No. 001 Version 1

May 10, 2022

www.catchprobe.com

DATA PROTECTION ADDENDUM

info@catchprobe.com

+1 (628) 208-6430

1160 Battery Street,
East Suite 100, San Francisco, CA 94111, USA

CATCH PROBE™

CATCHPROBE DATA PROTECTION ADDENDUM

1. PURPOSE

This Privacy Notice for California Residents ("CA Privacy Notice") applies solely to Consumers (as defined below) who reside in the State of California. We adopt this CA Privacy Notice to comply with the California Consumer Privacy Act of 2018 ("CCPA") and any terms used in this CA Privacy Notice shall have the same meaning as defined in CCPA. Capitalized terms not defined but used herein have the meaning assigned to such terms in the CatchProbe Privacy Policy.

2. SCOPE

We may use or disclose the personal information we collect for one or more of the following purposes:

To fulfill or meet the reason you provided the information. For example, if you share your name and contact information to request support in connection with your subscription to the Solutions, We will use that personal information to respond to your inquiry.

To create, maintain, customize, and secure your account with Us.

To provide you and the company you work with the Solutions as requested by such company.

To provide you with support and to respond to your inquiries, including to investigate and address your concerns and monitor and improve Our responses.

To help maintain the safety, security, and integrity of our Site, Solutions and Our business.

For testing, research, analysis, and product development, including to develop and improve Our Site and Solutions.

To respond to law enforcement requests and as required by applicable law, court order, or governmental regulations.

As described to you when collecting your personal information or as otherwise set forth in the CCPA.

We will not collect additional categories of personal information or use the personal information We collected for materially different, unrelated, or incompatible purposes without providing you notice.

3. DEFINITIONS AND ABBREVIATIONS

Recipient Group : The natural or legal person category to which personal data is transferred by the data controller.

Explicit Consent; Consent on a specific subject, based on information and explained with free will.

Anonymization: Making personal data unlikely to be associated with an identified or identifiable real person in any way, even by matching it with other data.

Employee: Payroll personnel working within CatchProbe.

Electronic Media: Environments where personal data can be created, read, changed and written with electronic devices.

Non-Electronic Media: All written, printed, visual, etc. media other than electronic media.

Service Provider: A natural or legal person providing services under a specific contract with CatchProbe.

Relevant Person: The real person whose personal data is processed.

Relevant User: Persons who process personal data within the organization of the data controller or in accordance with the authorization and instruction received from the data controller, except for the person or unit responsible for the technical storage, protection and support of data.

Destruction; Deletion, destruction or anonymization of personal data.

Law; Personal Data Protection Law No. 6698.

Recording Media; All kinds of media containing personal data that are fully or partially automated or processed in non-automated ways provided that they are part of any data recording system.

Personal Data; All kinds of information related to the identified or identifiable real person.

Personal Data Processing Inventory: The inventory that the data controllers create by associating the personal data processing activities they carry out depending on their business processes with the personal data processing purposes, data category, the group of recipients transferred and the group of persons subject to the data and that they elaborate by explaining the maximum period required for the purposes for which the personal data are processed, the personal data envisaged to be transferred to foreign countries and the measures taken regarding data security.

Processing of Personal Data; All kinds of processes performed on personal data such as obtaining, recording, storing, keeping, changing, re-arranging, disclosing, transferring, taking over, making available, classifying or preventing their use in whole or in part, automatically or in non-automatic ways, provided that they are part of any data recording system.

Board; Personal Data Protection Board.

Sensitive Personal Data; Data related to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, dress, membership to associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.

Periodic Destruction; In the event that all the conditions for processing personal data in the Law disappear, the process of deletion, destruction or anonymization of personal data to be carried out ex officio at repeated intervals specified in the personal data storage and destruction policy.

Data Processor ; The natural or legal person who processes personal data on behalf of the data controller based on the authority given by him.

Data Registration System: The registration system in which personal data is processed and structured according to certain criteria.

Data Controller; The natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.

4. PERSONAL DATA STORAGE AND DISPOSAL POLICY

All departments and employees of CatchProbe actively support the responsible units in taking technical and administrative measures to ensure data security in all environments where personal data are processed in order to ensure the proper implementation of the technical and administrative measures taken by the responsible units within the scope of the Policy, to increase the training and awareness of the employees of the unit, to monitor and continuously control the unlawful processing of personal data, to prevent unlawful access to personal data and to ensure the lawful storage of personal data.

Personal data is securely stored by CatchProbe in accordance with the law in the environments listed below;

ELECTRONIC ENVIRONMENTS	NON-ELECTRONIC ENVIRONMENTS
Servers (Domain, backup, email, Database, web, file sharing, etc. Software (Office Software, Pars) Information security devices (firewall, antivirus, etc.) Personal computers (Desktop, laptop) Mobile devices (phone, tablet, etc.) Removable memories (USB, Memory Card etc.)	Paper Written, printed, visual media

- **Storage of Personal Data**

CatchProbe stores and destroys the personal data of the employees of the third parties, institutions or organizations to which they are related as customers, employees, employee candidates, customer candidate, customer's contact person, potential employee, reference, trainee, parent/guardian/representative and visitors in accordance with the Law.

In this context, detailed explanations regarding storage and disposal are given below respectively.

In Article 3 of the Law, the concept of processing of personal data is defined, in Article 4, it is stated that the personal data processed should be related to the purpose for which they are processed, limited and measured and should be kept for the period stipulated in the relevant legislation or for the purpose for which they are processed, and in Articles 5 and 6, the processing conditions of personal data are specified. Accordingly, CATCHPROBE stores personal data within the framework of its activities for the period stipulated in the relevant legislation or in accordance with our processing purposes.

- **Processing Purposes Requiring Storage**
- Execution of Emergency Management Processes
- Execution of Employee Candidate / Intern / Student Selection and Placement Processes
- Execution of Application Processes of Employee Candidates
- Fulfillment of Employment and Legislation Obligations for Employees
- Conducting Training Activities
- Execution of Access Authorizations
- Providing Physical Space Security
- Execution of Communication Activities
- Planning of Human Resources Processes
- Execution / Supervision of Business Activities
- Execution of Goods / Services Procurement Processes
- Execution of Goods / Services After-Sales Support Services
- Execution of Goods / Services Sales Processes
- Execution of Activities for Customer Satisfaction
- Execution of Noc Services
- Execution of Penetration Processes
- Execution of Performance Evaluation Processes
- Potential Employee Detection Process
- Execution of Advertising / Campaign / Promotion Processes
- Execution of SOC Services
- Execution of Contract Processes
- Execution of Wage Policy
- Follow-up of Requests / Complaints

- **Reasons for Destruction**

Personal data;

- Amendment or repeal of the provisions of the relevant legislation, which are the basis for processing,
- The disappearance of the purpose requiring its processing or storage,
- In cases where the processing of personal data takes place only on the basis of explicit consent, the data subject withdraws his explicit consent,

- CatchProbe accepts the application made by the relevant person for the deletion and destruction of personal data within the framework of the rights of the person concerned, pursuant to the California Consumer Privacy Act of 2018 (“CCPA”),
- In the event that CatchProbe rejects the application made to it with the request of deletion, destruction or anonymization of its personal data by the relevant person, finds the answer inadequate or does not respond within the period stipulated in the Law; filing a complaint to the Personal Data Protection Board and this request is approved by the Board,
- The maximum period for storing personal data has passed and there is no condition to justify storing personal data for a longer period,

In these cases, these are deleted, destroyed or ex officio deleted, destroyed or anonymized by CatchProbe at the request of the person concerned.

- **Ensuring the Security of Personal Data**

CatchProbe takes all necessary technical and administrative measures to ensure the appropriate level of security required for the protection of personal data.

As stipulated in the California Consumer Privacy Act of 2018 (“CCPA”)

- To prevent the unlawful processing of personal data,
- To prevent unlawful access to personal data,
- To ensure the protection of personal data.

and to take the necessary measures to ensure the conditions.

The measures implemented by CatchProbe to ensure the security of personal data are detailed in the sub-clauses.

- **Technical Measures**
- CatchProbe employs knowledgeable and experienced people to ensure data security and provides its personnel with the necessary Information Security Awareness Trainings and GDPR trainings.
- Necessary internal controls are made for the installed systems. It operates the processes of risk analysis, data classification, information security risk assessment and business impact analysis within the scope of the established systems.
- It creates an access authorization and control matrix and implements a separate access policy and procedures.
- Access authorizations are made according to the minimum authorization principle. Access authorizations of the disassociated personnel are removed.
- Personal data in the electronic environment is restricted from access between network components to prevent personal data security breaches.

• Technical measures are taken in accordance with the developments in technology. Software including firewalls, installation of hardware and infrastructure investments in accordance with the developing technology are made.
• Firewall, gateway measures and control of access movements against unauthorized access threats over the Internet are provided through logs.
• It takes the necessary measures to ensure that the software and hardware work properly and that the security measures taken for the systems are sufficient, and to close possible security vulnerabilities with regular penetration tests.
• Evaluations are made according to the results of the tests on the resulting vulnerabilities.
• CatchProbe enforces restrictions on access to personal data according to the least authorization principle. Access authorizations are checked periodically within the scope of the California Consumer Privacy Act of 2018 ("CCPA") and make access and authorization definitions in accordance with management process requirements. Controls the compliance of accesses to authorizations.
• It reports the information obtained as a result of checking the security of the systems to the relevant persons. Necessary technical measures are taken by identifying the points that pose a risk.
• It disseminates awareness to be a part of the corporate culture with a model that continuously processes technical measures in order to maintain the security of Personal Data and ensures that the measures taken are maintained continuously with controls.
• Processes such as deleting, crossing out or starring certain areas of personal data with the IGDPR application in a way that cannot be associated with an identified or identifiable natural person are applied.
• Camera systems and physical security measures are kept at a high level within the organization. Media monitoring, automatic fire extinguishing systems and access authorization controls of digital environments where personal data are kept are provided.
• When creating passwords and passwords, a password policy is created with combinations consisting of uppercase and lowercase letters, numbers and symbols instead of numbers or letter sequences that are associated with personal information and are easy to guess.

• **Administrative Measures**
• CatchProbe takes appropriate measures by accurately determining the probability of occurrence of the risks that may arise in relation to the preparation of the Personal Data Processing Inventory and the protection of such data and the losses that may arise in the event of such occurrence.
• When determining the risks, whether the personal data is personal data of special nature, to what extent it requires confidentiality due to its nature, and the nature and quantity of the damage that may arise in case of security breach are taken into consideration.
• Control and solution alternatives for reducing or eliminating risks are evaluated in line with the principles of cost, applicability and usefulness and planning the necessary technical and administrative measures.

• Support is provided for employees to make the first intervention even if they have limited information about attacks that will damage personal data security and cyber security and to receive awareness training for employees to ensure personal data security.
• In case of significant changes in policies and procedures related to personal data security, it is ensured that these changes are presented to the employees with new trainings and their information about the threats related to personal data security is kept up-to-date.
• Policies and procedures prepared for personal data security are appropriately integrated into the work and operation of the data controller.
• It is periodically evaluated whether the personal data received by the data controllers for processing purposes are still needed.
• In addition to ensuring that personal data are stored in the right place, in order to prevent unauthorized access, the data controllers take measures to keep personal data, which are frequently kept for archival purposes and which do not require access, in safer environments.
• Personal data that is not needed is safely destroyed in accordance with the personal data storage and destruction policy and the regulation on the deletion, destruction or anonymization of personal data.

• **Audits Conducted for Sustainability of Personal Data Protection**

In accordance with the California Consumer Privacy Act of 2018 ("CCPA") Law, it carries out or has carried out the necessary audits. It provides internal and external audits to ensure the sustainability of Information Security. It regularly performs penetration tests to the systems for technical vulnerabilities that may occur in the systems. Systems are regularly monitored by data processing. Necessary technical and administrative measures are taken to eliminate the findings obtained after management systems audits and risk analysis. When unlawful access or processing of personal data is detected in the audits, action is taken by determining the nonconformities/risks detected in a short time by notifying the senior management.

• **Measures Applied to Ensure Protection of Personal Data by Third Parties**

In its contracts with third parties, CatchProbe mutually maintains the necessary sanction clauses to prevent the unlawful processing of personal data, to prevent unlawful access to data and to ensure the protection of data. Confidentiality agreements are signed before sharing information with third parties. Necessary information is provided to third parties to raise awareness.

• **Measures Applied for the Protection of Sensitive Personal Data**

Adequate measures should be taken for sensitive personal data, both in terms of their qualifications and as they may lead to victimization or discrimination of individuals.

These data are data related to race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, costume and clothing, membership to associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.

CatchProbe takes the necessary measures to protect sensitive personal data determined as "sensitive" by the Law and processed in accordance with the law. The technical and administrative measures taken to protect personal data show sensitivity for sensitive personal data.

- **Creating Awareness to Ensure the Protection of Personal Data**

Necessary information is provided to employees, trainings are organized and their effectiveness is measured in order to increase awareness to prevent unlawful processing of personal data, unlawful access to data and to ensure the protection of data. Other documents related to "Personal Data Protection and Processing Policy" have been published on the website of our institution.

In case of changes in the relevant laws, regulations or legislation, the policies are revised and announced to the relevant persons again.

PERSONAL DATA DESTRUCTION TECHNIQUES

CatchProbe destroys the personal data it obtains at the request of personal data owners, due to legal obligations or if it is not obligated to use it for the protection of public order and provided that it does not affect the business processes. Personal data of data owners are destroyed based on the decision to be taken by the institution when the requirements of maintaining the service to our customers, fulfilling legal obligations, planning employee rights and benefits are eliminated. Each year, personal data that is not deemed necessary to be stored on the dates determined by the Data Controller Contact Person is destroyed by the following techniques in accordance with the legislation.

- **Deletion of Personal Data**

The methods of deletion of personal data are specified in the table below;

Data Recording Environment	Description
Personal Data on Servers	The system administrator removes the access authorization of the relevant users and deletes them for those who have expired from the personal data on the servers.
Personal Data in Electronic Media	Among the personal data in the electronic environment, the ones whose period has expired are rendered inaccessible and non-reusable for other employees (related users) except the database administrator.
Personal Data in Physical Environment	Among the personal data kept in the physical environment, it is made inaccessible and non-usable in any way for other employees, except for the unit manager responsible for the document archive, for those whose period of time has expired. In addition, the process of blackening is applied by drawing/painting/erasing in a way that cannot be read.
Personal Data in Portable Media	Those whose period of time required to be stored from personal data kept in flash-based storage environments are encrypted by the system

	administrator and access authority is given only to the system administrator and stored in secure environments with encryption keys.

- **Destruction of Personal Data**

The destruction of personal data is indicated in the table below;

Data Recording Environment	Description
Personal Data in Physical Environment	Those of which period of time required to be stored from personal data in the paper environment has expired are irreversibly destroyed in paper shredders.

- **Anonymization of Personal Data**

Anonymization of personal data is the making of personal data that cannot be associated with an identified or identifiable real person in any way, even if it is matched with other data.

In order for personal data to be anonymized, personal data must be rendered unassociable to an identified or identifiable real person, even by using appropriate techniques in terms of the recording medium and the relevant field of activity, such as the return of personal data by the data controller or third parties and/or the matching of data with other data.

- **STORAGE AND DESTRUCTION PERIOD**

In relation to personal data processed by CatchProbe within the scope of its activities;

- In the Personal Data Processing Inventory, the storage periods on the basis of personal data related to all personal data within the scope of the activities carried out depending on the processes;

Storage periods by data categories are updated in the Inventory Table.

Updates are made by the Personal Data Contact Person if necessary on the storage periods in question. Personal data with expired storage periods are disposed of ex officio.

The storage periods of personal data are specified in the table below;

Data	STORAGE PERIOD

Biometric Data	1 week for employees, 2 years for customer's contacts after the employment contract is over
Criminal Conviction and Security Measures	10 years
Sexual Life	2 years
Association Membership	2 years
Philosophical Belief, Religion, Sect and Other Beliefs	2 years
Finance	10 years
Physical Space Security	3 months
Genetic Data	2 years
Audiovisual Recordings	10 years
Legal action	2 years
Communication	10 years
Race and Ethnicity	5 years
Transaction Security	2 years
Dress	2 years
Identity	10 years
Location	2 years
Professional experience	10 years
Customer Transaction	10 years
Personnel Information	10 years
Marketing	2 years
Risk Management	2 years
Health Information	10 years
Union Membership	2 years
Political Opinion Information	2 years
Foundation Membership	10 years