

Oxford Valuation Partners
Human Resources Data Privacy Policy

May, 2019

Table of Contents

| | |
|-------------------------------------------------------------------|----|
| Preamble | 4 |
| Scope | 4 |
| Collection and Use | 5 |
| Notice | 6 |
| Transparency | 6 |
| Consent: | |
| Alternative I (recommended by EEAC) | 7 |
| Alternative II (recommended by the National Workrights Institute) | 8 |
| Access and Correction | 9 |
| Disclosure | 10 |
| Choice | |
| Accuracy | 11 |
| Retention | 11 |
| Security | 11 |
| Compliance | 12 |
| Complaint Resolution | 13 |

Human Resources Data Privacy Policy

| PRINCIPLE | FREQUENTLY ASKED QUESTIONS REGARDING THE PRINCIPLES |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>PREAMBLE: The company recognizes and supports the need for reasonable protections regarding the privacy of personal “human resources” data collected by the company through the employment relationship. For this reason, the company has developed and adopted these general guiding Principles.</p> <p><u>All</u> company employees should help to ensure that the personal information the company holds about them is accurate and up to date. In addition, all company employees whose responsibilities include the collection, processing or storage of personal data are expected to assist in the protection of that data by adherence to these Principles.</p> <p>In following these Principles, the company complies with the applicable laws and regulations protecting the privacy of personal data in the employment relationship in the jurisdictions in which the company operates.</p> | <p>How do these Principles apply in practice?</p> <p>These are general Principles that establish the company’s intentions regarding the human resources data it collects from and about employees. The Principles should be implemented through locally applicable policies that take into consideration local legal requirements.</p> |
| <p>SCOPE: These Principles apply to all personal data about employees and applicants that is collected, maintained or used by the company as part of an actual or prospective employment relationship.</p> <p>Nothing in these Principles is intended to form a contract of employment or otherwise. The Company may amend these Principles from time to time, should it become necessary to do so.</p> <p>Personal data collected, maintained or used outside of the employment relationship, such as personal data arising from consumer marketing, is not covered by these Principles.</p> | <p>What is “personal data”?</p> <p>“Personal data” means data about an individual that is personally identifiable.</p> |
| <p>COLLECTION AND USE: The company collects and uses personal data in a reasonable and lawful manner. The company collects and</p> | <p>Why does the company collect and use personal data in the employment context?</p> |

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>uses personal data for relevant and appropriate purposes.</p> | <p>The collection and use of personal data in the employment context is essential to the operation of the company, and particularly to the human resources functions. Examples of the purposes for which the company collects and uses personal data include recruitment, administration of compensation and benefit programs, payroll, training, performance management, succession planning, meeting government requirements, or to protect the company, the workforce or the public against injury, theft, legal liability, fraud, abuse, or other misconduct.</p> <p>From what types of sources does the company collect personal data?</p> <p>The company believes that in most cases the individual is the best source of information about himself or herself. Therefore, to the extent practical and appropriate, the company collects personal data directly from the individual. In those cases in which it is necessary to collect personal data from other parties, the company uses sources that the company believes to be reputable and that take measures to ensure that the privacy interests of individuals are respected.</p> <p>Examples of when the company may seek information from others include:</p> <ul style="list-style-type: none"> ● Credit, reference and background checks; ● Investigations of possible employee wrongdoing; and ● Locating former employees and beneficiaries for purposes of administering our retirement, pension, and/or benefits plans. |
| <p>NOTICE: The company shall periodically inform individuals about whom the company collects personal data of (1) the type of data the company collects, (2) the purposes for which the company collects and discloses personal data, (3) the circumstances under which the company discloses personal data, including the types of potential recipients (4) that the company employs privacy and information safeguards; and (5) the circumstances under which individuals may access and correct their personal data.</p> | <p>How does the company provide notice of its information practices?</p> <p>The company provides periodic general notice regarding routine information practices. In addition, the company communicates these Principles and any implementing policies and procedures through normal communication channels.</p> |

| | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | |
| <p>TRANSPARENCY: The company shall periodically inform employees and others about our privacy principles, policies and procedures.</p> | <p>Why is transparency important?</p> <p>Communicating openly about the company’s privacy program is an important part of ensuring that the values expressed in these Principles are followed in practice, and in supporting employees’ confidence in the privacy of the HR data the company maintains. Communicating our policy also may be helpful to reinforce the company’s position when we refuse to disclose data to outsiders.</p> |
| <p>CONSENT</p> <p>The company collects personal data for employment-related business purposes. Where consent of the employee or a representative of employees for the collection, use, or disclosure of personal data is required by law or contract, the company will comply with the law or contract.</p> <p>In the event that an individual expresses a concern about the collection, use or disclosure of personal data, the company will respond to the employee’s concern consistent with applicable law.</p> | <p>What happens if an individual objects to the collection, use, and disclosure of his or her personal data?</p> <p>The company will not retaliate against any individual for expressing a concern about the collection, use, or disclosure of his or her personal data, or for exercising a legal right to refuse to provide information.</p> <p>This policy does not create a right to refuse to provide information that the company collects for employment-related business purposes. The company reserves the right to take appropriate action if an individual refuses to provide information that in the company’s judgment is necessary to the employment relationship or the provision of a benefit. For example, an applicant’s refusal to provide contact information is likely to disadvantage him or her in the hiring process. An employee’s refusal to identify his or her dependents is likely to interfere with the provision of group health insurance coverage for those dependents.</p> <p>Are there cases when the company may collect, use and disclose personal data without consent or accommodation?</p> <p>Yes. Under certain exceptional circumstances, such as investigation of possible wrongdoing, emergency situations, and when required by law or legal process, the company may collect, use or disclose personal</p> |

| | |
|--|--------------------------------------------------------------------------------------------------|
| | data without either requesting consent or providing an opportunity to object to such processing. |
|--|--------------------------------------------------------------------------------------------------|

ACCESS AND CORRECTION: Where the company maintains personal data in a structured filing system or database, it shall, upon request, provide employees with a reasonable opportunity to examine that information that pertains to them and add to or correct the data as appropriate, subject to certain exceptions where access would not be appropriate.

When can an employee access and correct personal data?

Upon request, employees will be given reasonable access to the personal data the company holds about them in a structured filing system or database, *e.g.* a personnel file or database, or an HRIS system. Reasonable access applies to both the process of accessing personal data and the types of data to be accessed (this second aspect of reasonable access is addressed in a separate FAQ). In terms of process, reasonable access means, for example, that requests for access are made during normal business hours, following standard procedures. Reasonable access also means that the frequency of access requests are not excessive.

Where local law contains additional requirements for access to HR data, the company will comply with local law.

If the individual reports that personal data we maintain is incorrect, the company will correct the information or allow the individual to provide comment, as appropriate.

Are there types of data to which the employee does not have access?

Yes. Confidential or proprietary information, such as business reorganization or succession plans; non-final performance evaluations, situations in which granting access might be subordinate to the privacy interests of others; when the information requested is related to an ongoing or completed investigation, litigation or potential litigation involving the company or its corporate parent, subsidiaries or affiliates, or non-final performance assessments. In addition, data that is diffuse and not maintained in a structured filing system, although subject to the rest of these Principles, is not available for access.

DISCLOSURE: The company places substantial importance on protecting the confidentiality of personal data and seeks the cooperation of all employees in furthering this goal.

Internal Disclosure: To the extent feasible, the company restricts access to personal data to those employees, agents, or contractors of the company, its corporate parent, affiliates divisions, or subsidiaries who have a legitimate business need for such access.

External Disclosure: Disclosure of personal data beyond the employees, agents, or contractors of the company, its corporate parent, affiliates, divisions or subsidiaries may be made pursuant to a labor agreement, for a sound business reason, as required by law or legal process, for another lawful purpose, *e.g.*, cooperation with local law enforcement authorities; to protect the interests of the company's employees, or, in the absence of any of the above, only with the authorization of the individual involved.

The company requires agents and contractors to whom the company discloses personal data for servicing to commit to protecting the privacy and security of the data and to refrain from any uses or further disclosures or not authorized by the company.

The company will not disclose personal data to unaffiliated third parties for consumer marketing purposes without the employee's written consent.

An employee's own request for the onward transfer of data (*e.g.*, confirmation of employment) must be made in writing (or according to other company procedures, such as a verifiable electronic request).

Aggregation: Where appropriate under the circumstances, the company will anonymize or

What's to keep those with access to some of an individual's personal data from browsing through other parts of it for other reasons?

The company is committed to training those who have access to personal data to act in accordance with these Principles, and thus to refrain from intentionally accessing information they have no business "need to know."

Under what circumstances might the company disclose personal data to third parties and what steps does the company take to safeguard that data?

As part of its normal business operations, the company may hire agents and contractors to carry out certain employment-related functions which require use of personal data, such as payroll. In all such instances, the company binds such parties through written agreements to safeguard the data, restrict the use and retention of the information to the purposes and timeframe of such outsourcing, and take other measures to ensure appropriate privacy protections.

In addition, under certain exceptional circumstances, the company may, as permitted by law, disclose other personal data without prior notice. Examples of such exceptional circumstances include when required by law or legal process, investigation of possible wrongdoing, emergency situations, and cases of business necessity, such as the sale of business units, in which disclosure of personal information is vital to the company's business interest.

The company will not make onward transfers of HR data for commercial gain, *e.g.* the sale of addresses to an outside firm for consumer marketing purposes.

| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>aggregate data to eliminate individual identifiers.</p> | |
| <p>The type or identity of third parties the company might disclose information to and what is the purpose of doing so</p> | <p>a) Anonymized information. If we anonymize personal data, we may share that personal data with anyone for any purpose. (b) Outsourcing providers. We may provide personal data to outsourcing providers who perform functions in support of our conduct of business. This might include data processing, storage, system administration, and similar functions. (c) Successors. If we sell or otherwise transfer all or a part of our business, or are investigating the possibility of doing so, we may transfer to, or share with, the actual or potential buyer or other transferee, the personal data associated with the actually or potentially sold or transferred business. (d) To comply with legal requirements. We may share your information if required by law enforcement, government agencies, courts, or others where we believe that our cooperation with information requests is required by law. We provide personal information to others so that we can accomplish the purposes stated above.</p> |
| <p>The choices and means the organization offers individuals for limiting the use and disclosure of their personal data</p> | <p>You have a choice about what personal data we retain and how we use it. See the principle choice for more details.</p> |
| <p>Being subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC)</p> | <p>We are subject to the investigatory and enforcement powers of the United States Federal Trade Commission (the “FTC”). You can learn more about the FTC’s role in enforcement of the Privacy Shield at https://www.commerce.gov/page/eu-us-privacy-shield</p> |
| <p>Liability in cases of onward transfers to third parties</p> | <p>If we transfer personal data to a third party and that transfer, or an act or omission by the third party, results in a violation of the Principles, we are liable for the transfer and/or the act or omission, even if it was the third party that committed the act or omission</p> |
| <p>CHOICE: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a</p> | <p>You have the right to choose (opt out) whether your personal data is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was</p> |

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.</p> | <p>originally collected or subsequently authorized by you. If you wish to opt out, all you need to do is contact us using the information in the section called “How to Contact Us.” Applicable law allows certain exceptions to your ability to opt out, such as where we are parties to a contract that is still being performed, where law requires us to maintain information tow warranty claims, or otherwise. Where applicable law permits us to retain and continue to use such information and we do so, we will do so only to the extent permitted or required by law. If you contact us to opt out, we will explain the options available and comply with your request as required by the Principles and applicable law.</p> |
| <p>By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.</p> | <p>The above choice/opt-out doesn’t apply where the sharing of your personal data is with a third party who is acting as our agent (such as our service providers who perform services that help us to run our business).</p> |
| <p>For sensitive information (see the above definitions), organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.</p> <p>“Sensitive information” under the EU-U.S. Privacy Shield means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or health or sex life. “</p> | <p>We will obtain your affirmative express consent (opt in) from you if we connect sensitive information and that information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. We also treat as sensitive any personal data received from a third party where the third party identifies and treats it as sensitive.</p> |

COMPLIANCE: The company proportionately ensures compliance with these Principles, as well as with applicable law or contractual agreements on handling of personal data.

A senior official of the company is responsible for implementing and overseeing the administration of these Principles.

All company employees whose responsibilities include the collection, processing or storage of personal data are required to adhere to these Principles and implementing policy. Failure to do so may be grounds for discipline up to and including termination.

Oxford Valuation Partners complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, the United States. Oxford Valuation Partners has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit <https://www.privacyshield.gov/>

What steps are taken to promote compliance with the Principles?

Compliance measures include:

- Training human resources employees and others with significant access to personal data on proper procedures for the processing of personal data;
- Requiring agents and contractors with significant access to personal data to make contractual commitments to safeguard the data and use it appropriately;
- Holding employees accountable for violation of these Principles and implementing policies, with sanctions, including the possibility of termination of employment; and
- Holding agents and contractors accountable for violation of their contractual commitments, with sanctions, including the possibility of termination of contracts.

COMPLAINT RESOLUTION: Any employee who has a concern about the collection, use or disclosure of the individual's personal data is encouraged to alert management.

In compliance with the Privacy Shield Principles, Oxford Valuation Partners commits to resolve complaints about our collection or use of your personal information. EU individuals with inquiries or complaints regarding our Privacy Shield policy should first contact our security department at:

security@oxfordvp.com

Oxford Valuation Partners has further committed to cooperate with the panel established by the EU data protection authorities (DPAs) with regard to unresolved Privacy Shield complaints concerning human resources data transferred from the EU in the context of the employment relationship.

May an employee be retaliated against for making a complaint or reporting potential violations of these Principles?

No. The company is committed to assisting employees in protecting their privacy and in providing opportunities to raise concerns about the security and potential use of their personal data. Retaliation against any employee who raises a concern under these Principles is against company policy and is strictly prohibited. In addition, the company will make reasonable efforts to maintain confidentiality regarding the employee's concern.

May an employee make an anonymous complaint?

Yes, but it may make it much more difficult for the company to conduct a proper investigation, and impossible for the company to respond to the employee.