ManpowerGroup Global

Privacy Notice (Notice)

Last Updated: February 2023

This ManpowerGroup Global Privacy Notice explains what you can expect regarding the collection and use of personal information by ManpowerGroup Global Inc. and its subsidiaries and affiliates listed here (as applicable, hereinafter each separately and/or jointly called the "Data Controller", “We”, “Our” or “Us”).

In general, our privacy practices conform with local law and regulation, including where applicable the provisions of the European Union’s General Data Protection Regulation (GDPR). Accordingly, our privacy practices may vary among the countries in which we operate to reflect local practices and legal requirements; you can view specific local terms by visiting our local websites.

Based on our relationship with you, we may also provide ‘just in time’ privacy notices that are tailored to the specific services/interactions you are eligible for, or receiving, at that particular time.

This Privacy Notice addresses the following topics (click on one of the links below to jump to the listed topic):

Who this Notice Applies to

This Privacy Notice applies to:

- associates, or job candidates, who are people we source and/or place in permanent or temporary work with one of our clients;

- candidates or participants that receive our Right Management career and/or talent management services;
- users of ManpowerGroup websites and apps (the "Sites");
- individual experts we engage to support our career and talent management services;
- representatives of our business partners, clients and vendors.

California residents can also view ManpowerGroup's North America Privacy Policy. https://www.manpowergroup.com/en/policies/north-america

This Privacy Notice does not apply to our headquarters and country-based staff employees, who are individuals employed by ManpowerGroup and who work directly for ManpowerGroup.

What do We mean by 'Personal Information' or 'Personal Data'?

Personal Information, also referred to as Personal Data, is information that whether alone, or combined with other information, allows you to be identified directly, or indirectly. Common personal data identifiers are attributes like your name, online identifier, or ID numbers. However, a

combination of one or more elements specific to your physical, physiological, genetic, psychological, economic, cultural, or social identity may also be identifiable personal information, given their potential to identify you when combined.

Some personal data types are considered more sensitive than others and the definition of sensitive data varies by local law. Across several major privacy laws, sensitive data examples include health and financial data, ethnic and racial origins, political opinions, genetic and biometric data, an individual's sex life or sexual orientation, religious/philosophical beliefs, trade union membership, precise geolocation and government issued identifiers.

Information We Collect

Depending on our relationship with you, we will collect personal information about you in various ways, such as through our Sites and social media channels, at our events, through phone and fax, through job applications and in-person recruitment, and in connection with our interactions with clients, vendors and business partners.

We may collect the following types of personal information (as permitted under local law and with consent where necessary):

- Information to identify you, such as your name and/or employee ID and, if you register on our Sites, your username and password;

- contact information, such as postal address, email address and telephone number;
- information about the organization you work for, your job title and/or department and the city/state/country or region you work in;
- cookies, web beacons and web server logs by automated means, consistent with the Cookie Notice published on the Site you visit ;
- device information and browser locale preferences, e.g. your language and time zone;
- dates, timestamps, and other records of our interactions with you and your usage of our Sites and services;
- information you provide about family, friends, or other people you would like us to contact or may need us to contact. The Controller assumes that the other person previously gave an authorization for such communication;
- Sensitive data, which may include racial or ethnic origin, political, religious, or philosophical beliefs, biometric data, data concerning health, information regarding sexual orientation; and
- other information you may provide to us, such as in surveys or through the "Contact Us" feature on our Sites.

If you are a candidate accessing career or talent management support or wishing to apply for a job, we may collect the following types of personal data (as permitted under local law and with consent where necessary):

- CV/Resume data, which may include contact details, social media URL, employment history, education history, professional memberships, qualifications, knowledge, skills, abilities, languages, licenses held;
- roles/opportunities of interest and salary expectations;
- personality, preference, and skills data from assessment participation and/or coaching, including personality traits, skills, strengths, motivators, career aspirations, development opportunities;
- a log of any events, interviews, training, or webinars attended or scheduled;
- profile picture if you register on one of our Sites that offers that functionality;
- video recording of any digital interview or interview practice you participate in;
- gender and age range; and
- information provided by job references or individuals requested to provide feedback on your work-related performance.

If you are a job candidate, we may also collect the following information (as permitted by local law and with consent where necessary);

- Social Security number, national identifier, or other government-issued identification;
- citizenship and work authorization status;

- bank account information;
- tax-related information;
- benefits information;
- date of birth; and
- results of drug tests, criminal and other background checks.

How We Use the Information We Collect

We use the data collected for the following purposes (dependent on our relationship with you and as permitted under local law):

1. identifying you and/or authenticating your identity;
2. sending you updates and notifications regarding the services you are receiving, and other related communications;
3. providing workforce solutions and connecting people to work;
4. creating and managing online accounts and optimizing and personalizing your user experience (please also consult the “Terms of Use” we publish on each Site footer);
5. providing coaching, feedback, analysis and advice and guidance to support you in your career management/development;
6. providing coaching, feedback, analysis and advice and guidance to support you in your career management/development;
7. assessing candidate’s suitability for available positions and/or client talent pools;

8. providing HR services, including administration of benefit programs, payroll, travel & expenses, performance management and disciplinary actions;
9. supporting our diversity and inclusion efforts and/or monitoring;
10. ensuring reasonable adjustment for individuals with disabilities or medical conditions that require it;
11. responding to queries, claims, and requests for assistance;
12. performing data analytics, such as;
    i. analyzing platform usage across our users,
    ii. analyzing our job candidate base,
    iii. assessing individual performance and capabilities, including scoring on work-related skills,
    iv. identifying skill shortages,
    v. using information to match individuals and potential opportunities,
    vi. analyzing pipeline data (trends regarding hiring practices),
    vii. determining the effectiveness of our engagement strategy, and
    viii. determining the effectiveness of our products and services.
13. aggregating data as part of our analytics efforts;
14. operating, evaluating, and improving our services;
15. auditing our interactions, transactions, accounting and other internal compliance functions;
16. protecting against, identifying, and seeking to prevent fraud, deceptive practices and other unlawful activity, claims and other liabilities;
17. enhancing the security of our network and information systems;
18. complying with and enforcing applicable legal requirements, exercise or defense of legal claims, relevant industry standards, contractual obligations, and our policies;
19. managing our client, vendor, and business partner relationships;

20. communicating around the services we offer, programs, special events, offers, surveys, evaluations, and market research - if you are a vendor representative, business partner or client representative;
21. processing payments and invoices; and
22. in a way consistent with the cookie notices we place on our Sites.

We also may use the information in other ways for which we provide specific notice at, or prior to, the time of collection. All processing will be carried out based on adequate legal grounds which may fall into a number of categories, including:

- consent or explicit consent from the data subject, where required by applicable law;
- to ensure that we comply with a statutory/legal obligation
- contractual requirement or any pre-contractual requirement necessary to enter into a contract;
- vital interests, where the processing is necessary to protect life; or
- it is essential and necessary for the legitimate business purpose of the Data Controller, as described in more detail below (e.g. allowing access to a website in order to provide the services offered).

Legitimate Business Interest

Depending on the privacy laws that apply, the Data Controller is permitted to process personal data for certain legitimate business interests, which can include some or all of the following:

- Where the process enables us to enhance, modify, personalize, or otherwise improve our services/communications for the benefit of our clients, candidates, and associates;
- to identify and prevent fraud;
- to enhance security of our network and information systems;
- to better understand how people interact with our websites;
- for direct marketing purposes;
- to provide postal communications to you which we think will be of interest to you; and

to determine the effectiveness of promotional campaigns and advertising.

Whenever we process data for these interests, we will ensure that we keep your rights in high regard and take account of these rights. You can object to such processing and may do so by contacting us as described below. Please bear in mind that if you exercise your right to object, this may affect our ability to carry out and deliver services to you for your benefit.。

Artificial Intelligence (AI) / Machine Learning (ML)

A number of the services we offer are enabled with AI, which may include AI/ML. With the assistance of AI, we can connect the right individuals with the best opportunities and get people into work more efficiently or prepare them for the job market more readily.

We perform risk assessments of the AI solutions we use at ManpowerGroup and use human oversight to the fullest extent possible to ensure no automated decisions are made that produce any legal or similarly significant effects on individuals.

If you are receiving a service that includes the use of AI/ML, you should be informed of this in more detail within the privacy notice provided in connection with that particular service.

How We Protect Personal Information

We maintain administrative, technical, and physical safeguards designed to protect the personal data we collect against accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure or use. Such measures are designed to provide an appropriate level of security taking

account, on one hand, the technical state of the art and, on the other hand, the sensitivity of the personal data and the evaluation of potential risks.

To provide the appropriate security and confidentiality of personal data, we apply the following non-exhaustive list of measures, as appropriate:

- Encryption of data at rest and in transit using industry standard encryption algorithms with appropriate key lengths;
- Strong user authentication and role-based access controls;
- Network monitoring solutions with events logging;
- Hardened network infrastructure;
- Measures for ensuring physical security of locations at which personal data are processed;
- Business continuity and disaster recovery plans with periodic testing;
- Incident management policy and processes;
- Periodic vulnerability and penetration testing;
- Certification/assurance of processes and products;
- Periodic employee privacy and security training and awareness program;
- Third party privacy and security assessments;
- Robust data processing and confidentiality agreements; and

- Organizational measures for ensuring data minimization, purpose limitation, retention, data quality and accountability.

How Long We Store the Data We Collect

We process the personal data we collect, also by automated means, for the purposes defined above and for a specific period of time, which complies with kept longer than necessary.

The personal information we collect is stored in an identifiable way only for the period of time we have determined is necessary, in light of the purposes for which the data was collected. We use the following criteria to determine our retention periods:

- The necessity to retain the personal data collected, in order to offer services established with the user;
- The legitimate interest of the Data Controller, as described above; and
- The existence of specific country or state legal obligations that make the processing and related storage necessary for specific period of times.

Information We Disclose

We may disclose the personal data collected, as described in this privacy notice, or in separate notices provided in connection with the services you are receiving or eligible for.

We may disclose a portion of personal data to vendors who perform services on our behalf, based on our instructions, to make our Sites and services available to you. We strive to ensure this data is minimized to what is necessary to perform the specific services instructed. We do not authorize vendors, that process data on our behalf, to use or disclose the information except as necessary to perform services or comply with legal requirements. Personal data will not be sold, rented, distributed or made available to vendors for their own commercial purposes, including for their direct marketing purposes.
We also may disclose your personal data
(i) with our subsidiaries and affiliates;
(ii) if you are a job candidate, with clients who may have job opportunities available or interest in placing our job candidates; and
(iii) with others with whom we work, such as consultants to provide the relevant career services or staffing suppliers who work with us to fill vacancies and place people into work (iv) if you are a recipient of talent management services,

we may disclose the status or progress of your program to the sponsoring client, along with any applicable assessment outcomes.

In addition, we may disclose personal data about you (i) if we are required to do so by law or legal process; (ii) to law enforcement authorities or other government officials based on a lawful disclosure request; and (iii) when we believe disclosure is necessary or appropriate to prevent physical harm or

financial loss, or in connection with an investigation of suspected or actual fraudulent or illegal activity. We also reserve the right to transfer personal data we have about you in the event we sell or transfer all or a portion of our business or assets (including in the event of a reorganization, dissolution or liquidation).

Links to External Tools and Resources

We may provide links to external third-party websites operated by organizations not affiliated with ManpowerGroup. We do not disclose your personal information to organizations operating such linked third-party websites and we do not review or endorse, and are not responsible for, the privacy practices of these organizations. We encourage you to read the privacy policy of each website that you visit. This privacy notice applies solely to information collected by ManpowerGroup and its subsidiaries and affiliates through the services.

Data Transfers

We also may transfer the personal data we collect about you to countries outside of the country in which the information originally was collected. Those countries may not have the same data protection laws as the country in which you initially provided the personal data.

When we transfer your information to other countries, we will protect that data as described in this Privacy Notice and any other specific notice given to you at the time of, or prior to, the processing. Such transfers will comply with applicable law.

When we transfer personal data from within the European Economic Area, the United Kingdom or Switzerland, to countries that do not benefit from Adequacy Agreements, transfers will take place on the basis of:
a) a legally binding and enforceable instrument between public authorities or bodies;
b) binding corporate rules;
c) standard contractual clauses (SCCs) adopted by the European Commission, along with the mandatory adoption provisions required for the UK and Switzerland to the extent the processing involves UK or Swiss residents.

Where transfers rely on SCCs, transfers will only take place after a transfer impact assessment of;
(1) The legal practices of the recipient country relating to access to data;
(2) The technical and organizational measures adopted to protect the data; and
(3) The nature of the processing to ensure purpose limitation and data minimization.

Subject to applicable law, you may obtain a copy of these safeguards by contacting us as indicated in the How to Contact Us section below.

Data Privacy Framework

ManpowerGroup (including ManpowerGroup Global Inc. and Right Management Inc.) complies with the EU-US Data Privacy Framework (EU-US DPF), the UK Extension to the EU-US DPF, and the Swiss-US Data Privacy Framework (Swiss-US DPF) as set forth by the US Department of Commerce. ManpowerGroup has certified to the US Department of Commerce that it

adheres to the EU-US Data Privacy Framework Principles (EU-US DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-US DPF and from the United Kingdom (and Gibraltar) under the UK Extension to the EU-US DPF. ManpowerGroup has certified to the US Department of Commerce that it adheres to the Swiss-US Data Privacy Framework Principles (Swiss-US DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-US DPF. If there is any conflict between the terms in this privacy policy and the EU-US DPF Principles and/or the Swiss-US 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/

ManpowerGroup is responsible for the processing of personal data it receives, under the EU-US DPF, the UK Extension to the EU-US DPF, and Swiss-US DPF and subsequently transfers to a third party acting as an agent on its behalf. ManpowerGroup complies with the EU-US DPF Principles and the Swiss-US DPF Principles for all onward transfers of personal data from the EU, UK, and Switzerland, including the onward transfer liability provisions.。

The Federal Trade Commission has jurisdiction over ManpowerGroup's compliance with the EU-US DPF, the UK Extension to the EU-US DPF, and the Swiss-US DPF. In certain situations, ManpowerGroup may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

In compliance with the EU-US DPF, the UK Extension to the EU-US DPF, and the Swiss-US DPF, ManpowerGroup commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-US DPF,

the UK Extension to the EU-US DPF, and the Swiss-US DPF to TRUSTe, an alternative dispute resolution provider based in the United States. 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 https://feedback-form.truste.com/watchdog/request for more information or to file a complaint. These dispute resolution services are provided at no cost to you.

In the context of the employment relationship, in compliance with the EU-US DPF, the UK Extension to the EU-US DPF, and the Swiss-US DPF, ManpowerGroup commits to cooperate and comply with the advice of the panel established by the EU data protection authorities (DPAs), the UK Information Commissioner's Office (ICO) and the Gibraltar Regulatory Authority (GRA), and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-US DPF, the UK Extension to the EU-US DPF, and the Swiss-US DPF.

For complaints regarding EU-US DPF, the UK Extension to the EU-US DPF, and Swiss-US DPF compliance not resolved by any of the other DPF mechanisms, you have the possibility, under certain conditions, to invoke binding arbitration. Further information can be found on the official DPF website: (https://www.dataprivacyframework.gov/s/article/ANNEX-I-introduction-dpf?tabset-35584=2)

Your Privacy Rights and Choices

When authorized by applicable law , you may exercise specific rights, such as:

1. Right of access: You have the right to obtain confirmation about whether personal data concerning you is being processed, and, where that is the case, to understand what personal data belonging to you that we hold and provide you with access to it.
2. Right to rectification: You have the right to request we correct or update of any inaccurate or incomplete data held about you, in order to protect the accuracy of such information and to adapt it to the data processing.
3. Right to erasure: you have the right to request that we delete and/or destroy information about you and no longer process that data. There might be latency in deleting information from servers and backed-up versions might exist for a short period after account deletion. Please note that erasure is not an absolute right; there may be legal or regulatory reasons to retain some, or all, of the data collected and this will be made clear to you if this is the case, for example to comply with our tax and accounting regulations.
4. Right to restriction of processing: You may request that the Data Controller restricts the processing of your data.
5. Right to data portability: You have the right to receive the personal data you have provided to us in a structured, commonly used, and machine-readable format. You have the right to request we transmit this data directly to another data controller/business.
6. Right to object: A data subject who provide a Data Controller with personal data may object, at any time, to the data processing on a number of grounds as set out under applicable laws, without needing to justify his or her decision. If you object, the previous processing of data will remain lawful.

7. Right to object: A data subject who provide a Data Controller with personal data may object, at any time, to the data processing on a number of grounds as set out under applicable laws, without needing to justify his or her decision. If you object, the previous processing of data will remain lawful.
8. Right to Opt-Out of the selling and sharing of your personal information: please note, we do not and will not sell or share your personal information as defined in California privacy laws.
9. Right to lodge a complaint with a supervisory authority: You have the right to lodge a complaint with a supervisory authority in the country or state of your habitual residence, place of work or place of the alleged infringement, if you consider the processing of your personal data infringes privacy law.
10. Whenever processing of your personal information is based on consent, you have the right to withdraw your consent at any time. There may be circumstances where we will still need to process your data for legal or official reasons after you withdraw your consent; where this is the case, we will restrict the data to what is necessary for the purpose of meeting those requirements. Any withdrawal of consent will not affect the lawfulness of the processing before its withdrawal.

How to Exercise your Privacy Rights and Choices

If you wish to exercise any of your data privacy rights or choices that you cannot perform yourself, you can do so via our Privacy Request Portal.

One of our team may contact you directly, or via our secure online portal, to verify your email address and thereafter your identity, before we provide access,

modify or erase your data. As part of this ID verification process you may be asked to provide a government issued ID and/or utility bill. We will permanently delete the verification information that you provide promptly after we have completed the verification process.

We are only required to respond to requests that are verifiable and legitimate. If we cannot verify your identity based on the processes described above, we may ask you for additional verification information. We will not use that information for any purpose other than verification. If we cannot verify your identity to a sufficient level of certainty to respond to your request, we will let you know promptly and explain why we cannot verify your identity and process your request.

Privacy Rights Requests by Authorized Parties

You may designate an authorized representative to exercise your rights on your behalf. If an authorized representative submits a request on your behalf, they must also submit a document signed by you that authorizes your representative to submit the request on your behalf.

In addition, we may ask that both you, and your representative, follow the applicable process described above for identity verification.

Data Processing related to Minors

We respect the privacy of children. Our Sites and services are not typically designed for, or targeted to, children. If you are under the age of 15, you should not send any information about yourself or your contact details through our Sites.

If you are a parent or guardian, please contact us if you believe we may have collected information from your child, and we will review and take appropriate action.

ManpowerGroup's Non-Discrimination Policy

Users of our Sites and services will not be subject to discriminatory treatment for exercising their privacy rights.

Please bear in mind that exercising some rights, like erasure, consent withdrawal or your right to object, may affect our ability to carry out and deliver some, or all, of the services you are eligible for.

Updates to Our Privacy Notice

From time to time, we may modify this Privacy Notice to reflect changes in technology, privacy practices and legal updates, or for other continuous improvement purposes. For significant changes, we will notify you by indicating at the top of each notice when it was most recently updated.

If we add additional services, or modify existing services, that we believe materially changes the nature of the processing you have been made aware of in this privacy notice and associated privacy notices provided to you in the delivery of our services, we will make reasonable efforts to provide you with additional notice. Depending on the reason for modification, we may also ask you to affirmatively consent to the changes. By continuing to use the services after such notice and/or consent, you agree to the terms of the revised Privacy Notice.

How to Contact Us

If you have any questions or comments about this Privacy Notice, or if you would like to exercise your rights, please submit a request through our Privacy Request Portal.

ManpowerGroup Inc.
Attn: General Counsel
100 Manpower Place
Milwaukee, WI 53212, USA