A: Pune, Maharashtra India-411047
W: fotoowl.ai

DATA BREACH MANAGEMENT MANUAL

1. POLICY STATEMENT

Foto Owl Software Solutions PVT. LTD. (hereinafter referred to as Foto Owl or Company), situated at Pune is committed to our obligations under the regulatory system and in accordance with the GDPR and maintain a robust and structured program for compliance adherence and monitoring. We carry out frequent riskassessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in a place where necessary. However,we recognize that breaches can occur, so this policy states our intent and objectives for dealing with such incidents.

Although we understand that not all risks can be mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from any risks associated with processing data. The protection and security of the personal data process is of paramount importance to us and we have developed data specificcontrols and protocols for any breaches relating to the GDPR and data protection laws.

2. PURPOSE

The purpose of this policy is to provide the Foto Owl's intent, objectives and procedures regardingdata breaches involving personal information. As we have obligations under the GDPR, we also have a requirement to ensure that the correct procedures, controls and measures are in place and disseminated to all employees, ensuring that they are aware of what the protocols and reporting lines are for personal information breaches. This policy details our processes for reporting, communicating and investigating incidents.

3. SCOPE

This policy applies to all persons within Foto Owl. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4. DATA SECURITY & BREACH REQUIREMENTS

The Company's definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

Alongside our 'Privacy by Design' approach to protecting data, we also have a legal, regulatory and business obligation to ensure that personal information is protected whilst being processed by the Company.

We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate tothe risks, including (but not limited to):

- Pseudonymisation and encryption of personal data
- Restricted access
- Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Disaster Recovery and Business Continuity Plan to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in theevent of a physical or technical incident

4.1 Objectives

- To adhere to the GDPR and EU Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any databreaches
- To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information
- To utilise information audits and risk assessments for mapping data and reducing the risk of breaches
- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information
- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes.

5. DATA BREACH PROCEDURES & GUIDELINES

Foto Owl AI has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Our procedures and guidelines for identifying,investigating and notification of breaches are detailed below. Our documented breach incident program aims to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

5.1 Breach Monitoring & Reporting

Breach Notifications can be sent to Akshay Gund at akshay@fotoowl.ai

6. BREACH NOTIFICATIONS

Foto Owl AI recognises the obligation and a duty to report data breaches in certain instances. All staff have been made aware of the Company's responsibilities and we have developed strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without delay.

6.1 Supervisory Authority Notification

The Supervisory Authority is to be notified of any breach where it is likely to result in a risk to therights and freedoms of individuals. These are situations in which if the breach was ignored, it wouldlead to significant detrimental effects on the individual.

Where applicable, the Supervisory Authority is notified of the breach no later than 72 hours after us becoming aware of it and is kept notified throughout any breach investigation, being providedwith a full report, including outcomes and mitigating actions as soon as possible, and always withinany specified timeframes.

If for any reason it is not possible to notify the Supervisory Authority of the breach within 72 hours,the notification will be made as soon as is feasible, accompanied by reasons for any delay. Wherea breach is assessed by the DPO and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons, we reserve the right not to inform the Supervisory Authority in accordance with Article 33 of the GDPR.

Breach incident procedures and an investigation are always carried out, regardless of our notification obligations and outcomes and reports are retained to be made available to the Supervisory Authority if requested.

Where the Company acts in the capacity of a processor, we will ensure that controller is notified of the breach without undue delay. In instances where we act in the capacity of a controller usingan external processor, we have a written agreement in place to state that the processor is obligatedto notify us without undue delay after becoming aware of a personal data breach.

6.2 Data Subject Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of naturalpersons, we will always communicate the personal data breach to the data subject without unduedelay, in a written, clear and legible format.

The notification to the Data Subject shall include:

- The nature of the personal data breach
- The name and contact details of our Data Protection Officer and/or any other relevant point ofcontact (for obtaining further information)
- A description of the likely consequences of the personal data breach

- A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational protection measures which render the data unintelligible to any person who is not authorised to access it (i.e., encryption, data maskingetc) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

7. RECORD KEEPING

All records and notes taken during the identification, assessment and investigation of the data breach are recorded and authorised and are retained for a periodof 5 years from the date of the incident. Incident forms are to be reviewed Semi Annually to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

8. RESPONSIBILITIES

The Company will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines.

9. VERSION HISTORY:

This policy has been revised last on 10th August, 2024 by Tushar Kolhe.

ANNEXURE 1 -
DATA BREACH INCIDENT FORM:

DPO/COMPLIANCE OFFICER/INVESTIGATOR DETAILS:			
NAME:		**POSITION:**	
DATE:		**TIME:**	
DDI:		**EMAIL:**	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DESCRIPTION & NATURE OF BREACH:			
TYPE OF BREACH:			
CATEGORIES OF DATA SUBJECTS AFFECTED:			
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NO. OF DATA SUBJECTS AFFECTED:		**NO. OF RECORDS INVOLVED:**	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
STAFF INVOLVED IN BREACH:			
PROCEDURES INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			