IPS Data Privacy Policy

for

Employees, Suppliers, and Contractors

Innovative Project Solutions, Inc.
50 California Street 15th Floor, San Francisco, CA 94111

Table of Contents

Introduction

Innovative Project Solutions Inc (IPS) has always had an absolute determination to do the right thing. In all of its dealings, IPS is committed to unyielding integrity and the highest standard of business conduct. This commitment is integral to IPS's continued success, and we believe it positively impacts our diverse and worldwide suppliers, contractors, customers, employees, and investors, and the communities where we do business.

At IPS, Inc. , d/b/a IPS Design Build ("us", "we", "our" or the "Company") we value your privacy and the importance of safeguarding your data. This Privacy Policy (the "Policy") describes our privacy practices for the activities set out below. As per your rights, we inform you how we collect, store, access, and otherwise process information relating to individuals. In this Policy, personal data ("Personal Data") refers to any information that on its own, or in combination with other available information, can identify an individual. This policy sets out the rules that we will follow when processing your personal information to preserve the right to protect your personal data, your privacy, and to ensure that your personal data is not misused. We will follow this policy for the entire period during which we process any of your personal information.

Your personal information is stored in the United States. We control the personal information of those with whom we have directly interact. Examples of this are users who applies for employment or fill out a form on our website. We do NOT maintain or share personal information for other controller organizations.

IPS is committed to protecting your personal information from any attacks or data breaches. We have implemented appropriate security controls throughout our business systems. In the unlikely event of data breach, we will honor the EU's GDPR requirements for notification.

Reasons for collecting personal data

We will only collect and process personal data from you if it is necessary for:

1. Fulfilling the contract that you have signed or closed with us.
2. Personal data you provide on our career website
3. Employment application with IPS
4. Compliance with the requirements of the law.

We are committed to protecting your privacy in accordance with the highest level of privacy regulation. As such, we follow the obligations under the below regulations:

- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the applicable provincial legislations
- EU's General Data Protection Regulation (GDPR)
- California's Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA) and California Online Privacy Protection Act (CalOPPA)
- Colorado Privacy Act (CPA)
- Utah Consumer Privacy Act (UCPA)
- Connecticut Data Privacy Act (CTDPA)
- Virginia Consumer Data Protection Act (VCDPA)

Scope

This policy applies to the IPS, Inc. websites, employment applications, and master services agreements.

This Policy does not apply to third-party applications, websites, products, services or platforms that may be

accessed through (non-) links that we may provide to you. These sites are owned and operated independently from us, and they have their own separate privacy and data collection practices. Any Personal Data that you provide to these websites will be governed by the third-party's own privacy policy. We cannot accept liability for the actions or policies of these independent sites, and we are not responsible for the content or privacy practices of such sites.

IPS headquarters is located in San Francisco, California. Any demand by a government for disclosure of data is carefully reviewed by our lawyers. We will not do so until it is proven that a current law that affects us clearly requires to do so. And even if this hypothetically situations arises, we well point out that we do not have any personal user data that we could provide

What Personal Data We Collect

We collect the following types of Personal Data:

This includes:

- Account Information such as company name, your name, email address
- Social security number (only employees)
- Driver license or passport (only employees)
- Name and signatures
- Government Identification documents
- Home address (only employees)
- Mobile device phone number
- Location Data of your company address
- Business Certifications
- Company Financial Information. Financial Information including credit card numbers or banking account details
- Mobile device phone number
- Health insurance information
- Education information
- Employment information: employment history, employee number, performance appraisals, salary and benefits, healthcare information, emergency contact information.
- Protected class information: Age, race, color, national origin, citizenship, religion or creed, marital status, disability information, sex, genetic information, military or veteran status.

How We Collect Your company and Personal Data

We collect company and Personal Data from the following sources:

- Applying for job application
- Create an account on our website;
- Master Service Agreement with IPS to use your services

Third parties: We may receive Personal Data about you and your company from various third parties, including:

- Account Information and Payment Data from third parties, including organizations (such as law enforcement agencies), associations and groups, who share data for the purposes of fraud prevention and detection and credit risk reduction;

Purpose and Legal Basis for the Processing of Personal Data

We collect and use your Personal Data with your consent to provide services and maintain your employment.

These purposes include:

- To deliver your product or service
- Building a Safe and Secure Environment
- To verify or authenticate your identity;
- Investigate and prevent security incidents such as breaches, attacks and hacks
- Enable you to access IPS, Inc. services and set up accounts.
- Provide you with technical and customer support
- Fulfilling a legal or contractual obligation
- Managing employee relationships, including the administration of benefits.
- Processing job applications, including background investigations.

International Data Transfer and Storage

Your Personal Data may also be transferred to, and maintained on, servers residing outside of your state, province, country or other governmental jurisdiction where the data laws may differ from those in your jurisdiction. We will take appropriate steps to ensure that your Personal Data is treated securely and in accordance with this Policy as well as applicable data protection law. Data may be kept in other countries that are considered adequate under your laws. More information about these clauses can be found here. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32021D0914

Data Integrity and Purpose Limitation

IPS collects and processes personal information only to the extent that it is compatible with the purposes for which it was collected or subsequently authorized by the data subject. IPS does not retain personal information after it no longer serves the purposes for which it was collected or subsequently authorized. IPS takes reasonable steps to ensure that personal information is accurate, complete, current, and reliable for its intended use.

EU-US Data Privacy Framework

Innovative Project Solutions inc. complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) as set forth by the U.S. Department of Commerce. Innovative Project Solutions inc has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/

In compliance with the EU-U.S. DPF Innovative Project Solutions Inc. commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF to USCIB, an alternative dispute resolution provider based in the United States and the European Union. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit Data Protection Authorities (dataprivacyframework.gov)for more information or to file a complaint. The services of DPF of alternative dispute resolution provider are provided at no cost to you.

- Individuals have the right of individuals to access their personal data
- Individuals have the choices and means your organization offers individuals for limiting the use and disclosure of their personal data
- Individuals have the right to organization being subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC)
- Individuals have the possibility, under certain conditions, for the individual to invoke binding arbitration

    - Note: Your organization is obligated to arbitrate claims and follow the terms as set forth in Annex I of the DPF Principles, provided that an individual has invoked binding arbitration by delivering notice to your organization and following the procedures and subject to conditions set forth in Annex I of Principles.
- Individuals have the possibility, under certain conditions, for the individual to invoke binding arbitration
    - Note: Your organization is obligated to arbitrate claims and follow the terms as set forth in Annex I of the DPF Principles, provided that an individual has invoked binding arbitration by delivering notice to your organization and following the procedures and subject to conditions set forth in Annex I of Principles.
- IPS is liable in cases of onward transfers to third parties

Asia-Pacific Economic Cooperation Cross-Border Privacy Rules System And Privacy Recognition For Processors.

IPS's privacy practices, described in this Privacy Policy, comply with the Asia-Pacific Economic Cooperation ("APEC") Cross Border Privacy Rules ("CBPR") system and the Privacy Recognition for Processors ("PRP"). The APEC CBPR system provides a framework for organizations to ensure protection of personal data transferred among participating APEC economies and the PRP demonstrates an organization's ability to provide effective implementation of a personal data controller's privacy obligations related to the processing of personal information. More information about the APEC framework can be found here (https://cbprs.blob.core.windows.net/files/CBPR%20Policies,%20Rules%20and%20Guidelines%20Revised%20For%20Posting%203-16.pdf) If you have an unresolved privacy or data use concern related to our APEC CBPR or PRP certifications that we have not addressed satisfactorily.

Your California Privacy Rights

This section provides additional details about the personal information we collect about California consumers and the rights afforded to them under the California Consumer Privacy Act or "CCPA," as amended by the California Privacy Rights Act or "CPRA".

California law requires that we detail the categories of personal information that we collect and disclose for certain "business purposes," such as to service providers that assist us with securing our services or marketing our products, and to such other entities as described in earlier sections of Privacy Policy. In addition to the information provided above in the 'Information We Collect And Receive' section, we collect the following categories of personal information from you, your employer, data analytics providers, data brokers, and Third-Party Services for our business purposes:

- Identifiers/contact information;
- Commercial information;
- Internet or electronic network activity information;
- Financial information;
- Geolocation information;
- Professional or employment-related information;
- Audio and visual data;
- In limited circumstances where allowed by law, information that may be protected under California or United States law; and
- Inferences drawn from any of the above categories.

IPS does not sell (as such term is defined in the CCPA or otherwise) the personal information we collect (and will not sell it without providing a right to opt out). We may also share personal information (in the form of identifiers and internet activity information) with third party advertisers for purposes of targeting advertisements on non-IPS

websites, applications, and services. In addition, we may allow third parties to collect personal information from our sites or services if those third parties are authorized service providers who have agreed to our contractual limitations as to their retention, use, and disclosure of such personal information, or if you use our sites or services to interact with third parties or direct us to disclose your personal information to third parties.

Subject to certain limitations, the CCPA provides California consumers the right to request to know more details about the categories or specific pieces of personal information we collect (including how we use, disclose, or may sell this information), to delete their personal information, to opt out of any "sales", to know and opt out of sharing of personal information for delivering advertisements on non-IPS websites, and to not be discriminated against for exercising these rights.

California consumers may make a request pursuant to their rights under the CCPA by contacting us at info@ipsinc.net . We will verify your request using the information associated with your account, including email address. Government identification may be required. Consumers can also designate an authorized agent to exercise these rights on their behalf. Authorized agents must submit proof of authorization.

If you would like to opt-out of sharing activity based on your cookie identifiers, turn on a Global Privacy Control in your web browser or browser extension. Please see the California Privacy Protection Agency's website at https://oag.ca.gov/privacy/ccpa for more information on valid Global Privacy Controls. If you would like to opt-out of sharing activity based on other identifiers (like email address or phone number), contact us in accordance with the "Contacting IPS" section, below.

For more information on IPS's role and obligations under the CCPA, please visit IPS's California Consumer Privacy Act (CCPA) FAQ.

Data Protection Authority

Subject to applicable law, you also have the right to (i) restrict IPS's use of Other Information that constitutes your Personal Data and (ii) lodge a complaint with your local data protection authority. If, however, you believe that we have not been able to assist with your complaint or concern, and you are located in the European Economic Area, you have the right to lodge a complaint with the competent supervisory authority. If you work or reside in a country that is a member of the European Union, you may find the contact details for your appropriate data protection authority on the following website (https://edpb.europa.eu/about-edpb/about-edpb/members_en).

Legal Requirement

We may use or disclose your Personal Data in order to comply with a legal obligation, in connection with a request from a public or government authority, or in connection with court or tribunal proceedings, to prevent loss of life or injury, or to protect our rights or property. Where possible and practical to do so, we will tell you in advance of such disclosure.

How We Keep Your Data Safe

We have appropriate organizational safeguards and security measures in place to protect your Personal Data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed.

The communication between you and our website uses a secure encrypted connection wherever your Personal Data is involved.

We require any third party who is contracted to process your Personal Data on our behalf to have security measures in place to protect your data and to treat such data in accordance with the law.

In the unfortunate event of a Personal Data breach, we will notify you and any applicable regulator when we

are legally required to do so.

Your Rights for Your Personal Data

Depending on your geographical location and citizenship, your rights are subject to local data privacy regulations. These rights may include:

- Right to Access (PIPEDA, GDPR Article 15, CCPA/CPRA, CPA, VCDPA, CTDPA, UCPA, LGPD, POPIA)
- You have the right to learn whether we are processing your Personal Data and to request a copy of the Personal Data we are processing about you.
- Right to Rectification (PIPEDA, GDPR Article 16, CPRA, CPA, VCDPA, CTDPA, LGPD, POPIA)
- Right to be Forgotten (right to erasure) (GDPR Article 17, CCPA/CPRA, CPA, VCDPA, CTDPA, UCPA, LGPD, POPIA)
- You have the right to request that we delete Personal Data that we process about you, unless we need to retain such data in order to comply with a legal obligation or to establish, exercise or defend legal claims.
- Right to Restriction of Processing (GDPR Article 18, LGPD)
- You have the right to restrict our processing of your Personal Data under certain circumstances. In this case, we will not process your Data for any purpose other than storing it.
- Right to Portability (PIPEDA, GDPR Article 20, LGPD)
- You have the right to obtain Personal Data we hold about you
- Right to Objection (GDPR Article 21, LGPD, POPIA)
- Where the legal justification for our processing of your Personal Data is our legitimate interest, you have the right to object to such processing on grounds relating to your particular situation. We will abide by your request unless we have compelling legitimate grounds for processing which override your interests and rights, or if we need to continue to process the Personal Data for the establishment, exercise or defense of a legal claim.
- Nondiscrimination and nonretaliation (CCPA/CPRA, CPA, VCDPA, CTDPA, UCPA)
- File an Appeal (CPA, VCDPA, CTDPA)
- You have the right to file an appeal based on our response to you exercising any of these rights. In the event you disagree with how we resolved the appeal, you have the right to contact the attorney general located here:

File a Complaint (GDPR Article 77, LGPD, POPIA)

- You have the right to bring a claim before their competent data protection authority. If you are based in the EEA, please visit this website (http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=50061) for a list of local data protection authorities.

Withdrawing Consent

If you have consented to our processing of your Personal Data, you have the right to withdraw your consent at any time, free of charge, such as where you wish to opt out from marketing messages that you receive from us. If you wish to withdraw your consent, please contact us using the information found at the bottom of this page.

How to Exercise Your Rights

You can make a request to exercise any of these rights in relation to your Personal Data by sending the request to our privacy team by using the form below.

For your own privacy and security, at our discretion, we may require you to prove your identity before providing the requested information.

Storage
The security measures IPS uses vary based on the sensitivity of the personal information we collect, process, and store, and the current state of technology. We also take measures to ensure service providers that process personal data on our behalf also have appropriate security measures.

Retention
IPS retains Personal Data only as long as necessary to fulfill the purposes outlined in this Privacy Policy, unless a longer retention period is required or not prohibited by law.

If you have consented to the processing of your Personal Data, IPS will retain and process your Personal Data until you withdraw your consent ("opt-out"), unless the Personal Data must be kept for administrative, legal, or regulatory purposes.

If IPS has not received your opt-in, IPS will delete your Personal Data once the purpose of the collection and processing of such Personal Data has been fulfilled and the adequate duration for documentation and backup storage of such Personal Data has lapsed.

Self-assessment and staff training
IPS self-asses our privacy policies. IPS Information Security Professionals are required to update our credentials regularly. Any new information regarding information security is embedded in the questions, staff training modules, action plan, and policy changes they recommend. An annual self-assessment and staff training is not only recommended by law, but also beneficial to our company. Hackers have a way of exploiting the smallest loopholes in a company's data architecture. This can be avoided by regularly analyzing if all systems are complying with the best practices and seeking help to explore additional security options to fortify a IPS's defenses.

Changes
We may modify this Policy at any time. If we make changes to this Policy then we will post an updated version of this Policy at this website. When using our services, you will be asked to review and accept our Privacy Policy. In this manner, we may record your acceptance and notify you of any future changes to this Policy.

Enforcement
In compliance with the Principles, PwC commits to resolve complaints about our collection or use of your personal information. Individuals with inquiries or complaints regarding our Privacy Shield Policy should first contact IPS at HR@IPSINC.NET has a policy of responding to individuals within forty-five (45) days of an inquiry or complaint. the International Centre for Dispute Resolution/American Arbitration Association ("ICDR/AAA"). Please contact or visit ICDR/AAA for more information or to file a complaint. If the dispute involved human resources personal information, or information collected in the context of an employment relationship, we will cooperate with the competent EU data protection authorities and comply with the advice of such authorities.

You may have the option to select binding arbitration under the Privacy Shield Panel for the resolution of your complaint under certain circumstances. For further information, please see the Privacy Shield website. To learn more about the Privacy Shield Framework, and to view IPS's certification, please visit https://www.privacyshield.gov.

How to Submit a Data Subject Rights Request:
You may exercise your data subject rights using any of the following methods:

Emailing hr@ipsinc.net

Calling our office number at 1-510-289-0067

Mailing the request to the Privacy Officer at

50 California St 15th Fl
San Francisco CA 94111

We will verify your identity prior to completing these requests. Please provide sufficient information in your request for us to be able to reasonably locate our records about you and what actions you are requesting we take with regards to your data.

How we will respond to your data subject rights request

IPS will respond as described below:

IPS will deliver the required information within 45 days of a verifiable request, and you will receive notification if IPS will need an additional 30 days to respond.

IPS will provide response to requests for access to data in a written, readily usable format for data portability and free of charge to the consumer after Turner receives a valid request.

You will receive your requested information either by your account, electronically, or via mail.

Turner will not provide you with specific pieces of personal information if the disclosure would create a substantial, articulable, and reasonable risk to the security of the personal information, your account with the business, or the security of Turner's systems or networks.

Turner will notify you when data has been deleted.

There may be circumstances where Turner must deny your verified request because of a conflict with state law, federal law, or an exception to applicable privacy laws. If Turner must deny a request accordingly, you will be informed and given the basis for the denial. If the request is denied only in part, Turner will disclose the other information sought by you.

[END OF DOCUMENT]