both mandatory social obligations and legal standards and ethical rules and security needs to direct computer science software development methods. The development process of Task Management Systems requires developers to conduct assessments of these professional factors in order to create systems that benefit workplace activities while upholding integrity standards. The deployed considerations enable TMS platforms to follow best practices through features for security maintenance and ethical procedures and transparent operation.

Workplace task management systems function as essential tools that support modern teams to coordinate their projects while task assignment and progress tracking occur efficiently. Strategic development of digital platforms and their ethical deployment must become essential as reliance on such systems grows. Multiple critical factors need assessment to start with social effects and ethical challenges while also handling legal elements and security protocols. The professional caliber of a TMS results from these factors which allow organizations to use their systems without hurting their workforce or compromising their private data.

1.1 Social Impact

The social aspects of a task management system generate changes in users and companies while affecting overall organizational output and operational efficiency. Task management systems help enhance productivity during work while enabling better collaboration and remote task tracking which introduces user-specific difficulties. Businesses need to verify that efficiency systems do not deteriorate work-life equilibrium or diminish employee satisfaction levels.

1.1.1 Beneficial Aspects

An effective TMS enables teams to schedule tasks while setting crucial deadlines and track how work develops efficiently. Remote workers can connect better due to a centralized task delegation system present on this platform which monitors their work activities.

- **For Users:** Users possess the ability to join projects, accomplish assigned tasks, eliminate projects from their tasks and maintain real-time progress management. Users remain informed about task timing and accomplish their assigned responsibilities before deadlines.
- **For Admin:** Admin can build projects, develop tasks, assign work tasks to platform members and establish deadline times for tasks. However, they also possess the ability to delete tasks while managing projects and viewing platform administration status. The responsibilities of these team members include both distributed task assignments and ensuring that project deadlines remain on schedule for operational effectiveness.

1.1.2 Detrimental Aspects

A TMS has various advantages, yet it also brings some detrimental aspects.

- Using digital tools to excess causes users to lose their ability to manage tasks manually.
- The process of continuous tracking and monitoring leads users to experience stress which generates increased pressure that negatively affects their job satisfaction.
- User and project data will become accessible to unauthorized people when managers improperly handle the system.

To achieve the advantages of task management systems, organizations must implement suitable preventive measures that reduce these negative aspects.

1.2 Ethical Issues

A TMS system raises ethical problems by managing user information together with project information and performance tracking. The ethical framework depends on both transparent systems along with fair data management rules.

1.2.1 Case Study 1: User Privacy in Task Management

Business organizations use task tracking software as their main tool to monitor their operational performance indicators. In 2021 users found out that a leading company monitored their activities without their specific consent. The privacy breach of users became a major ethical issue because of this situation.

The following preventive measures must be added to the Task Management System to battle such ethical problems:

- The system shows users every trackable procedure with absolute clarity, so they understand all data usage processes.
- The system demands users to authorize tracking functions through explicit notices before it activates the monitoring capabilities. The practice establishes transparency which safeguards users from unauthorized surveillance activities.
- System encryption methods together with user access controls enforce full restrictions against unauthorized access to personal information. The system accesses user data solely for approved operational requirements but not for any performance evaluation assessments.
- Personal information management by task monitoring systems will ensure complete security while actively blocking their use in discriminatory performance evaluations.
- The monitoring system operates under all current privacy regulations by maintaining strict compliance. (Drapkin, 2021)

The My Task Management System implements solutions for these problems by following three approaches:

- Before tracking begins the system asks users to confirm with detailed information explaining the collected data and its purpose. All tracking functions need users to confirm permission through an explicit agreement before the system can initiate data tracking operations.
- User data maintained both during storage and transfer receives full encryption through Endto-End Encryption which stops unauthorized access.
- The system applies Role-Based Access Control (RBAC) which restricts sensitive data access through evaluation of user roles so authorized staff members receive access to certain types of information.

- A privacy dashboard exists for users to check what data is gathered while they can control permissions and demand deletion of their data when needed.

A set of security and privacy features built into my Task Management System allows ethical monitoring practices together with data protection for users and strict adherence to regulatory standards.

1.2.2 Case Study 2: Bias in Task Allocation

An artificial intelligent Task Management System at the organization selected users with monotonous low-priority work based on historical data assignment patterns which led to unequal workloads among users.

The resolution for preventing biased allocation in TMS needs developers to execute these specific actions during system development.

- The system processing algorithms need full transparency and must perform tasks without developing any form of bias throughout their operation.
- The framework blocks static historical distribution methods to determine task assignments. The system performs dynamic work distribution using factors that include important deadline criteria together with employee skills and present work volumes.
- The system enables users and administrators to conduct manual task reassignment which maintains fair work distribution while stopping AI-based biases from developing.
- Workers possess the autonomy to move tasks between colleagues to ensure balanced work assignments in the team. (Team, n.d.)

The Task Management System employs several strategies through which it handles bias issues during task distribution tasks.

- Task distribution through this system applies multiple factors to assignments through combination of workload equilibrium and deadline requirements with staff competency profiles rather than using single ancient allocation information.

- The system enables administrators and users to perform hand-driven reassignment of tasks to guarantee balanced allocation.

- The system performs continuous workload assessment to perform real-time adjustments which protect fairness levels.
- Users need to submit their task allocation reports to the system which then performs assessments for possible adjustments.

1.2.2 Possible Ethical Issues in TMS

- Unauthorized access to user work patterns combined with their performance data collection represents data exploitation.
- Performance ratings occur based on biased or incomplete evaluation data.
- Monitoring to excess creates user anxiety that becomes a new form of stress.

Ethical compliance in TMS requires a balance between performance tracking and user rights, ensuring fairness and security.

1.3 Legal Implications

A TMS system needs developers to protect data and respect intellectual property rights according to legal standards. The developers must obey existing regulations or risk facing legal consequences.

1.3.1 Case Study 1: GDPR Compliance in User Tracking

Due to its failure to gain valid consent for measuring productivity metrics the European company using a TMS system received a financial penalty under GDPR. A GDPR enforcement notice displayed the essential requirement for all organizations to honor data protection rules.

To achieve legal compliance with the implementation of TMS users must perform all essential steps.

- TMS software requires express authorization from users before it initiates tracking operations.

- Through the platform users must be able to erase accumulated data they possess. The interface allows users complete information control to examine and properly handle accumulated data before performing permanent removal anytime they want.

  The solution requirements need to fulfill all specifications dictated by GDPR together with the mandatory standards of each regional data privacy law. The system maintains ethical and lawful data management through encryption protocols along with anonymization methods and it implements role-based access controls (RBAC) to protect data processing. (MINDK, n.d.)

The combined application of privacy-first measures throughout the project safeguards user rights with tracking solutions that obey international data privacy directives.

The My Task Management System upholds GDPR standards and safeguards user information through these specified implementations:

- Users have full access to a detailed consent form that the system presents before tracking to meet GDPR standards.
- Users access the privacy dashboard where they handle their data management by viewing all their information and performing permanent data deletion at any desired time.
- The program defends user information through end-to-end encryption combined with anonymization procedures which protect data against unapproved access and misuse.
- Role-Based Access Control (RBAC) limits access to critical data through user roles which lets authorized staff see or change only their assigned data areas.

These security measures integrated into my system guarantee ethical tracking combined with protection of user privacy alongside strict compliance with GDPR along with other applicable international data protection laws.

1.3.2 Intellectual Property Rights

Users have the capability to submit project information that belongs to the company. Sensitivity data leakage occurs when inadequate access control implementation allows data exposure which begins the process of intellectual property disputes.

- The implementation of role-based access control (RBAC) represents a measure for developers to block unauthorized user access.

-
- The use of organizational data requires organizations to create precise rules defining IP policies.

1.4 Security Aspects

Secure design in a TMS remains fundamental since it protects data from unauthorized use and cyber incidents.

1.4.1 Case Study 1: Data Breach in Task Management

A widely used project task management application became the target of cyberattacks during 2022 due to weak authentication platforms which led to sensitive project information exposure. The incident proceeded to show why improved security measures should be implemented.

To reduce such potential risks TMS developers should enact these measures:

- Every user should authenticate their access through multiple authentication factors for secure login.
- Encrypt sensitive data using AES-256 encryption. Project data together with user credentials undergo AES-256 encryption to guarantee security for the information in case of a breach.
- Security teams should run periodic checks that help discover security weaknesses in the system. The system will feature automated security checks to detect vulnerabilities and enforce compliance with industry security standards. Regular penetration testing will also be conducted to strengthen system defenses.

1.4.2 Security Features in TMS

- SHA-256 hash functions should be used to protect user passwords.
- Project data protection relies on access-control measures that depend on user roles.
- Organizations should establish automated processes to back up their data because this practice prevents information loss.
- The system will automatically terminate user sessions when users remain inactive to increase security levels.

- Users should obtain complete data removal when demanding its deletion through secure procedures.

2. Conclusion

A tasks management system designed thoughtfully increases productivity and allows teams to work together better and checks the progress of work. A well-designed Task Management System demands ethical and legal and security solutions to remain responsible in its development practices. Accomplishing fairness along with upholding privacy regulations and meeting compliance requirements leads to sustaining trust in TMS platforms. Organizations need developers who focus on security protection of data and transparency and ethical practices to build dependable professional systems that fulfill user and organizational requirements.

3. References

Drapkin, A., 2021. Data Breaches.

MINDK, n.d. GDPR Compliance.

Team, H. A., n.d.