One Maritime Plaza

PRIVACY POLICY

Effective as of [_____].

PDF version.
Prior versions.

This Privacy Policy is not a contract and does not create any legal rights or obligations.

This Privacy Policy describes how PPF OFF One Maritime Plaza, LP and our corporate subsidiaries and affiliates (collectively, "One Maritime Plaza", "we", "us", or "our") collects, uses and shares your personal information if you visit our property at One Maritime Plaza in San Francisco, California, visit onemaritimeplaza.com or our other websites or services that link to this Privacy Policy (collectively, the "Services"), contact us, receive our communications or attend our events.

This Privacy Policy does not address your relationship with your employer if your employer is a tenant of the building nor the Host App, which is developed by a service provider to us. You can learn more about how the Host app developer and host (CBRE, Inc.) uses data on connection with Host here.

Table of Contents (click to jump)

Personal Information We Collect

- Building Management. The below contact information are used to manage the lease and for managing the building.
    - Tenant Contact Info: Name, Email, Phone Number(s).

- Access Control. We use a variety of measures to control who can access the building. We do this for security and to protect the rights of the tenants and other lawful visitors.
    - For tenant employees or contractors: Mobile App Data from Blubox (see description below and privacy policy here); location data; identification details. Name, email, phone number.
    - For guests: first and last name; we inspect the guest's driver's license to verify name. As of the date of this policy, our practice is that if a contractor wants to check out a key to a part of the building, we write down the first and last name and hold the id in a locked box until the key is returned.
    - Deliveries: We collect license plate details of vehicles entering the loading dock. As of the date of this policy, our practice is that a security officer sits at the loading dock desk and writes the information down; it is then scanned and the papers are stored. Our policy is to not keep this for longer than 5 years.
- Security. We collect personal information as part of our security programs.
    - We use closed circuit television cameras ("CCTV") as part of our security program. CCTV captures images only. In other words, we collect video only; no audio. The building has cameras internally and externally throughout the building and the larger property. We use CCTV footage to help secure the building and protect tenants and their employees and guests. We also use it to review past incidents. As of the date of this policy, our practice is that we do not use a facial recognition technology to match the images to names.
    - In addition to building security, we may use video cameras to monitor activities in bars and restaurants on our property. In particular, we may in the future engage service providers to monitor alcohol consumption to help ensure legal distribution and consumption of alcohol. Restaurants and bars on our property have video surveillance in place.
    - BOLO. As part of our security program, we may receive alerts to "Be On the Lookout" for a specified person considered to be a security threat, such as flagged terminated employees or those who have or have been accused of relationship violence or stalking ("BOLO"). We may receive a BOLO request from law enforcement or from tenants and their employees and contractors. The information often includes: first and last name, address, height/weight, photo, last alias, and where last located.
- Tenant Amenities. We collect information about individuals seeking to use tenant amenities to provide those amenities.
    - Pet Guests: For building occupants that wish to bring a pet, our policy is to collect first and last name (in connection with a description of the pet and the pet's photo), company/employer name, floor number, and occupant's phone

number; if the pet is a service animal, our policy is to also collect the license number of the service animal.
    - Bike Storage: if a building occupant wishes to bring a bike into the bike room, our policy is to collect the person's first and last name + company/employer name, floor number, occupant's phone number, and a description of the bike.
    - Shower rooms: name, phone number, company/employer.
    - Liability Waivers: Our policy is to collect liability waivers from each of the foregoing categories of occupants and then scan them into our electronic document retention system.
- Emergency Procedures. We collect certain personal information for use in an emergency.
    - Emergency Contact List: We receive various information related to individuals to contact in the event of an emergency (e.g., phone numbers, names of contact, office/home/cell numbers, titles, floors, email; if offsite, physical address of notification person.)
    - Disabilities and Health Conditions
        - We collect various disability and health-related information so that we may use it if an evacuation occurs and to coordinate emergency responses. We may share it with emergency responders.
    - Deliveries: We collect license plate details of vehicles entering the loading dock. As of the date of this policy, our practice is that a security officer sits at the loading dock desk and writes the information down; it is then scanned and the papers are stored. Our policy is to not keep this for longer than 5 years.
- Contact Details for Tenant Occupants (e.g., employees and contractors): Name, address, email, telephone number.
- Identification Data: Our driver’s license or passport ID scanner collects information from government-issued documentation (via the magnetic strip on the back of the ID card) to verify and store identity of various individuals in the building. Our policy is to set the preferences of the third-party electronic readers to pull from documentation the first and last name only. We have communicated this preference to the vendor we use for the scanners. You can review our current vendor's (i.e., Blusky/Blubox, which licenses this technology from a third party) privacy policy here.
- Location Data: For building occupants using an app to access access-controlled building space, our service provider will collect from your phone GPS coordinates or similar location information regarding the location of your device. In particular, when have the app open, it detects where you are in the building. This information is used to identify the closest card reader location for mobile entry access. The service provider has indicated to us that this feature doesn't run in the background; it runs

only while app is open. The privacy policy for our current service provider, Blubox, is here.

- Mobile App Data for Building Access via MobileAccessHID (app) or a KeyCard: We use HID for key card access to building spaces and to apply access invitations to the users' mobile calendar. The mobile app collects: Wi-Fi SSID/Mac Address; user commands, voice commands, and transcriptions; text commands; user history; scheduled calendar events and attendees; in-app actions; device info; browser history; and user preferences. The key card also uses and holds the same information. So building occupants must either download the MobileAccessHID app or use a key card for access. HID's privacy policy is here.
- Professional Information: An individual's professional information, for example, business title, position, organization, etc. is collected to create the users' profiles within building apps.
- Written Signature- An individual's written signature, such as a signature on a contract, indemnity form, and/or lease contract are collected as part of building management (examples include security officers collecting it from contractors signing in, tenants needing to sign to get a property removal pass (such as when taking out boxes or computers)).

Feedback or correspondence, such as information you provide when you contact us with questions or feedback or otherwise correspond with us. Angus is the online system we currently use for submitting maintenance requests (and in the future we may use the Host app for this functionality). The system requires name, building floor, phone number, and tenant identity and work email. And you must be logged in to the system to make these requests.

Usage information, such as information about how you use the Services and interact with us, including information you provide when you use any interactive features of the Services, such as through the Host app.

Marketing information, such as your preferences for receiving communications about the building (e.g., we have a newsletter that is sent to tenant contacts) and details about how you engage with our communications.

Other information that we may collect which is not specifically listed here, but which we will use in accordance with this Privacy Policy or as otherwise disclosed at the time of collection.

Information Collected by Automated Means

We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and activity occurring on or through the Services or your use of our website. The

information that may be collected automatically includes your computer or mobile device operating system type and version number, manufacturer and model; device identifier; browser type; screen resolution; IP address; the website you visited before browsing to our website; general location information such as city, state or geographic area; and information about your use of and actions on the Services, such as pages or screens you viewed, how long you spent on a page or screen, navigation paths between pages or screens, information about your activity on a page or screen, access times, and length of access. Our service providers and business partners may collect this type of information over time and across third-party websites and mobile applications.

How We Use Your Personal Information

We use your personal information for the following purposes and as otherwise described in this Privacy Policy or at the time of collection:

To manage the building. We use your personal information as provided above and generally to:

- provide, operate, and improve the facilities;
- establish and maintain your occupant profile;
- communicate with you about the building, including by sending you announcements, updates, security alerts, and support and administrative messages;
- provide support and maintenance for the building; and
- respond to requests, questions, and feedback.

To comply with law. We use your personal information as we believe necessary or appropriate to comply with applicable laws, lawful requests, and legal process, such as to respond to subpoenas or requests from government authorities.

For compliance, fraud prevention, and safety. We may use your personal information and disclose it to law enforcement, government authorities, and private parties as we believe necessary or appropriate to: (a) protect our, your, or others' rights, privacy, safety, or property (including by making and defending legal claims); (b) enforce the terms and conditions that govern the Services; and (c) protect, investigate, and deter against fraudulent, harmful, unauthorized, unethical, or illegal activity.

With your consent. In some cases we may specifically ask for your consent to collect, use, or share your personal information, such as when required by law.

To create anonymous data. Our service providers may create aggregated and other anonymous data from your personal information and other individuals whose personal information we collect. They may make personal information into anonymous data by removing information that makes the data personally identifiable to you. They may use this anonymous data and share it with third parties for lawful business purposes, including to analyze and improve the Services and promote our business.

How Long We Retain Your Personal Information

We retain personal information as long as necessary to provide the Services. Our policy is that when a person is terminated, they become inactive in our systems. When a tenant leaves, our policy is to delete the personal data related to their employees and contractors. Our current vendor allows us to identify and request deletion of personal data in 90 days and our policy is to do that when a person becomes inactive due to their or their

employer's termination. We also retain your information as necessary to comply with our legal obligations, resolve disputes, and enforce our terms and policies.

How We Share Your Personal Information

We do not share your personal information with third parties without your consent, except in the following circumstances or as otherwise described in this Privacy Policy:

Affiliates. We may share your personal information with our corporate subsidiaries and affiliates for purposes consistent with this Privacy Policy.

Service providers. We may share your personal information with third-party companies and individuals that provide services on our behalf or help us operate the Services (such as CBRE). These third parties may use your personal information only as authorized by their contracts with us. As of the date we wrote this policy, we use CBRE to manage the building and provide the Host App (privacy policy is here); Avigilon as our surveillance company for CCTV and Glimpse may be used by our operators to review surveillance footage for improper activity within Bar Sprezzatura; Blubox/Blusky for access control (privacy policy is here); Allied Universal PP0 14417 Security Services (physical, electronic security contractor with a privacy policy here).

Professional advisors. We may disclose your personal information to professional advisors, such as lawyers, bankers, auditors, and insurers, where necessary in the course of the professional services that they render to us.

For compliance, fraud prevention and safety. We may share your personal information for the compliance, fraud prevention and safety purposes described above.

Government Requests. Notwithstanding anything to the contrary in this policy, we may preserve or disclose your information if we believe that it is reasonably necessary to comply with a law, regulation, or legal request or to protect the safety, property, or our rights or others'. However, nothing in this policy is intended to limit any legal defenses or objections that you may have to a third party or government request to disclose your information.

Business transfers. We may sell, transfer, or otherwise share some or all of our business or assets, including your personal information, in connection with a (potential) business transaction such as a corporate divestiture, merger, consolidation, acquisition, reorganization or sale of assets, or in the event of bankruptcy or dissolution.

Your Choices

In this section, we describe the rights and choices available to all users.

Access or update your information. If you have registered for an account with us, you may review and update certain personal information in your account profile by logging into your account. Tenant contacts, please contact us to do this. Tenant employees can do this in the Host app or by contacting us and for other purposes (bike agreement, showers, property checkout, etc.) please contact us.

Do Not Track. Some Internet browsers may be configured to send "Do Not Track" signals to the online services that you visit. We currently do not track users and hence do not respond to "Do Not Track" or similar signals. To find out more about "Do Not Track," please visit www.allaboutdnt.com.

Choosing not to share your personal information. Where we are required by law to collect your personal information, or where we need your personal information to provide the Services to you, if you do not provide

this information when requested (or you later ask to delete it), we may not be able to provide you with the Services. We will tell you what information you must provide to receive the Services by designating it as required at the time of collection or through other appropriate means.

Other Sites, Mobile Applications, and Services

The Services may contain links to, or content or features from, other websites and online services operated by third parties such as Host. These links are not an endorsement of, or representation that we are affiliated with, any third party. In addition, our content may be included on web pages or in mobile applications or online services that are not associated with us. We do not control third-party websites, mobile applications, or online services, and we are not responsible for their actions. Other websites and services follow different rules regarding the collection, use, and sharing of your personal information. We encourage you to read the privacy policies of the other websites and mobile applications and online services you use.

Security Practices

The security of your personal information is important to us. We employ a number of organizational, technical and physical safeguards designed to protect the personal information we collect. However, security risk is inherent in all internet and information technologies and we cannot guarantee the security of your personal information. As of the date of this policy, it is our policy to use the following security practices:

Examples of some of our security practices (not all of these are used in all instances, but give a sense of our policies and practices) include:

1. Quarterly password change prompts for critical infrastructure access
2. Encrypted WiFi for tenants
3. Encrypted websites (ie, they use https as opposed to http)
4. Least permissioning on Windows accounts containing access to personal information
5. Isolated subnets on some of our network
6. Least internet permission on lighting system subnet
7. Restricted physical access to company computers containing personal information
8. Use of Windows Defender
9. Client isolation on WiFi
10. No cookies/trackers on our website
11. Only employees who need the information to perform a specific job (provide record of person arrival/departure time or verifying status of employment by searching status of access badge) are granted access to personally identify information. The computers and servers in which we store personal identity information are kept in a secure environment.
12. Where offered by our service providers, we use MFA (2-factor authentication) for services that process personal info.
13. CBRE has assured us that its employees and contractors use an intranet and a secure firewall.

Data Retention

We retain your information for as long as necessary to provide you and our other users of our website and apps and visitors and tenants of our buildings our services. In several instances, we strive to delete personal data every 90 days, such as for security video footage and our tenant directory maintained by our security team for badging. Similarly, certain personal data stored in our in cloud infrastructure is 90 days by default. Storage of

activity on our website may be kept for up to a year. In all instances, we may store personal information for a longer period where we have a security concern. We also retain your information as necessary to comply with our legal obligations, resolve disputes, and enforce our terms and policies.

Your California Privacy Rights

For rights under the California Consumer Privacy Act and the amendments to it enacted by the Consumer Privacy Rights Act (CCPA), if applicable, please see our separate policy below. This section covers California rights other than CCPA.

- Shine Your Light Law. Under California law, California residents are entitled, once per calendar year, to ask us for a notice identifying the categories of personal customer information that we share with certain third parties for the third parties' direct marketing purposes, and providing contact information (i.e., names and addresses) for these third parties. If you are a California resident and would like a copy of this notice, please submit a written request to us via email at privacy-notices@onemaritimeplaza.com. We currently do not respond to "Do Not Track" or similar signals. To find out more about "Do Not Track," please visit www.allaboutdnt.com. This is distinct from our response to opt-out signals such as Global Privacy Control (aka GPC) under the California Consumer Privacy Act and other state privacy laws, which is addressed in our state-specific privacy notice below, if applicable.

International Data Transfers

We are headquartered in the United States and have service providers in other countries, and your personal information may be transferred outside of your state, province, or country to the United States or other locations where privacy laws may not be as protective as those in your state, province, or country.

Children

The Services are not directed to, and we do not knowingly collect personal information from, anyone under the age of 18. If we learn that we have collected personal information of a child without the consent of the child's parent or guardian, we will delete it. We encourage parents with concerns to contact us.

Changes to this Privacy Policy

We may amend this Privacy Policy by posting the amended version on the Services and indicating the effective date of the amended version. We may announce any material changes to this Privacy Policy through the Service and/or via email if we have your email address. In certain circumstances, we may also provide an email blast to tenant contacts and post it wherever else the new terms apply (and maybe highlight the changes in our newsletter). In all cases, your continued use of the Services after the posting of any modified Privacy Policy indicates your assent to the amended Privacy Policy.

How to Contact Us

If you have any questions or comments about this Policy or One Maritime Plaza's privacy practices, email us at privacy-notices@onemaritimeplaza.com. You may also write to us via postal mail at:

Property Manager On Site, Attn: Legal – Privacy, One Maritime Plaza, San Francisco, CA 94111

California Privacy Rights

Under California law, California residents are entitled to ask us for a notice identifying the categories of personal customer information that we share with certain third parties for marketing purposes, and providing contact information for such third parties. If you are a California resident and would like a copy of this notice, please submit a written request to us via email at privacy-notices@onemaritimeplaza.com. You must put the statement "Your California Privacy Rights" in your request and include your name, street address, city, state, and ZIP code. We are not responsible for notices that are not labeled or sent properly, or do not have complete information.

We do not collect personal information for direct marketing purposes. As a result, California's Shine Your Light law does not apply.

1. California Privacy Notice

Effective January 1, 2023

This privacy notice ("Notice") describes how PPF OFF One Maritime Plaza, LP and our corporate subsidiaries and affiliates (collectively, "One Maritime Plaza", "OMP", "we", "us" and "our") collect, use, and share personal information about California residents in and their rights with respect to that information.

1. Scope.
This Notice applies only to "personal information", as defined in the California Consumer Privacy Act of 2018 as amended including by CPRA (the "CCPA"), that we collect to the extent we qualify as a "business" as defined in the CCPA, but does not apply to personal information excluded from the scope of the CCPA. This Notice does not apply to you if you are not a California resident or you are otherwise not entitled to a notice under CCPA. In addition, this Notice does not apply to personal information covered by a different privacy notice that we give to California residents, such as the privacy notices we give to our California employees (and their beneficiaries), consultants, contractors, directors, owners, business contacts (such as on-site visitors, event attendees, contacts at partner companies), and job candidates. Sections 2-5 of this Notice describe our practices currently and during the twelve months preceding the effective date of this Notice.

2. Personal Information We Collect

(a) Categories of Personal Information: see privacy policy above.

(b) Sources of Personal Information: see privacy policy above.

3. How We Use Personal Information

See policy above. We may also use personal information for other purposes consistent with the Notice or that are explained to you at the time of collection of your personal information.

4. How We Disclose Personal Information

We may disclose for business purposes all of the categories of personal information described above with the following categories of third parties:

- **Affiliates**. Our affiliates, for purposes consistent with this Notice or to operate shared infrastructure, systems and technology.
- **Service providers**. Companies that provide us with services that help us provide services or operate our business, such as IT and software services, mailing services, marketing services, event management services, cyber security services, and office security services.
- **Government entities and law enforcement**. Government authorities, law enforcement, courts, and others as described in the compliance and protection section above.
- **Corporate transaction participants**. Parties to transactions and potential transactions for the sale, transfer or licensing of a portion or all of our business or assets, including your personal information, such as a corporate divestiture, merger, consolidation, acquisition, reorganization or sale of assets, or in the event of bankruptcy or dissolution.
- **Professional advisors**. Our lawyers, accountants, bankers, and other outside professional advisors in the course of the services they provide to us.
- **Other.** We may also share personal information with other categories of third parties with your consent or as described to you at the time of collection of your personal information.

5. Selling or Sharing Personal Information.

No Sales or Sharing. We do not “sell” or "share" your personal information as defined in the CCPA.

Categories of Personal Information Shared and Categories of Third Parties We Shared With. We do not share personal information with third parties for the purpose of cross-context behavioral advertising.

6. Minors

OMP’s services and website are not directed to children, and we don’t knowingly collect personal information from children under the age of 16; accordingly we don’t knowingly share the personal information from children under the age of 16 for cross-context behavioral advertising nor do we sell that information. If we find out that a child under 16 has given us personal information, we will take steps to delete that information. If you believe that a child under the age of 16 has given us personal information, please contact us at privacy-notices@onemaritimeplaza.com.

7. Sensitive Personal Information.

OMP does not use or disclose sensitive personal information other than to provide you the OMP Platform and as permitted by California law. OMP does not sell or share sensitive personal information for the purpose of cross-context behavioral advertising.

8. Deidentified Information.

As mentioned in our privacy policy above, personal information does not include information that is deidentified. When we receive or use deidentified information, we maintain it in deidentified form and do not attempt to reidentify the information.

9. No Financial Incentives

We do not offer financial incentives to consumers based upon the retention or sale of a consumer's personal information.

10. Retention of Personal Information.

We retain personal information as long as necessary to provide the Services. Our policy is that when a person is terminated, they become inactive in our systems. When a tenant leaves, our policy is to delete the personal data related to their employees and contractors. Our current vendor allows us to identify and request deletion of personal data in 90 days and our policy is to do that when a person becomes inactive due to their or their employer's termination. We also retain your information as necessary to comply with our legal obligations, resolve disputes, and enforce our terms and policies.

11. Exercising Your Rights

California law provides some California residents with the rights listed below. To exercise these rights see the "Exercising Your California Privacy Rights" section below**.**

Right to Know. You have the right to know and see what personal information we have collected about you, including:

- The categories of personal information we have collected about you;
- The categories of sources from which the personal information is collected;
- The business or commercial purpose for collecting or sharing your personal information;
- The categories of third parties with whom we have disclosed your personal information; and
- The specific pieces of personal information we have collected about you.

Right to Delete. You have the right to request that we delete the personal information we have collected from you (and direct our service providers to do the same).

Right to Correct. You have the right to request that we correct inaccurate personal information.

Right to Opt Out. You have the right to opt out of certain uses and sharing of personal information, including any sale of personal information, sharing of personal information for cross-contextual behavioral advertising purposes, or use of sensitive personal information for certain purposes (e.g., use or disclosure beyond what is reasonably necessary to provide the services or provide the goods reasonably expected by an average consumer).

Other Rights. You can request certain information about our disclosure of personal information to third parties for their own direct marketing purposes during the preceding calendar year. This request is free and may be

made once a year. You also have the right not to be discriminated against for exercising any of the rights listed above.

Exercising Your California Privacy Rights. To request access to or deletion of your personal information, or to exercise any other privacy rights under California law, please contact us using one of the following methods: Global Privacy Control and other automated signals: We will honor GPC opt-out signals and other mandatory automated signals that we are aware of. Currently, GPC is not applicable because we do not sell or share personal information.

Contact us at privacy-notices@onemaritimeplaza.com or via our toll-free number at 833-557-8883 to exercise your CCPA rights or by mail at Property Manager On Site, Attn: Legal – Privacy, One Maritime Plaza, San Francisco, CA 94111

Verification of Your Identity. To respond to some rights we may need to verify your request. This additional information may vary depending on the nature of your request and the nature of the information you are requesting. In some cases, we may also be required by law to obtain a signed declaration under penalty of perjury from you attesting that you are the subject of the request. If we suspect fraudulent or malicious activity on or from your account, we will delay taking action on your request until we can appropriately verify your identity and the request as authentic.

We will verify requests using a reasonable process. Our current process is to verify your request via the Host App or your work email address if you are an employee of a tenant. If you are not a holder of an account related to OMP, reasonable verification may include matching at least two data points provided by the consumer with data points maintained by us, which we have determined to be reliable for the purpose of verifying you. For example, if we have collected your ID and a mobile phone number, we may ask you to provide those as verification. The verification will depend on the nature of the personal data we have about you. If you have legal authority to request information on another's behalf, please provide a notarized power of attorney.

You may designate an authorized agent to make a request on your behalf pursuant to applicable law. We accept documentation of your designation in the form of a valid power of attorney or a notarized statement. We may require verification of your authorized agent in addition to the information for verification above for consumers and households.

Response Timing and Format. We aim to respond to a consumer request in relation to these rights within 45 days of receiving that request. If we require more time, we will inform you of the reason and extension period in writing.

Use of Verification Information. Information that you submit for the purpose of allowing us to verify your identity in furtherance of a consumer-related or household-related request pursuant to California law will only be used by us, and our service providers if any, for that purpose and no other. Except where we are required by or advisable under law to maintain this information for record-keeping purposes, we will take steps to delete any new personal information collected for the purpose of verification as soon as practical after processing your request.

Exceptions. Please also be aware that making a request does not ensure complete or comprehensive removal or deletion of Personal Information or content you may have posted, and in some circumstances the law does not

require or allow us to fulfill your request. This may occur where fulfilling your request may infringe upon the rights and freedoms of other consumers.

Request Fees. We reserve the right to charge a reasonable fee or take other appropriate action in response to requests from a consumer or household that are manifestly unfounded or excessive, in particular because of their repetitive character.