PFP Cybersecurity Inc Privacy Policy

PFP Cybersecurity ("PFP") takes your privacy seriously and is committed to protecting your privacy rights. We want you to know why we collect your personal information, what we collect, how we use it, and for how long we store it. We also want you to know how you can access, amend, correct, and in some cases delete your information.

Who we are

PFP is a small cybersecurity firm located in the Washington DC metro area. We provide a unique cybersecurity solution based on side channel analysis of electrical output and power consumption.

Why we collect information

- We collect personal information when you request our content marketing assets, in order to provide useful content and follow up on its effectiveness for marketing purposes.
- We collect information when you contact us to respond to your request, question, or issue, and to follow up on the resolution.
- We collect information when you buy and/or use our software or services. We do this to be able to deliver our services, to send you important operational information, for contractual reasons, to process financial transactions, and for legal and regulatory reasons.
- If you are an PFP partner, we collect information to enable you to resell and provide services around our software and services, and to fulfill our contractual obligations to you as a partner.

What we collect

- Most often, we collect name, email, phone, address, job title, company.
- If you are an PFP customer, we may collect which products and services you use.
- If you sign a contract with PFP, we may collect further details such as your signature or other proof of identity, the IP address (if signing a contract digitally).
- We may collect other data you have provided while contacting us, especially using the contact, download, or signup forms on our website.
- We collect data that you have provided to us through event attendance application, support ticket, or job application.
- We collect anonymous information sent by your browser when you visit our websites, including IP address, operating system, and browser version. If you identify yourself by filling out a form, some data (such as what pages you view on our websites) will be connected to your personal information.
- **Information we and partners collect when you browse our website**

- On our websites, we include a number of scripts from third-party vendors. These scripts may gather data for web statistics, they may be used for interest-based advertising on other services (such as Google, Facebook, or LinkedIn), and they may offer additional functionality to the web sites (such as chat).
  - The websites and third-party scripts may use cookies or local storage. Cookies and local storage can be used to identify a returning visitor. Cookies and local storage in themselves to not identify you as an individual – but if you for instance are using Facebook, and subsequently visit our websites, Facebook may learn about your visit.
  - **We cannot tell who you are unless you willingly identify yourself on our websites.**
  - If you at some point have identified yourself by filling out a form on our websites, pages you view on our websites may be connected to your personal information. We do this to understand the effectiveness of our website.

  - For certain parts of our websites, for instance pages that require a login, cookies are required for the website to work properly. Otherwise, cookies are generally not required for the operation of the website. - We set a cookie and use local storage in your browser that contains information that we use to identify you between visits. In particular, we set an identifier that identifies you for the functional site features described below:

    - Google Analytics: We use Google Analytics to analyze the performance of our websites and follow up on the effectiveness of on marketing efforts. Google Analytics allow us to analyze data in aggregate, we do not collect or store any personal information in Google Analytics. Read Google's privacy policy here.
    - Hotjar Analytics: We use Hotjar Analytics to evaluate your experience with our website, specifically for the purpose of revamping the site. Hotjar is a technology service that helps us better understand our users experience (e.g. how much time they spend on which pages, which links they choose to click, what users do and don't like, etc.) and this enables us to build and maintain our site with user feedback. Hotjar uses cookies and other technologies to collect data on our users' behavior and their devices (in particular device's IP address (captured and stored only in anonymized form), device screen size, device type (unique device identifiers), browser information, geographic location (country only), preferred language used to display our website). Hotjar stores this information in a pseudonymized user profile. Neither Hotjar nor we will ever use this information to identify individual users or to match it with further data on an individual user. For further details, please see Hotjar's privacy policy by clicking on this link.

- You can opt-out to the creation of a user profile, Hotjar's storing of data about your usage of our site and Hotjar's use of tracking cookies on other websites by following this opt-out link.
- Leadfeeder: We use Leadfeeder to find out the names of companies visit our websites and what pages visitors from those companies have viewed. Leadfeeder does not collect any personal information on our websites, but you may have provided them with information on other websites that also use Leadfeeder, and that information may then be connected to your visit on our websites. Read Leadfeeder's privacy policy here.

- **Information we collect when you fill out a form on our websites** ○ When you submit a form on our websites, we collect the information that is listed in the form – typically your name, email address, company name, phone number, and survey questions about the nature of your company.
  - By submitting a form on our websites, you confirm that you have you have read and accept this privacy policy, and that you understand that data will be collected and processed for the purposes outlined in this policy. ○ If you have filled out a form on our websites, we may collect the URLs of any pages viewed or links clicked on our websites and connect them to your profile. We do this to better understand your needs.
  - If you open or click a link in an email we have sent you in response to you filling out a form, including email newsletter, that information will be connected to your profile. We may do this to either verify your email address to prevent spam and misuse, or to follow up on the usefulness of our email marketing.
- **Information we collect when you register with us at a trade show or industry event** ○ If you meet us at a trade show or industry event, you may leave your contact details in order for us to follow up with you, to enter a competition or a game, or to subscribe to our newsletter. We will collect the information that is available by using a badge scanner or other electronic device. ○ Please note that when you register for an industry event, you might have consented to sharing your personal information with us when signing up for the event.

How we use information

- **We never sell or rent your personal information to third parties.** If you are an individual based in the EU individual and have given us your express permission, we may share your personal information to select partners that you decide. If you are an individual not based in the EU, we may share your personal information to select partners that are clearly labelled when you sign up. We always make clear when we share that information – as an example when we provide an event or an asset in collaboration with a partner of ours.
- If you have requested a marketing asset or have participated in a marketing event, we use your personal information to follow up on the effectiveness of the marketing activity.

- If you are an individual based in the EU and you have registered to access one of our content marketing assets or a webinar, me may use your address to send you marketing communications. If you are an individual not based in the EU and you have registered to access one of our content marketing assets or a webinar, me may use your address to send you marketing communications.
- If you are a customer or a partner of ours, we may use your contact information to send you product or services updates and information that is relevant to your use of the products and services.
- Your information may be processed by vendors that act on our behalf, such as services we use to maintain our contact records, provide webinar services, or provide back office services such as email. These vendors are under a data processing agreement with us, act on our instructions and adhere to the policies described in this document.
- **Protection of your information**
  - We take care to protect your personal data against abuse or loss. As an example, we store it in secure environments. We also provide training to our employees on data protection best practices and require them to enter into a confidentiality agreement.
  - We cannot guarantee absolute security though. If you would like to learn more about what we do to protect your data, please contact us at compliance@pfpcyber.com.
- **Information shared with vendors and service providers**
  - In order to deliver our services, we rely on a number of different vendors. This covers everything from the software we use in our finance department to the infrastructure we use to run P2Scan and other services. These vendors act as data processors on our behalf.
  - We hold our vendors and service providers to the same high privacy standards as we hold ourselves to. In all cases where we share your information with anyone outside of PFP, we explicitly require them to acknowledge and adhere to our privacy and customer data handling policies through a data processing agreement.

How long we keep information

- We keep your information only for as long as it is warranted from to fulfill our commitments to you, or to adhere to legal or regulatory requirements.
- If you are a customer or partner, we keep the information for the duration of our relationship. Certain information may be kept for longer though, for instance contracts will be archived even when terminated.
- If you have requested to receive marketing communications, we will keep your personal information only for as long as you interact with us.
- In most cases, we keep your personal information for no more than 12 months after the last contact or when your contract has expired, with the exception of information we have to keep for legal reasons, such as signed contracts.
- **If you are an PFP customer or partner**
  - If you are an PFP customer or partner, we may keep your personal information for the duration of our contract between your

organization and us. If not required by law or regulation to keep your information beyond that term, we will remove it within 12 months of the contract ending.
    - If you have signed or entered into a contract with us, we typically archive and store that contract for an extended period of time, typically seven years or longer, depending on jurisdiction. Other items such as invoices may also be kept for longer than 12 months. ○ If you have asked to receive marketing communications from us, we will keep your personal information to maintain your subscription, even if you would no longer be a customer or partner of ours.
- **If you are not an PFP customer or partner** ○ If you have downloaded any of our online marketing materials, your personal information will be kept for us long as you seem to be an active subscriber.
    - If we haven't seen any activity on your part for 12 months, we will remove your personal information or anonymize it. ○ If you have been in touch with us with a question, demo request, asked for a quote, or have engaged with a sales representative, your information will be stored for up to 12 months after the last recorded activity, and will then be removed or anonymized. ○ If you have submitted a valid GDPR data subject access request to exercise your right to be forgotten we will delete your data within 30 days of the request.

P2Scan and other products and services

- We provide software and services to our customers. This software and these services allows our customers to continually monitor systems and devices against tampering, intrusion, counterfeiting and other nefarious activity.
- **Information processed in P2Scan and other products and services** ○ Our customers use P2Scan to continually monitor systems and devices against tampering, intrusion, counterfeiting and other nefarious activity.
    - Information that is collected using our services on behalf of our customers belongs to them and is used, disclosed and protected by them according to their privacy policies and is not subject to this Privacy Policy.

Your choices and rights

- You can choose to opt out of marketing communications at any time, regardless if you are a customer, partner, or none of the above.
- If you are an individual based in the EU you can request a copy of your personal information and you can update any incorrect information.
- If you are an individual based in the EU, you can ask to have your personal information removed, or in some cases limit our processing of personal information. This does not apply when we need to keep your information for legal reasons.
- **How you can opt out of marketing** ○ If you don't want to receive marketing communications from us, you can at any time use the "Unsubscribe" link present in all

marketing emails from us or go to our unsubscribe page. ○ Please note that opting out of email marketing typically doesn't mean that you won't see ads from us – please see the section below on how you can opt out of web tracking, although it doesn't mean that you will opt out of ads altogether.

- **How you can opt out of web tracking** ○ There are several ways to opt out of web tracking:
    - ✦ Most browsers allow you to block third-party cookies or prevent crossdomain tracking. This will limit the cookies that can be set by thirdparty scripts. This will not completely eliminate tracking by some thirdparty services though as they may use first-party cookies.
    - ✦ Most browsers also allow you ask not to be tracked (it sends the "Do Not Track" request header). If you have enabled this feature, we will not track the pages you visit in a way that enables us to connect them to your personal information. Your page views may still be collected anonymously though. Many of the third-party services we use for collecting anonymous data also respect the Do Not Track setting.
    - ✦ Google Analytics: You can use Google's opt-out browser add-on to prevent tracking in Google Analytics, see https://tools.google.com/dlpage/gaoptout.
- **Your rights as an individual based in the EU** ○ Access to your information: You have the right to request a copy of the personal information we hold about you. ○ Correcting your information: We want to have accurate data. Please contact us if you think the data we hold is not up to date or correct. ○ Deletion of your information: You have the right to ask us to delete Personal Data about you if it no longer is required for the purpose it was collected, you have withdrawn your consent, you have a valid objection to us using your Personal Data, or our use of your Personal Data is contrary to law or our other legal obligations.
    - ○ Objecting to how we may use your information: You have the right at any time to require us to stop using your Personal Data for direct marketing purposes. In addition, where we use your Personal Data to perform tasks carried out in the public interest then, if you ask us to, we will stop using that Personal Data unless there are overriding legitimate grounds to continue. ○ Restricting how we may use your information: In some cases, you may ask us to restrict how we use your Personal Data. This right might apply, for example, where we are checking the accuracy of Personal Data about you that we hold or assessing the validity of any objection you have made to our use of your information. The right might also apply where this is no longer a basis for using your Personal Data but you don't want us to delete the data. Where this right to validly exercised, we may only use the relevant Personal Data with your consent, for legal claims or where there are other public interest grounds to do so. ○ Automated processing: If we use your Personal Data on an automated basis to make decisions which significantly affect you, you have the right to ask that the decision be reviewed by an individual to whom you may make

representations and contest the decision. This right only applies where we use your information with your consent or as part of a contractual relationship with you
    - Withdrawing consent using your information: Where we use your Personal Data with your consent you may withdraw that consent at any time and we will stop using your Personal Data for the purpose(s) for which consent was given. ○ Please contact if you wish to exercise any of these rights. You can find the contact details below.
- **If you want to submit a complaint** ○ We have appointed a Data Protection Officer. If you are a European Union ("EU") resident who requires assistance in exercising your privacy rights, please write to Data Protection Officer at dpo@pfpcyber.com.

Children's Privacy

PFP encourages parents and guardians to take an active role in their children's online activities. PFP does not knowingly collect personal information from children without appropriate parental or guardian consent. If you believe that we may have collected personal information from someone under the applicable age of consent in your country without proper consent, please let us know using the methods described in the Contact Us section and we will take appropriate measures to investigate and address the issue promptly.

How to contact us

- Send email to: compliance@Pfpcyber.com.
- You can contact our Data Protection Officer at dpo@Pfpcyber.com.
- You can write to:

  PFP Cybersecurity c/o Legal
  Department 1577 Spring Hill
  Rd, Suite 405 Vienna, VA
  22182

Individuals not based in the EU

The following terms apply, in addition to the privacy policy described above:

- COMPELLED DISCLOSURE: PFP may be required to disclose Personal Data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.
- DISPUTE RESOLUTION: Any questions or concerns regarding the use or disclosure of Personal Data should be directed to the notices address specified in Contact Information below. PFP will investigate and attempt to resolve complaints and disputes regarding use and disclosure of Personal Data in accordance with the principles contained in this Policy. For complaints that cannot be resolved between PFP and the complainant, PFP has agreed to participate in the dispute resolution procedures of the panel established by the

European data protection authorities to resolve disputes pursuant to the Privacy Shield Principles. Under certain conditions, as more fully described on the Privacy Shield website https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint, individuals may be able to invoke binding arbitration before the Privacy Shield Panel jointly created by the U.S. Department of Commerce and the European Commission. • YOUR CALIFORNIA PRIVACY RIGHTS: California's "Shine the Light" law permits customers in California to request certain details about how certain types of their information are shared with third parties and, in some cases, affiliates, for those third parties' and affiliates. Under the law, a business should either provide California customers certain information upon request or permit California customers to opt in to, or opt out of, this type of sharing.

- PFP may share Personal Data as defined by California's "Shine the Light" law with third parties and/or affiliates for such third parties' and affiliates. If you are a California resident and wish to obtain information about our compliance with this law, please e-mail or write to us at the addresses specified in "Contact Information" below. Requests must include "California Privacy Rights Request" in the first line of the description and include your name, street address, city, state, and ZIP code. Please note that PFP is not required to respond to requests made by means other than through the provided e-mail address or mail address.
- ENFORCEMENT AND COMPLIANCE: PFP will conduct compliance audits of its relevant privacy practices to verify adherence to this Policy. Any employee that PFP determines is in violation of this policy will be subject to disciplinary action up to and including termination of employment. PFP will respond promptly to inquiries and requests by the Department of Commerce for information relating to the Privacy Shield and/or to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. PFP is subject to the investigatory and enforcement powers of the Federal Trade Commission with respect to its compliance with the EU-U.S. Privacy Shield Framework. If PFP becomes subject to an FTC or court order based on non-compliance, PFP will make public any relevant Privacy Shieldrelated sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. PFP may be required to disclose Personal Data in response to a lawful request by public authorities, including to meet national security or law enforcement requests.
- ONWARD TRANSFER: If a third-party processes Personal Data on behalf of PFP in a manner inconsistent with the General Data Protection Regulation and applicable law, PFP could be liable unless PFP can prove that it is not responsible for the event giving rise to any damage. If PFP transfers data to a third party agent, PFP will: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the Personal Data transferred in a manner consistent with PFP's obligations under the Principles; (iv) require the agent to notify PFP if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to

stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department of Commerce upon request.

Changes to this privacy policy

- We keep this privacy policy under regular review and will place any updates on this website.
- The privacy policy was last updated May 24, 2018.

Revision history of this privacy policy:

Version	Date	Summary of Changes
1.0	May 24, 2018	Effective Date of Notice