Surveillance Technology Policy

Tennis Reservations Application
Recreation and Parks Department

The City and County of San Francisco values privacy and protection of San Francisco residents' civil rights and civil liberties. As required by San Francisco Administrative Code, Section 19B, the Surveillance Technology Policy aims to ensure the responsible use of the Tennis Reservations Spotery Application itself as well as any associated data, and the protection of City and County of San Francisco residents' civil rights and liberties.

PURPOSE AND SCOPE

The Recreation and Parks Department's ("Department") mission is to provide enriching recreational activities, maintain beautiful parks and preserve the environment for the well-being of our diverse community.

The Surveillance Technology Policy ("Policy") defines the manner in which the Tennis Reservations Spotery Application ("Spotery Application") will be used to support this mission, by describing the intended purpose, authorized and restricted uses, and requirements.

This Policy applies to all to department personnel that use, plan to use, or plan to secure Spotery , including employees, contractors, and volunteers. Employees, consultants, volunteers, and vendors while working on behalf of the City with the Department are required to comply with this Policy.

POLICY STATEMENT

The authorized use of Spotery Application technology for the Department is limited to the following use cases and is subject to the requirements listed in this Policy.

Authorized Use(s):

– Confirm that the person who reserved the booking for a tennis court is at the location at the reserved time.
– Utilize data to determine if there are any reservation holders who are violating booking policies because they are not showing up at the reserved time. Data can be accessed on the Spotery web application or as a report delivered by Spotery

Prohibited use cases include any uses not stated in the Authorized Use Case section.

Departments may use information collected from technology only for legally authorized purposes, and may not use that information to unlawfully discriminate against people based on race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, gender, gender identity, disability status, sexual orientation or activity, or genetic and/or biometric data. Additionally, departments may not use automated systems to scan footage and identify individuals based on any of the categories listed in the preceding sentence.

BUSINESS JUSTIFICATION

The Spotery Application supports the Department's mission and provides important operational value in the following ways:

The surveillance technology allows for equitable access to our recreational sites.

In addition, the Spotery Application promises to benefit residents in the following ways:

X Health - Residents are able to book reservations for tennis courts which allow for recreational and physical activity.

The Spotery Application will benefit the department in the following ways:

X Time Savings, Staff do not need to review and research anecdotal evidence about reservation holders not utilizing the court for the reserved time.

To achieve its intended purpose, the Spotery Application (hereinafter referred to as "surveillance technology" or "Spotery") allows a reservation holder to book a tennis court up to seven days in advance. 24 hours prior to the reservation, a reminder email is sent to the reservation holder. The reminder email contains a check-in button. The reservation holder can use the check-in button on their mobile device within 15 minutes before or after the reservation time. Spotery checks the location of the reservation holder to ensure that they are within 0.1 miles of the tennis court. Spotery needs access to the reservation holder's location so "Enable Location Services" must be turned on the mobile device.

POLICY REQUIREMENTS

This Policy defines the responsible data management processes and legally enforceable safeguards required by the Department to ensure transparency, oversight, and accountability measures. Department use of surveillance technology and information collected, retained, processed or shared by surveillance technology must be consistent with this Policy; must comply with all City, State, and Federal laws and regulations; and must protect all state and federal Constitutional guarantees.

Specifications: The software and/or firmware used to operate the surveillance technology must be up to date and maintained.

Safety: Surveillance technology must be operated in a safe manner. Surveillance technology should not be operated in a way that infringes on resident civil rights, including privacy, or causes personal injury or property damage.

Data Collection: Departments shall minimize the use, collection, and retention of Personally Identifiable Information (PII) to what is strictly necessary to accomplish the intended purpose of the surveillance technology.

Department shall only collect data required to execute the authorized use case. All data collected by the surveillance technology, including PII, shall be classified according to the City's Data Classification Standard.

Should information be incidentally collected that is not necessary to accomplish the intended purpose of the surveillance technology, including information that may be used to identify persons or private information, Department shall remove all incidental PII from raw data.

The surveillance technology collects the following data types:

- Types of Data Collected: Name, email address, address, geolocation data
- Data Classification Level: Level 2

Geolocation is briefly accessed by the Spotery Company at the time a reservation holder checks-in. It is not stored or made accessible to the Department.

Notification: Departments shall notify the public of intended surveillance technology operation at the site of operations through signage in readily viewable public areas. Department notifications shall identify the type of technology being used and the purpose for such collection.

Department includes the following items in its public notice:

- Contact information
- Data Retention
- Description of the authorized use
- Information on the surveillance technology
- Type of data collected

Access: All parties requesting access must adhere to the following rules and processes (please refer to the data sharing section to ensure all information covered in that section is also included below):

- Prior to accessing or using data, authorized individuals receive training and instruction regarding authorized uses. Training includes how to login and run reports.

Data must always be scrubbed of PII as stated above prior to public use.

A. Department employees

Once collected, the following roles and job titles are authorized to access and use data collected, retained, processed or shared by the surveillance technology:

- Chief Information Officer (0941)

- Director of Property, Permits, and Reservation (0953) or designee – Administrative Analyst(s) (1820 series)

B. Members of the public, including criminal defendants

The Recreation and Parks Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

Collected data that is classified as Level 1-Public data may be made available for public access or release via DataSF's Open Data portal. Anyone, including criminal defendants, may access such data. Open Data has a Public Domain Dedication and License, and makes no warranties on the information provided. Once public on Open Data, data can be freely shared, modified, and used for any purpose without any restrictions. Any damages resulting from use of public data are disclaimed, including by criminal defendants.

Members of the public, including criminal defendants, may also request access by submission of a request pursuant to San Francisco's Sunshine Ordinance. No record shall be withheld from disclosure in its entirety unless all information contained in it is exempt from disclosure under express provisions of the California Public Records Act or some other statute.

Data Security: Department shall secure PII against unauthorized or unlawful processing or disclosure; unwarranted access, manipulation or misuse; and accidental loss, destruction, or damage. Surveillance technology data collected and retained by the Department shall be protected by the safeguards appropriate for its classification level(s).

To protect surveillance technology information from unauthorized access and control, including misuse, Departments shall, at minimum, apply the following safeguards:

The access is limited only to the following roles: Chief Information Officer, Director of Property, Permits and Reservations, or designee.

Data Sharing: The Recreation and Parks Department will endeavor to ensure that other agencies or departments that may receive data collected by the Recreation and Parks Department's Spotery Application will act in conformity with this Policy.

For internal data, shared data shall not be accessed, used, or processed by the recipient in a manner incompatible with the authorized use cases stated in this Policy.

The Recreation and Parks Department shall ensure proper administrative, technical, and physical safeguards are in place before sharing data with other CCSF departments, outside government entities, and third-party providers or vendors. (See Data Security)

The Recreation and Parks Department shall ensure all PII and restricted data is de-identified or adequately protected to ensure the identities of individual subjects are effectively safeguarded.

Further, in sharing data, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual person, data concerning health or data concerning an individual person's sex life or sexual orientation shall be prohibited.

Each department that believes another agency or department receives or may receive data collected from its use of surveillance technologies should consult with its assigned deputy city attorney regarding their response.

Before sharing data with any recipients, the Department will use the following procedure to ensure appropriate data protections are in place:

- X Confirm the purpose of the data sharing aligns with the department's mission.
- X Consider alternative methods other than sharing data that can accomplish the same purpose.
- X Redact names, scrub faces, and ensure all PII is removed in accordance with the department's data policies.
- X Review of all existing safeguards to ensure shared data does not increase the risk of potential civil rights and liberties impacts on residents.
- X Evaluation of what data can be permissibly shared with members of the public should a request be made in accordance with the San Francisco's Sunshine Ordinance.
- X Ensure data will be shared in a cost-efficient manner and exported in a clean, machine-readable format.

The Recreation and Parks Department will comply with the California Public Records Act, the San Francisco Sunshine Ordinance, the requirements of the federal and State Constitutions, and federal and State civil procedure laws and rules.

The Department currently participates in the following sharing practices:

A. Internal Data Sharing

The department does not share surveillance technology data with other departments or entities inside the City and County of San Francisco.

B. External Data Sharing

To ensure that entities receiving data collected by the surveillance technology comply with the Surveillance Technology Policy, Department shall:

The Chief Information Officer and the Director of Property, Permits and Reservations or designee will be responsible for enforcing the Surveillance Technology policy through recurring review of functionality and use.

The department does not share surveillance technology data externally with entities outside the City and County of San Francisco.

Before data sharing with any recipient, the Department will confirm the purpose of the data sharing aligns with the department's mission to ensure appropriate data protections are in place.

Data Retention: Department may store and retain raw PII data only as long as necessary to accomplish a lawful and authorized purpose.

The Department's data retention period and justification are as follows:

Retention Period	**Retention Justification**
Report Downloaded from Spotery (see Appendix A for example report)- These are manually downloaded from the web application by Department staff and are saved on the file server. These will be stored for up to 1 year. Geolocation – Spotery briefly accesses geolocation as determined by the application user's mobile device Global Positioning System (GPS) at the time the user checks-in to tennis reservation. This data is not made accessible to the department.	Reports - This retention period allows for ample time for staff to analyze data regarding reservation holder usage and can determine if there were any violations to Department policy. Geolocation data is only accessed to determine that the user is within 0.1 miles of the tennis court and to update reservation status (see Appendix A for sample data). Geolocation data is not stored by Spotery and is never accessed by the Department (see Appendix B for Spotery Privacy Policy).

PII data shall not be kept in a form which permits identification of data subjects for any longer than is necessary for the purposes for which the personal data are processed.

Data collected in the Spotery Application reports downloaded by the Department is stored and safeguarded in the following location:

- DT Data Center

- Spotery's Privacy Policy (Appendix B) provides information on how the Spotery Company safeguards data

Data Disposal: Upon completion of the data retention period, Department shall dispose of data in the following manner:

- Reports (See Appenda A for sample report) - these are manually downloaded from the Spotery web application by Department staff and are saved on the file server. These will be stored for up to 1 year and deleted in an automated process.

- Geolocation Data - No geolocation data is provided to the Department. Spotery Application temporarily accesses geolocation data but does not retain ongoing (see Spotery Privacy Policy in Appendix B).

Training: To reduce the possibility that surveillance technology or its associated data will be misused or used contrary to its authorized use, all individuals requiring access must receive training on data security policies and procedures.

At the very least, department shall require all elected officials, employees, consultants, volunteers, and vendors working with the technology on its behalf to read and formally acknowledge all authorized and prohibited uses. Department shall also require that all individuals requesting data or regularly requiring data access receive appropriate training before being granted access to systems containing PII.

Training is required for authorized individuals to use or access the information collected. Prior to accessing or using data, authorized individuals receive training and instruction regarding authorized uses. Training includes how to login and run reports.

COMPLIANCE

Department shall oversee and enforce compliance with this Policy using the following methods:

The Chief Information Officer and the Director of Property, Permits and Reservations or designee will be responsible for enforcing the Surveillance Technology policy through recurring review to ensure data is used only for the approved use cases: (a) Confirmation that the person who reserved the booking for a tennis court is at the location at the reserved time; (b) Utilization of data to determine if there are any reservation holders who are violating booking policies because they are not showing up at the reserved time. Data can be accessed on the Spotery web application or as a report delivered by Spotery.

Department shall be assigned the following personnel to oversee Policy compliance by the Department and third-parties:

> Chief Information Officer (0941) and the Director of Property, Permits and Reservation (0953) or designee - Administrative Analysts (1820 series)

Sanctions for violations of this Policy include the following:

> Violation of the policy will be subject to Recreation and Parks Departmental policies, which may include disciplinary action up to and including termination.

If a Department is alleged to have violated the Ordinance under San Francisco Administrative Code Chapter 19B, Department shall post a notice on the Department's website that generally describes any corrective measure taken to address such allegation.

Department is subject to enforcement procedures, as outlined in San Francisco Administrative Code Section 19B.8.

EXCEPTIONS

Only in exigent circumstances or in circumstances where law enforcement requires surveillance technology data for investigatory or prosecutorial functions may data collected, retained or processed by the surveillance technology be shared with law enforcement.

DEFINITIONS

Personally Identifiable Information:	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.
Raw Data:	Information collected by a surveillance technology that has not been processed and cleaned of all personal identifiable information. The distribution and use of raw data is tightly restricted.
Exigent Circumstances	An emergency involving imminent danger of death or serious physical injury to any person that requires the immediate use of Surveillance Technology or the information it provides.

AUTHORIZATION

Section 19B.4 of the City's Administrative Code states, "It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class."

QUESTIONS & CONCERNS

Public:

Members of the public can register complaints/concerns or submit questions to San Francisco Recreation and Parks Department through several ways: (a) Send written correspondence to McLaren Lodge in Golden Gate Park, 501 Stanyan Street, San Francisco, CA 94117; (b) Call to the Recreation and Parks Department Front Desk 415-831-2700; (c) Send an email to rpdinfo@sfgov.org; or (d) Contact 311.

Department shall acknowledge and respond to complaints and concerns in a timely and organized response.

All calls/complaints from the public received via mail or via call to the Department Front Desk are routed to the Department IT HelpDesk and logged in our department's request management system. Any requests from 311 are received in our department's dispatch system and routed to the Department IT HelpDesk which then is logged in the request management. Once the request is tracked in the request management system, IT will work with all relevant parties to ensure completion. Review of open / closed requests occur with the CIO on a weekly basis.

City and County of San Francisco Employees:

All questions regarding this policy should be directed to the employee's supervisor or to the director. Similarly, questions about other applicable laws governing the use of the surveillance technology or the issues related to privacy should be directed to the employee's supervisor or the director.

Appendix A: Sample of Report Downloaded by Department from the Spotery Application

Reservation	Spot	Status	Date from	Time from	Time to
2714335.	Hamilton Rec Tennis Court #2	Checked-In	3/17/2022	1:30 PM	3:00 PM
2714327.	Hamilton Rec Tennis Court #1	Canceled by User	3/17/2022	10:30 AM	12:00 PM
333369.	Hamilton Rec Tennis Court #2	Booked	5/01/2022	12:00 PM	1:30 PM

Appendix B: Spotery Privacy Policy

Last updated: March 2022

Welcome to Spotery, an online marketplace for short term rental of facilities provided by Social Solutions, LLC (the "Company", "SSL", "Spotery", "us", "our", and/or "we"). We are committed to ensure that the personal information that you share on our Site and/or Services is protected and kept confidential. By accepting the Terms of Service or providing information through our Site or mobile application, you agree to the use and disclosure of personal identifiable information, as detailed in this Privacy Policy.

I. Key Terms

Unless otherwise defined in this Privacy Policy, capitalized terms shall have the meaning set forth on the Terms of Use.

II. Information Collected

1. Information Collected from your use

We ask for and collect the following personal information about you when you use the Site. This information is necessary for the adequate performance of the contract between you and us and to allow us to comply with our legal obligations and given our legitimate interest in being able to provide and improve the functionalities of the Site and Services. Without it, we may not be able to provide you with all the requested services.

- **Account Information.** When you sign up for a Spotery Account, we require certain information such as your first name, last name, email address, and date of birth.
- **Profile and Listing Information.** To use certain features of the Site (such as booking or creating a listing), we may ask you to provide additional information, which may include your address, phone number, and a profile picture.
- **Identity Verification Information.** To help create and maintain a trusted environment, we may collect identity verification information (such as images of your government issued ID, passport, national ID card, or driving license, as permitted by applicable laws) or other authentication information.
- **Payment Information.** To use certain features of the Site (such as booking or creating a listing), we may require you to provide certain financial information (like your bank account or credit card information) in order to facilitate the processing of payments.

- **Communications with Spotery and other Members.** When you communicate with Spotery or use the Site to communicate with other Members, we collect information about your communication and any information you choose to provide.
- **Geolocation Information.** For certain features of the Site, we may capture geolocation information about your approximate location as determined by your mobile device's GPS to provide you with an enhanced user experience. Most mobile devices allow you to control or disable the use of location services for apps in the device's settings menu. We do not store geolocation data, as it is only necessary to activate certain functionalities at the time of use.
- **Usage Information.** We collect information about your interactions with the site such as the pages or content you view, your searches for Listings, bookings you have made, and other actions on the Site.
- **Log Data and Device Information.** We automatically collect log data and device information when you access and use the Site, even if you have not created a Spotery Account or logged in. That information includes, among other things: details about how you've used the Site (including if you clicked on links to third party applications), IP address, access dates and times, hardware and software information, device information, device event information, unique identifiers, crash data, cookie data, and the pages you've viewed or engaged with before or after using the Site.
- **Cookies and Similar Technologies.** We use cookies and other similar technologies when you use our platform, use our mobile app, or engage with our online ads or email communications. We may collect certain information by automated means using technologies such as cookies, web beacons, pixels, browser analysis tools, server logs, and mobile identifiers. In many cases, the information we collect using cookies and other tools is only used in a non-identifiable without reference to personal information. For example, we may use information we collect to better understand website traffic patterns and to optimize our website experience. In some cases, we associate the information we collect using cookies and other technology with your personal information. Our business partners may also use these tracking technologies on the Site or engage others to track your behavior on our behalf.
- **Pixels and SDKs.** Third parties, including Facebook, may use cookies, web beacons, and other storage technologies to collect or receive information from our websites and elsewhere on the internet and use that information to provide measurement services and target ads. For apps, that third parties, including Facebook, may collect or receive information from your app and other apps and

use that information to provide measurement services and targeted ads. Users can opt-out of the collection and use of information for ad targeting by updating their Facebook account ad settings and by contacting support@spotery.com with a description of your request and validation information.

- **Total Fee Payment Transactions.** We collect information related to your payment transactions through the Site, including the payment instrument used, date and time, payment amount, payment instrument expiration date and billing postcode, email address, IBAN information, your address and other related transaction details. This information is necessary for the adequate performance of the contract between you and Spotery.

2. Information Collected from you from third parties

- **Third Party Services.** If you link, connect, or login to your Spotery Account with a third party service (e.g. Google, Facebook), the third party service may send us information such as your registration, friends list, and profile information from that service. This information varies and is controlled by that service or as authorized by you via your privacy settings at that service.
- **Background Information.** To the extent permitted by applicable laws, Spotery may obtain reports from public records of criminal convictions or sex offender registrations.
- **Referrals.** If you are invited to Spotery, the person who invited you may submit personal information about you, such as your email address or other contact information.
- **Other Sources.** To the extent permitted by applicable law, we may receive additional information about you, such as demographic data or information to help detect fraud and safety issues, from third party service providers and/or partners, and combine it with information we have about you. For example, we may receive background check results (with your consent where required) or fraud warnings from service providers like identity verification services for our fraud prevention and risk assessment efforts. We may receive information about you and your activities on and off the site through partnerships, or about your experiences and interactions from our partner ad networks.

III. Use and Sharing of Information Collected

Your acceptance of the Terms of Service and this Privacy Policy grant Spotery a worldwide non-exclusive, transferable, irrevocable, sublicensable, royalty-fee license to use your personal information for the purposes set forth herein and as permissible under applicable laws or regulations. By accepting the Privacy Policy and the Terms of Service, you understand our policies and practices regarding your personal information and how we will treat it.

We may use, store, and process personal information to (1) provide, understand, improve, and develop the Site, (2) create and maintain a trusted and safer environment (such as to comply with our legal obligations and ensure compliance with our policies) and (3) provide, personalize, measure, and improve our advertising and marketing.

We process this personal information for these purposes given our legitimate interest in improving and protecting the Site and our Members' experience with it, and where it is necessary for the adequate performance of the contract with you and to comply with applicable laws. We will also process your personal information for the purposes listed in this section, given our legitimate interest in undertaking marketing activities to offer you products or services that may be of your interest.

We may share your personal information for one or more of the following reasons:

- **Social media**

  Where permissible according to applicable law we may use certain limited personal information about you, such as your email address, to hash it and to share it with social media platforms, such as Facebook or Google, to generate leads, drive traffic to our websites or otherwise promote our products and services or the Site. These processing activities are based on our legitimate interest in undertaking marketing activities to offer you products or services that may be if your interest.

  The social media platforms with which we may share your personal information are not controlled or supervised by Spotery. Therefore, any questions regarding how your social media platform service provider processes your personal information should be directed to such provider.

- **Members**

  To help facilitate bookings or other interactions between Members, we may need to share certain information, including personal information but excluding financial information, with other Members, as it is necessary for the adequate performance of the contract between you and us

- **Affiliated parties**

  To enable or support us in providing the Site and Services, we may share your information, including personal information, within our corporate family of companies (both financial and non-financial entities) that are related by common ownership or control.

- **Compliance with Law and Government Requirements**

  Spotery may disclose your information, including personal information, to courts, law enforcement, governmental authorities, tax authorities, or authorized third parties, if and to the extent we are required or permitted to do so by law or if such disclosure is reasonably necessary:

  (i) to comply with our legal obligations, (ii) to comply with a valid legal request or to respond to claims asserted against Spotery or its affiliated parties, (iii) to respond to a valid legal request relating to a criminal investigation or alleged or suspected illegal activity or any other activity that may expose us, you, or any other of our users to legal liability, (iv) to enforce and administer our Terms of Service or other policies and agreements with Members, or (v) to protect the rights, property or personal safety of Spotery, its employees, its Members, or members of the public.

  Where appropriate, we may notify Members about legal requests unless: (i) providing notice is prohibited by the legal process itself, by a court order we receive, or by applicable law, or (ii) we believe that providing notice would be futile, ineffective, create a risk of injury or bodily harm to an individual or group, or create or increase a risk of fraud upon Spotery's property, its Members and the Site. In instances where we comply with legal requests without notice for these reasons, we may attempt to notify that Member about the request after the fact where appropriate and where we determine in good faith that we are no longer prevented from doing so.

  In jurisdictions where Spotery facilitates or requires a registration, notification, permit, or license application of a Facility Owner or Service Provider with a local governmental authority through the Site in accordance with local law, we may share information of participating Facility Owners or Service Provider with the relevant authority, both during the application process and, if applicable, periodically thereafter.

In jurisdictions where Spotery facilitates the Collection and Remittance of Occupancy Taxes where legally permissible according to applicable law, expressly grant us permission, without further notice, to disclose Members' data and other information relating to them or to their transactions, bookings, Accommodations and Occupancy Taxes to the relevant tax authority.

- **Service Providers**

  Spotery uses a variety of third-party service providers to help us provide services related to the Site and the Services. Spotery will require compliance with the laws from said third parties. But you as a user must understand that Spotery is not responsible for the privacy practices of any third-party service provider, nor for their acts or omissions.

IV. Security

We are continuously implementing and updating administrative, technical, and physical security measures to help protect your information against unauthorized access, loss, destruction, or alteration. Some of the safeguards we use to protect your information are firewalls and data encryption, and information access controls. If you know or have reason to believe that your Spotery Account credentials have been lost, stolen, misappropriated, or otherwise compromised or in case of any actual or suspected unauthorized use of your Spotery Account, please contact us following the instructions in the Contact Us section below.

V. Severability

All personal information collected will be secured in accordance with the policies in force at the time of its collection. If any of these conditions is considered invalid, void or for any reason unenforceable, that condition will be considered severable and will not affect the validity and enforceability of any remaining conditions.

VI. Modifying or deleting your personal information

If you wish to modify your personal information, or if you wish to discontinue receiving materials from us or wish to remove your personal information from Spotery's database, you can contact us at s upport@spotery.com. Please allow up to 72 hours to process your request.

VII. Personal data retention

We retain personal data only for as long as is needed to exercise our legal obligations and for appropriate business purposes.

If you contacted us to delete your data, Spotery may retain limited aggregate information for research purposes and to help us further improve our services and exercise our legal obligations.

This aggregate information does not include any personal data that relates to you as an individual.

VIII. Changes to the Privacy Policy

In the future, we may modify our Privacy Policy. In case of changes, we will make sure to publish them on the Site and in other places that we consider appropriate.

CONTINUING USING THE SITE AFTER PUBLICATIONS REGARDING CHANGES OR MODIFICATIONS TO THE PRIVACY POLICY CONSTITUTES AN ACCEPTANCE BY THE USER OF SUCH CHANGES OR MODIFICATIONS. IF USER DISAGREES WITH THE CHANGES OR MODIFICATIONS, THE USER MUST IMMEDIATELY WITHDRAW FROM THE USE OF THE SITE.

IX. Questions

If you have any questions regarding our Privacy Policy, email us at info@spotery.com.