



Date: 1 September 2022

Global Contingent Worker Privacy Notice

This Global Contingent Worker Privacy Notice (“**Notice**”) explains how Honeywell International Inc. and its subsidiaries and affiliates (together “**Honeywell**,” “**we**,” or “**us**”) collects, uses, shares and transfers personal information relating to contingent workers regardless of status. We are your data controller for the purposes of applicable data protection laws.

It is important that you read this Notice together with the Data Privacy Policy For Contingent Workers at <https://sharepoint.honeywell.com/sites/PolicyManual/GPPS/GPPSHome.html> and any other privacy statements we may provide to you so that you are aware of how we process your personal information and your data protection rights.

Overview of our Privacy Practices

Personal Information We Collect	We collect personal information directly from you or indirectly from third parties such as our partners, service providers and social media sites. For more information about the types and sources of information we collection about use, please see “ Personal Information We Collect ”
How we Process Your Personal Information	We use your personal information to fulfil the contractual relationship. For more information about how we use your personal information, please see “ Why we Process Your Personal Information ”
The Legal Bases for Processing Your Personal Information	For more information about the legal bases we use for processing your personal information, please see “ The Legal Bases for Processing Your Personal Information ”
Who We Share Your Personal Information With	We share your personal information within Honeywell only with (i) those who access in order to perform their tasks and duties, and (ii) with authorised third parties who have a legitimate business purpose. For more information on who we share your personal information with, please read “ Who We Share Your Personal Information With ”
Transfers of Personal Information	We may transfer your personal information to our affiliates and authorised third parties around the world. For more information on international transfers, please refer to “ Transfers of Personal Information ”
Retention	For more information on how long we retain your personal information, please see the “ Retention ” section below.
Workplace Monitoring	We conduct workplace monitoring activities. For more information on Honeywell’s workplace monitoring activities, please refer to “ Workplace Monitoring ” below.



Your Data Protection Rights	You may exercise any applicable rights you may have under applicable law by sending an email to. For more information refer to " Your Data Protection Rights "
Automated Processing and Profiling	We may conduct automated processing and profiling activities. For more information on our automated processing and profiling activities please see " Automated Processing and Profiling "
Contact Us	If you have any questions or complaints about how your personal information is processed or wish to exercise your rights, please send an email to HoneywellPrivacy@honeywell.com
Our use of cookies and other similar tracking technologies	We may automatically collect certain information from you using "cookies" and other similar tracking technologies when you visit our websites, platforms or use our office applications. For more information, please read Honeywell's Cookie Notice at https://www.honeywell.com/us/en/cookie-notice#language3/

Personal Information We Collect

(i) *Personal Information*

We will collect and use your personal information directly from you or indirectly from our recruitment agency, partners and service providers ("**Suppliers**") as part of your working relationship or when you are selected to provide contracted work. This includes information in resumes, applications, information collected in connection with the onboarding process and as part of your working relationship. The types of personal information we collect, and process, may include:

- **Name, identity and contact details** such as your name, Honeywell identification number, date of birth, nationality, citizenship, gender, personal and business email address, and telephone numbers;
- **Work details** such as your job title, role, date of hire, office location, work permit status, working hours, attendance records, vacation and other leave of absence records, performance evaluations and ratings, resignation or termination information, disciplinary records, grievances or other internal complaint procedures, and location preferences;
- **Background and hiring information** such as your educational history, academic and professional qualifications, resume, job history, hiring references, interview notes and assessments;
- **Emergency contact information** of individuals whose information you have provided;
- **Your image and/or voice** which may be captured through photo identification badges, key card systems, security cameras, photographs, video recordings, audio recordings or similar media;
- **IT information** such as information required to provide access to or captured by your use of Honeywell's IT systems, networks and authorized devices such as internet browsing history, phone



numbers dialed, IP addresses, device identifiers, log files, login information, authentication information, software and hardware inventories, documents and files stored on Honeywell's systems or networks (including computer desktops), and emails transmitted from and received on Honeywell's email accounts. For more information about how we process IT information, see our "**Workplace Monitoring**" section below;

- **Workplace investigations information** about a work or business-related incident that has occurred inside or outside our offices and may include information obtained from witnesses, law enforcement, or public sources (for example, news sources);
- **Publicly available information** about you from sources such as social media sites (for example, LinkedIn), registries of company information, bankruptcy registries, financial, and tax registries; and
- **Other information you choose to share with us** such as your hobbies, personal, and social preferences.

(ii) Sensitive Personal Information We Collect

Some of the personal information we collect about you may be considered "Sensitive" under applicable laws. We will collect Sensitive personal information from you where we have a legal obligation to do so or with your explicit consent. The types of Sensitive personal information we process may include:

- **Identity and Immigration Information** such as national identity card, passport, details of residency and work permit for purposes of verifying your legal ability to work and to maintain your employment with Honeywell;
- **Demographic data** such as your gender, race, ethnicity, sexual orientation, disability, religious or philosophical belief for purposes of Honeywell's Inclusion and Diversity initiatives;
- **Health information** (for example, to accommodate a disability or dietary);
- **Biometric information** such as your fingerprint, voiceprint or scan of your hand or face geometry (for example, for authentication purposes when using work-related devices and/or systems);
- **Criminal offenses or convictions** for background check purposes to determine your suitability for an open position or opportunity at Honeywell where this is permitted by applicable law.

Any request by Honeywell for your Sensitive personal information will generally be accompanied by a statement of the business justification for the request and explanation about our use of the information. We will normally seek your express permission first unless there are compelling and lawful reasons not to do so (for example, we need to investigate and secure evidence relating to an alleged offense).

(iii) Personal Information We Collect Automatically from You

We may automatically collect certain information from you using "cookies" and other similar tracking technologies when you visit our websites, platforms or use our office applications. For more information, please read Honeywell's [Cookie Notice](https://www.honeywell.com/us/en/cookie-notice#language3/) at <https://www.honeywell.com/us/en/cookie-notice#language3/>.



How We Process Your Personal Information

(i) *Engagement-related Purposes*

We use your personal information primarily for the purposes of determining your eligibility for an assignment and to manage your working relationship with us. Examples of why we use your personal information include:

- Identify, review, and manage candidacy for work assignments;
- Administration and delivery of the Supplier contract, assessing your onboarding application and supporting;
- Management of the assignment, including facilitating, monitoring, or evaluating your conduct, attendance and performance;
- Background checks and verification of references and qualifications, processing payroll, withholding taxes (or addressing other income tax matters), administering other required withholdings, or complying with various reporting or disclosure obligations under applicable law;
- Determine eligibility under export control regulations under applicable law;
- Analytical and statistical purposes to improve our understanding and make decisions about our contingent worker population (such as recruitment, engagement and retention risk);
- Analyze, improve, or develop process or tools related to your work assignment which may use algorithms, analytics software, surveys and other similar methods
- Supplying business contact information, including names, images, and other business contact information to employees, customers, suppliers, contractors, or other business associates and affiliates;
- Facilitating investigations (including suspected misconduct or non-performance of duties and related disciplinary actions);
- Maintaining and improving workplace and health, safety, and security (including the use of CCTV systems for monitoring Honeywell facilities, assets, investigating incidents and crime prevention and detection purposes);
- Authorizing, granting, administering, monitoring, improving, and terminating access to, use of, or the efficiency of company electronic systems, Information Resources, company-issued or company-authorized applications (including social media), facilities, records, property and infrastructure to the extent permitted and in compliance with law;
- Protecting company assets, including and in connection with internal investigations, through the (a) monitoring and review of email, communications, and information on company Information Resources to the extent permitted by and in compliance with law; (b) backup or storage of information on company desktops/laptops and other company Information Resources; and (c) authentication of employees' identities and the implementation of security measures;
- Understanding and improving business operations;
- Facilitating business communications;
- Maintaining global directories;



- Monitoring compliance with Honeywell's policies, procedures, and processes;
- Supporting Honeywell's aspirational Inclusion and Diversity objectives and initiatives or internal policies related to diversity and anti-discrimination;
- Preparing for, defending, or participating in litigation or potential litigation; and
- Facilitating compliance with contractual and legal obligations, such as any contract we may have with you or your Supplier.
- Comply with legal requirements, assist in investigation, comply with requests from regulatory and law enforcement authorities and meet contractual obligations;
- Other legitimate business reasons permitted or required by applicable Law

The Legal Bases for Processing Your Personal Information

The legal bases on which we collect or process your personal information will depend on the specific personal information and context in which we collect it. The processing of your personal information will take place based on one of the following legal bases where and to the extent they exist or are permitted by applicable law:

- Your **consent**;
- To comply with **legal obligations** (i.e., where statutes or regulations require the processing of your personal information);
- **Conclusion or performance of a contract** (for example, to execute an agreement between you and Honeywell or you and the Supplier);
- For the protection of your **vital interests** (for example, providing your health information to a doctor in a medical emergency at work);
- In Honeywell's (or a third party's) **legitimate interests** (for example, for compliance with a foreign law or as may be necessary for Honeywell's operational purposes) so long as those legitimate interests are not overridden by your fundamental rights or interests; or
- Where necessary for **credit protection**; or
- To **establish, exercise or defend a legal claim** including the exercise of right in legal proceedings.

If you have questions or need more information concerning the legal basis on which we use your personal information please contact HoneywellPrivacy@honeywell.com.

Error! Reference source not found.

We disclose your personal information to Honeywell personnel and third parties for purposes consistent with those described in this Notice.

(i) *Honeywell Group Entities*

Your personal information may be shared among Honeywell's legal entities including but not limited to Honeywell International Inc., Honeywell Technology Solutions Lab Pte Ltd., Honeywell International



Philippines Inc., and Honeywell Automotive de Mexico S.de R.L. de C.V.

(ii) Suppliers, External Advisors, and Other Third Parties

We will share your personal information with Suppliers that perform specific services on our behalf (for example, payroll support, data analytics services, tax and travel management services) as permitted by applicable law. These Suppliers may vary depending on the Honeywell entity for whom you provide a service to and may change over time. Additionally, we may share information about you with your Supplier in connection with the assignment.

Honeywell may share your personal information with external advisors (for example, accountants, auditors and law firms), business or joint venture partners, suppliers, vendors, contractors, affiliates, or any competent law enforcement body, regulator, government agency, court or other third party where we believe the disclosure is necessary or permitted under applicable law or in the good-faith belief that such action is necessary to exercise, establish or defend our legal rights or to protect your vital interests or those of another person. We may also share your personal information with others with your consent or at your direction.

Third parties who handle your personal information are required to do so in a manner that is consistent with applicable law and, when applicable, consistent with their contractual obligations to Honeywell.

In addition, when sharing your personal information with third parties, Honeywell will also fulfill other mandatory obligations as may be required by applicable law, such as informing you of the details of the recipients of your data and obtaining your separate consent where applicable.

For more information on the third parties with whom Honeywell shares your personal information, please contact HoneywellPrivacy@honeywell.com.

Transfers of Personal Information

Honeywell processes your personal information through our global platforms and on local systems. Operating our global platforms will involve transferring your personal information outside of your country to other countries where we operate and do business, including the United States, India, China, the Philippines, Mexico, and other countries. Third parties to whom Honeywell may disclose your personal information may also be located outside your country. This means that when we collect your personal information it may be processed in countries that have data protection laws that do not offer the same level of protection as your country of residence. However, Honeywell will take appropriate steps to provide a level of protection for personal information that is comparable to that of your country of residence which may include implementing Standard Contractual Clauses approved by relevant regulatory bodies. Honeywell will also fulfill other mandatory obligations as may be required by the applicable laws, such as informing you of the details of the recipients of your data, obtaining your separate consent and completing necessary procedure and steps required for such transfer.



Retention

We will retain your personal information until the end of your assignment plus a period of time thereafter as necessary to process matters related to your assignment (generally 10 years) unless otherwise required by applicable law.

Workplace Monitoring

Honeywell monitors its IT and communications systems through automated security and data loss prevention tools such as anti-malware software, website filtering and spam filtering software. We also monitor our locations through CCTV and badge scans (for instance, for security and safety purposes and to ensure that no unauthorized persons enter our sites). We conduct this monitoring principally for the following purposes:

- To ensure the safety and security of our systems, information assets, buildings, employees, and visitors;
- To maintain proof of business transactions and for recordkeeping purposes;
- To prevent or investigate alleged wrongful acts or violations of Honeywell policies (including violations of Honeywell's Code of Business Conduct and Acceptable Use of Information Resources Policy);
- To protect confidential information, intellectual property, and other business interests; and
- For other legitimate purposes permitted under applicable law.

Our monitoring activities are generally continuous and ongoing. However, they will always be proportionate, conducted for legitimate business purposes, and comply with any applicable data protection laws and collective bargaining agreements.

You should be aware that any messages, files, data, documents, facsimiles, audio, video, social media post, instant message communications or any other type of information transmitted to or from, received or printed from, created, stored or recorded on our IT and communications systems and assets are presumed to be business-related and may be monitored by Honeywell in accordance with applicable law. For more information on Honeywell's workplace monitoring practices, you must read Honeywell's [Acceptable Use of Information Resources Policy](https://sharepoint.honeywell.com/sites/PolicyManual/GPPS/GPPSHome.html) at <https://sharepoint.honeywell.com/sites/PolicyManual/GPPS/GPPSHome.html>. For your ease of reference, the **policy** is also embedded in this document for offline reference.

Your Data Protection Rights

Depending on applicable law, you may have certain rights with respect to your personal information. You may have the (i) right to access, rectify, erase, object, restrict or withdraw your consent to the processing of your personal information; (ii) the right to not have a decision made about you that is based solely on automated processing, including profiling, if that decision produces legal effects about you or significantly affects you, and (iii) a right to lodge a complaint with a supervisory authority.



We will facilitate your exercise of the rights that apply to you in accordance with applicable law. To exercise any of your rights relating to your personal information, please submit a data subject request form found at <https://honeywellhub.secure.force.com> or send an email to the Data Protection Officer at HoneywellPrivacy@honeywell.com.

Automated Processing and Profiling

We may automatically process your personal information by using software to evaluate or profile certain of your personal characteristics for analytical and statistical purposes to improve our understanding of and make decisions about recruitment, retention, performance and succession planning.

In general, these types of decisions will not be based solely on automated decision-making processes (i.e., your personal information will be always ultimately subject to human-made decisions) and will not have legal or similar effects for you. Any decisions based on sensitive personal information are taken manually by specially trained staff. If you are to be subjected to automated decision making, we will make it clear at the time and you have the right to contest the decision, to express your point of view, and to require a human review of the decision.

For more information on how this activity may affect you, or if you have any concerns or would like to object to this activity, please contact [HRHelp](#).

Security

Honeywell maintains and requires its Suppliers to maintain appropriate organizational and technical security measures to protect the security and confidentiality of your personal information.

Changes to this Notice

You may request a copy of this Notice from us using the contact details set out below. We may modify or update this Notice from time to time. If we change this Notice, we will notify you of the changes.

Contact Us

If you have any questions or complaints about how your personal information is processed or wish to exercise your rights, please send an email to [HRHelp](#) or the Data Protection Officer at HoneywellPrivacy@honeywell.com.

Consent

By signing below, I affirm that I have read, understood and agreed to the terms of this Notice, including:

- The purposes for which Honeywell processes my personal information;
- The type of personal information that Honeywell processes about me;
- The retention periods for which my personal information will be stored;
- The existence of my rights to be informed, to have access to the personal information processed



about me by Honeywell and to correct the same if necessary;

- The processing of my sensitive personal information;
- The data processing by, and transfer to, other third-party recipients located locally or abroad, including countries such as the United States, India, the Philippines and Mexico;
- That the equipment and information technology provided by Honeywell is for business purposes and not personal purposes; and
- That Honeywell has informed me that it has the right to investigate, monitor, verify or track the data and information handled by or contained in its equipment and information technology provided to me for use during the performance of my job.

Signature: _____

Name: _____

HID/EID (if applicable): _____

Date: _____

Commented [AM1]: To be deployed only in countries with consent requirements. **DELETE** for EEA, Switzerland and UK. Check the Global Data Privacy Standards for list of countries where consent is required



Acceptable Use of Information Resources Policy



0202 - Acceptable
Use of Information Re