The **General Data Protection Regulation** (EU) 2016/679 (**GDPR**)

Audit Report

Table of Contents

Auditor:

Name: Balasubramanyam Gopatipalyam
Designation: Lead Implementer – InfoSec & Data Privacy
Company: Bellwether
E-mail: balu@bellwetherindia.com

1. Executive Summary

Introduction

As part of the GDPR readiness and audit program, approved by the leadership team of Uffizio India Software Consultants Pvt Ltd, we have undertaken an audit of Uffizio India Software Consultants Pvt Ltd's (The Organization) system of internal control and governance in relation to the mandates set forth by the General Data Protection Regulation (GDPR).

The audit was conducted in accordance with the guidelines set forth in GDPR and with our conclusions based on discussions with the Organization's Management and the information available at the time the assessment was performed.

The contents of this report have been agreed with the appropriate personnel at the Organization

Background

The EU legislation 2016/679 GDPR provides individuals with more power and control over their personal data by strengthening and unifying data protection for all EU individuals and more rights and control over how their personal data is handled by organizations such as the Organization. The main changes are:

Consent: The conditions for consent have been strengthened, and organizations must use consent requests which are clear and plain. It must also be made as easy to withdraw consent as it is to give it.

Breach Notification: Breach notification is mandatory where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach.

Right to Access: Data subjects have the right to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose.

Right to be forgotten: This entitles the data subject to have their personal data erased, cease further dissemination of the data, and potentially have third parties halt processing of the data. The exceptions to this right are if the personal data belonging to the data subject is related to the delivery of a statutory service or to prospective legal claims.

Data Portability: Data portability is the right for a data subject to receive the personal data concerning them, which they have previously provided, in a "commonly used and machine readable format" and have the right to transmit that data to another controller.

Privacy by Design: Privacy by design requires the inclusion of data protection from the onset of the design of systems or process, rather than as an addition. This means The Organization needs to consider data protection at the beginning and throughout the design process.

Penalties: Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements, e.g. not having sufficient customer consent to process data or violating the Privacy by Design concepts.

Assertion of the Organization's management

Uffizio India Software Consultants Pvt Ltd is an innovative product company with an aim to provide made-to-order IoT software solutions and services using GPS technology to empower businesses.

Trakzee is Uffizio's flagship product innovated as a fleet management solution. Trakzee simplifies real-time fleet tracking and monitoring while promoting fleet operations at efficient capacities. Trakzee lets a business regulate key metrics like fleet usage, fuel consumption, tire pressure, on-board diagnostics, driver behavior, and maintenance reminders.

As a product company aiming to provide services for organizations of all sizes, Uffizio India Software Consultants Pvt Ltd. thrives to streamline the processes the organization needs to follow to manage activities diligently.

Uffizio India Software Consultants Pvt Ltd. felt that client data deserved a greater level of protection than the one that is currently provided by GPS fleet management software industry. As a progressive organization, doing the right thing is at the heart of what we do. It is important for us to seek a rigorous independent review, from time to time, through a Data Privacy audit to attest that our systems, policies, and processes are robust to keep our clients data safe and to provide evidence that Uffizio India Software Consultants Pvt Ltd. is a trusted partner to protect confidentiality and Privacy of customers' data

The description is intended to provide users with information about the business application system that may be useful when assessing the data privacy risks arising from interactions with the Organization's systems, particularly information about system controls that Uffizio India Software Consultants Pvt Ltd. has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements of "Data Privacy" were achieved

We confirm, to the best of our knowledge and belief, that:

- the description presents Uffizio India Software Consultants Pvt Ltd.'s business application system that was designed and implemented as on 14th June 2021, in accordance with the description criteria.

- the controls stated in the description were suitably designed as on 14th June 2021, to provide reasonable assurance that the organization's service commitments and system requirements of Privacy would be achieved if its controls operated effectively throughout the following period.

{signed by}

Managing Director,

Uffizio India Software Consultants Pvt Ltd.

Date:

Scope

The scope of the audit was to ensure that appropriate governance and procedures are in place to ensure The Organization will comply with the requirements of GDPR.

Audit Opinion

We provide an overall audit opinion for all the audits we conduct. This is based on our judgment on the level of assurance which we can take over the established internal controls, governance and management of risk as evidenced by our audit work. Full details of the five possible categories of audit opinion are provided in Appendix 2 to this report.

Our overall audit opinion, for this audit, is that we can take a **substantial** level of assurance.

This means that internal control, governance and the management of risk are broadly sound. However, there are some areas of weakness which put some system objectives at minor risk and specific elements of residual risk that are slightly above an acceptable level and need to be addressed within a reasonable timescale.

Key Findings

We have highlighted one low priority item where we believe there is scope to strengthen the control and governance environment. This is summarized below:

- The notice of online privacy practices/Privacy policy has been drafted in line with the organization's data processing practices and shared with the team to be made visible on the website
- The cookie policy to explain the cookies used by the website is prepared and shared with the team to be made visible on the website
- A cookie consent opt-in mechanism needs to be set-up on the website, to comply with e-Privacy directive of the EU

Full details of the audit findings, recommendations and management responses can be found in Section 3 of this report and in the action plan at Appendix 1.

2. Objectives and Summary Assessment

Exhibit 1 sets out the control objectives identified during the planning phase of the audit and our assessment against each objective.

Exhibit 1 – Summary Assessment of Control Objectives

	Control Objective	Assessment	Summary Conclusion
1	There is appropriate governance in place to effectively manage the activity required to ensure GDPR compliance.	Substantial	There is clarity over responsibility for ensuring GDPR compliance with appropriate progress monitoring and reporting in place. The project was monitored by the management team which covered the main tasks required for compliance. Organization's staff have been informed of the key requirements.

2	Satisfactory progress is being made to ensure the Organization has appropriate procedures in place to ensure GDPR compliance.	Substantial	Appropriate procedures have been prepared and forwarded to the relevant personnel which cover all areas of GDPR in order to ensure compliance. A data protection policy has been adapted, a privacy notice covering all Organization's privacy policy has been prepared and available on the website. The cookie policy is also in place. Organization procedures for breach management, Subject access request are defined and published as a part of Privacy Information Management System/ PIMS of the Organization. Anonymization of data, as mandated by the regulation, is being performed.
3	The Organization has a GDPR risk register in place.	Substantial	The implementation of GDPR, and its associated risks is included in the Data Protection Impact Assessment. Heads of all functions are notified about performing frequent risk assessments.

Further details of our conclusions against each control objective can be found in Section 3 of this report.

3. Detailed Findings

There is appropriate governance in place to effectively manage the activity required to ensure GDPR compliance

The Governance and compliance function is responsible for managing the project to ensure the GDPR compliance. To deliver the project a Governance & Risk Management team (G&RM) has been created with resources from IT, Engineering and Executive Management functions

The G&RM heads the Organization's Information Security team with the members acting as lead officers who liaise with other resources to provide support and guidance to prepare for GDPR. The team comprises of stakeholders from the product/engineering team, IT and management teams. G&RM meets regularly to assess data protection regulatory landscape and it is clear that it gives appropriate attention to GDPR compliance.

This GDPR readiness assessment and audit program is based on a gap assessment that tracks compliance with each article of GDPR, which addresses the gaps and main tasks required to cover the gaps and ensure compliance with. Progress against the gaps is regularly reported to the Senior Management Team via regular status reports.

Key information on GDPR has been made available to all employees via the emails and a training course is planned to be available via the Organization's preferred training platform. The course has been classified as mandatory for all staff who deal with personal data..

GDPR requires the organization to document the personal data it holds, where it came from and who they share it with. The core product has an Information Asset Register (IAR), derived from Data flow diagram, that summarizes the data they hold across various IT platforms. Guidance was issued that outlined what additional information should be included in these IARs to address GDPR compliance and all IAR's are compliant.

The Organization is required to supply data subjects with information, such as the requirement to explain the lawful basis for processing their data, data retention periods and the right to complain to the supervisory authority if they are concerned about the manner in which the Organization is handling their data. The ICO recommend that this information is provided via a privacy notice. There is guidance outlining the various scenarios where The Organization can legally process an individual's data and also guidance for services to enable them to prepare the privacy notices.

GDPR sets out the various rights that individuals will have and they have been included in the privacy notices with fuller details on the website. These include the right:

- to be informed of data held
- of access to data
- to rectification of data
- to erasure of data
- to restrict processing
- to data portability
- to object to data held.

The Organization has established procedures to manage enquiries from individuals about the personal data The Organization may hold on them. Information is available to members of the public on their rights and the subject access request process on the website and guidance has been issued to staff on their role if they receive a subject access request, this is available in the PIMS.

The Organization has procedure enabling individuals to grant consent to process their data. The Organization has provided assurances that it will require individual consent for the delivery of its services. Areas where consent is currently held is considered as being compliant with the requirements of the new legislation.

In compliance with GDPR, The Organization has prepared a comprehensive data breach procedure document which defines the type of incident that would qualify as a data breach, who is responsible for reporting it, who it should be reported to and the reporting timescale.

The Organization is required to consider data protection and privacy in the early stages of any project and throughout its lifecycle. E.g. while developing new information technology systems, developing policy or strategies or, when embarking on a data sharing initiative. The project management team prepares guidance for "Privacy by Design and Data Protection Impact Assessment" for all such new projects before project initiation.

The organization is using strong encryption algorithms to encrypt (data at rest & motion) all personally identifiable information/PII

GDPR requires The Organization to have data sharing arrangements with services internal to The Organization and also external organizations. The organization has obtained sufficient assurances in the form of Data Processing Addendums with standard contractual clauses from all third parties who may potentially access data as a part of business operations.

DocuSigned by:
Balasubramanyam Gopati
7773330C1FB8455...

6/15/2021

Balasubramanyam G

Lead implementer – InfoSec & Data Privacy

Bellwether

Appendix 1 – Action Plan

	No.	Finding	Risk	Agreed Action	Responsibility / Due Date
	1	**Completion of GDPR Training** A GDPR training module needs to be designed and to be made available for relevant staff. The training needs to be classified as mandatory for all staff who deal with personal data. A completion deadline of 30th June 2021 has been set. As on the day of the audit, the executive and managerial staff have completed training.	Some of the staff are not appropriately aware of GDPR requirements and what is required of them to ensure Organization's compliance.	G&RM team will ensure IT department will send an e-mail that relevant staff should complete GDPR training module. Further, there will be refresher courses designed to ensure retention of the knowledge gained during the initial training program. Further, all the tests are duly graded and staff with sub-optimal grades are retrained and given the tests again for verifying performance.	Governance and Risk Manager/ IT team/ Infosec Team 30th June, 2021

In order to assist management in using our reports a system of grading audit findings has been adopted to allow the significance of findings to be ascertained. The definitions of each classification are as follows:

Grading	Definition
High	A major observation on high level controls and other important internal controls or a significant matter relating to the critical success of the objectives of the system. The weakness may therefore give rise to loss or error.
Medium	Observations on less significant internal controls and/or improvements to the efficiency and effectiveness of controls which will assist in meeting the objectives of the system. The weakness is not necessarily substantial however the risk of error would be significantly reduced if corrective action was taken.
Low	Minor recommendations to improve the efficiency and effectiveness of controls or an isolated issue subsequently corrected. The weakness does not appear to significantly affect the ability of the system to meet its objectives.

Appendix 2 – Audit Opinion

Level of Assurance	Definition
High	Internal control, governance and the management of risk are at a high standard. Only marginal elements of residual risk have been identified with these either being accepted or dealt with. A sound system of control designed to achieve the system objectives is in place and being applied consistently.
Substantial	Internal control, governance and the management of risk is sound. However, there are minor areas of weakness which put some system objectives at risk and specific elements of residual risk that are slightly above an acceptable level and need to be addressed within a reasonable timescale.
Reasonable	Internal control, governance and the management of risk are broadly reliable. However, whilst not displaying a general trend, there are a number of areas of concern which have been identified where elements of residual risk or weakness may put some of the system objectives at risk.
Limited	Internal control, governance and the management of risk are displaying a general trend of unacceptable residual risk above an acceptable level and placing system objectives are at risk. Weakness must be addressed with a reasonable timescale with management allocating appropriate resources to the issues raised.
No Assurance	Internal control, governance and the management of risk is poor. Significant residual risk and/or significant non-compliance with basic controls exists leaving the system open to error, loss or abuse. Residual risk must be addressed immediately with management allocating appropriate resources to the issues.