

**EMPLOYMENT SCREENING RESOURCES (ESR)**

**EU-U.S. PRIVACY SHIELD POLICY  
AND  
SWISS-U.S. PRIVACY SHIELD POLICY**

ESR PRIVACY SHIELD POLICY ..... 2

Definitions:..... 2

Provisions of ESR EU-U.S. and EU Swiss Privacy Shield Policy ..... 2

    1. NOTICE ..... 2

    2. CHOICE ..... 4

    3. ACCOUNTABILITY FOR ONWARD TRANSFER ..... 4

    4. SECURITY ..... 4

    5. DATA INTEGRITY AND PURPOSE LIMITATION ..... 4

    6. ACCESS ..... 5

    7. RECOURSE, ENFORCEMENT AND LIABILITY ..... 5

PRIVACY SHIELD SUPPLEMENTAL PRINCIPLES ..... 6

    1. Sensitive Data ..... 6

    2. The Role of Data Protection Authorities ..... 6

    3. Self-Certification ..... 7

    4. Verification ..... 8

    5. Access ..... 8

    6. Human Resources Data ..... 10

    7. Obligatory Contracts for Onward Transfers ..... 10

    8. Dispute Resolution and Enforcement ..... 10

    9. Public Record and Publicly Available Information ..... 11

ANNEX I ..... 11

## ESR PRIVACY SHIELD POLICY

Employment Screening Resources (ESR) complies with the EU-U.S. the Swiss-U.S. Privacy Shield Frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. Employment Screening Resources 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/>.

This Privacy Shield Policy (“Policy”) applies to personal information about an identified or identifiable person that is received by ESR from the European Union and Switzerland, as applicable, and other personally identifiable information (“PII”) that ESR acquires in the performance of services for its clients, or other third parties with whom ESR has contractually agreed to apply this privacy policy. This Policy does not apply to data collected and used by ESR which is within the scope of the Directive.

### Definitions:

- a. “Personal Data,” and “Personal Information” refer to data about an identified or identifiable individual that are within the scope of the Directive, received by ESR in the United States from the European Union and Switzerland, as applicable and recorded in any form.
- b. “Processing” of Personal Information or Personal Data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.
- c. “Controller” means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- d. “Department” means the U.S. Department of Commerce.

### Provisions of ESR EU-U.S. and Swiss U.S. Privacy Shield Policies

#### 1. NOTICE

- a. ESR is a voluntary participant in both the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework and self-certifies according to the requirements of the program. You can find Privacy Shield Framework participants at <https://www.privacyshield.gov/PS-Application>.
- b. ESR gathers personal information regarding individuals, that have unambiguously consented to in writing, on behalf of its clients by manually or electronically contacting the appropriate sources of the data (court records, references, licensing bureaus, etc.) including but not limited to:
  - Criminal history at the federal, state and county levels;
  - Verification of credentials, including education and licensure;
  - State motor vehicle records abstracts;
  - Consumer Credit Reports;
  - Verification of present and past employment;
  - Personal and professional references;
  - National and international sanctions and exclusions database checks;
  - Sex offender registry checks; and
  - Drug and occupations health screening;

More information regarding the nature and scope of consumer data inquiries is available by contacting ESR in writing or by e-mail at the addresses listed on the Contact Us page (<http://www.esrcheck.com/Contact-Us/>) or by writing to the contacts listed below.

- c. ESR is unequivocally committed to apply the EU-U.S. and Swiss-U.S. Privacy Shield Framework requirements in their entirety to all personal information received from the EU or Switzerland, as applicable, in reliance on the Privacy Shield. ESR hereby verifies adherence to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks via ongoing in-house verification of the internal policies and procedures implemented by the ESR’s management of our company.

- d. ESR collects and uses personal information to prepare and provide background checks reports to employers or their agents (such as recruiters or staffing firms) for use in making employment-related decisions, such as who to hire, retain, promote, or re-assign. These reports may at time be use for Investigation into a suspicion of work-related misconduct or wrongdoing; Investigation into matters of employee compliance with employer policies, or Investigation into matters of employee compliance with Federal, State, or local laws and regulations.
- e. Persons who would like to make any type of inquiry about the Policy or to register a complaint under it may contact ESR as follows:

Employment Screening Resources

Attention: Brad Landin, President and Chief Compliance Officer

United States Telephone: +1-415-761-9018

Email: [privacy@esrcheck.com](mailto:privacy@esrcheck.com)

- f. With respect to the transfer of personal information to third parties (other than ESR agents), the principles of “Notice” and “Choice” apply. Accordingly, personal information is only provided to third parties for purposes described in the “Notice” section or otherwise disclosed to consumers, and will not be disseminated to a third party where a consumer has “opted-out” or, in the case of sensitive information, failed to “opt-in.”
- g. A person may request, in writing, access to all personal information collected and maintained about him or her by ESR. Upon receipt of such request ESR will provide all such information in a manner and form that maintains the security and confidentiality of the information. ESR affords the person a reasonable opportunity to correct, amend, or delete information that is inaccurate or incomplete, except where the burden or expense of providing access would be disproportionate to the risks to the individual’s privacy, or where the rights of persons other than the individual would be violated. In cases where the information is subject to the FCRA, ESR complies with the FCRA’s requirements regarding access and correction rights of consumers. To request information relating to his or her personal information, the party may contact ESR by e-mail at the following email address, [privacy@esrcheck.com](mailto:privacy@esrcheck.com), or by fax at +1-415-680-1627. In addition, the consumer will be asked to provide sufficient evidence of his or her identity so we may ensure that information is being released only to the subject of the data. If we are unable to provide the consumer with access to his or her EU or Swiss Personal Data or to correct the data, we will notify the consumer and provide all relevant details and circumstances preventing ESR from doing so.
- h. ESR offers individuals the opportunity to choose to “opt-out” or to “opt-in” whether their EU or Swiss Personal Data will be disclosed to a third party (not including ESR agents). These options are detailed in section number 2. Choice of this Policy.
- i. ESR is committed to resolve complaints about privacy and our collection or use of personal information fairly and efficiently. Individuals should begin by first contacting ESR. For any unresolved privacy complaints, ESR has chosen the EU Data Protection Authorities (EU DPAs) and the FDPIC, as applicable to serve as the independent dispute resolution body to address complaints and provide appropriate recourse free of charge to the individual. ESR has agreed to fully participate in the EU PDA’s and the FDPIC procedures to resolve disputes pursuant to the Privacy Shield Framework.
- j. ESR is subject to the to the investigatory and enforcement powers of the federal Consumer Financial Protection Bureau (CFPB), the federal Fair-Trade Commission (FTC), the California Investigative Consumer Reporting Agency Act (ICRAA), and the California Consumer Credit Reporting Agencies Act (CCRAA).
- k. An individual may invoke binding arbitration as the method for dispute resolution in accordance with the requirements and procedures set forth in Annex I of the Privacy Shield Framework.
- l. ESR is required to disclose Personal Information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.
- m. In the context of an onward transfer, ESR has responsibility for the processing of Personal Information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. ESR remains liable under the Principles if its agent processes such Personal Information in a manner inconsistent with the Principles, unless the ESR proves that it is not responsible for the event giving rise to the damage.
- n. ESR will provide a link to this notice when individuals are first asked to provide Personal Information to the ESR, or as soon thereafter as is practicable, but in any event before ESR uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

## 2. CHOICE

- a. ESR offers individuals the opportunity to opt-out of whether their Personal Information 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 originally collected or subsequently authorized by the individuals.
    1. Any third party ESR uses as an agent to perform task(s) on behalf of and under the instructions of the ESR are contractually bound to treat the information in a manner consistent with the Principles.
    2. In accordance with ESR's Written Information Security Policy, Personal Information is never used for a purpose other than what it was originally collected for and approved by the written consent of the subject person.
  - iii. OPTING-OUT
    1. Although ESR first obtains a person's unambiguous consent in writing, and because of ESR's commitment to afford individuals every possible protection, if you would like to opt-out from ESR using your Personal Information in either of the cases outlined in items i. and ii. above, simply send an email to [privacyshieldopt-out@esrcheck.com](mailto:privacyshieldopt-out@esrcheck.com), or call by United States Telephone: +1-415-761-9018.
      - a. If opting-out by email or telephone, please provide us with:
        - i. Your complete legal name,
        - ii. Month and year of birth, and
        - iii. The name of the ESR client with whom you have applied for a position.

## 3. ACCOUNTABILITY FOR ONWARD TRANSFER

- a. When ESR transfers Personal Information to a third party acting as a controller, the third party must comply with the Notice and Choice Principles. ESR holds contracts with the third-party controllers that provide that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify ESR if it makes a determination that it can no longer meet this obligation. The contract provides that when such a determination is made the third party controller will cease processing or takes other reasonable and appropriate steps to remediate.
- b. When transferring Personal Information to a third party acting as its agent, ESR: (i) transfers such data only for limited and specified purposes; (ii) has ascertained that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) takes reasonable and appropriate steps to ensure that the agent effectively processes the Personal Information transferred in a manner consistent with ESR's obligations under the Principles; (iv) requires the agent to notify ESR if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), ESR will take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) will provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department of Commerce upon request.

## 4. SECURITY

ESR in creating, maintaining, using and/or disseminating Personal Information takes reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the risks involved in the processing and the nature of the personal data. To this end ESR undergoes annual SSAE 16 Service Organization Control SOC 2 audits. A Service Organization Control (SOC) report is an audit of a service organization by an outside CPA firm using stringent criteria set by the American Institute of Certified Public Accountants (AICPA). This in-depth audit assesses ESR's internal controls across areas related to delivery of its services. The SOC 2 audit report assesses security controls. ESR's SSAE 16 SOC 2 annual audit report examines these trust principles, Security, Privacy, and Confidentiality. In addition, ESR is PCI-DDS Security compliant and tested and is accredited by the National Association of Professional Background Screeners Background Screening Credentialing Council.

## 5. DATA INTEGRITY AND PURPOSE LIMITATION

- a. Consistent with the Principles, ESR use of Personal Information is limited to the information that is relevant for the purposes of processing. ESR does not process Personal Information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, ESR takes reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. ESR adheres to the Principles for as long as it retains such information.
- b. ESR retains information in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing within the meaning of 5a, or as required by law or regulation. ESR takes reasonable and appropriate measures to comply with this provision.

## **6. ACCESS**

- a. Individuals have access to their Personal Information held by ESR and are able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated. Individuals may contact ESR using the contact information set forth in section 1.e. of this Policy.

## **7. RECOURSE, ENFORCEMENT AND LIABILITY**

- a. ESR's privacy protection includes robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and acknowledges there are consequences for ESR when the Principles are not followed. ESR's mechanisms include:
  - i. EU Data Protection Authorities (EU DPAs) and the FDPIC serve as the independent dispute resolution bodies to address complaints and provide appropriate recourse free of charge to the individual. ESR has agreed to fully participate in the EU PDA's and FDPIC procedures to resolve disputes pursuant to the Privacy Shield Framework, and is subject to damages awarded where the applicable law or private-sector initiatives so provide;
  - ii. Obtaining a copy of ESR's annual SOC2 Type 2 audit report is the procedure for verifying that the attestations and assertions ESR makes about its privacy practices are true and that privacy practices have been implemented as presented, including any areas of non-compliance; and
  - iii. ESR by announcing its adherence to them acknowledges its obligation to remedy problems arising out of failure to comply with the Principles and realizes that there are consequences for failure to comply, and acknowledges that any sanctions levied will be sufficiently rigorous to ensure its future compliance.
- b. ESR will respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield. ESR will respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State or Swiss authorities through the Department. ESR as an organization that processes non-human resources data has chosen to cooperate with DPAs and the Swiss authorities, and will respond directly to such authorities with regard to the investigation and resolution of complaints.
- c. ESR acknowledges its obligation to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to ESR and following the procedures and subject to conditions set forth in Annex I.
- d. In the context of an onward transfer, ESR is responsible for the processing of Personal Information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. ESR acknowledges it is liable under the Principles if its agent processes such Personal Information in a manner inconsistent with the Principles, unless ESR proves that it is not responsible for the event giving rise to the damage.
- e. Should ESR become subject to an FTC or court order based on non-compliance, ESR will make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. ESR acknowledges that the Department has established a dedicated point of contact for DPAs for any problems of compliance by Privacy Shield organizations, and that the FTC will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State or Swiss authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.

## PRIVACY SHIELD SUPPLEMENTAL PRINCIPLES

### 1. Sensitive Data

- a. ESR is not required to and does not obtain affirmative express consent (opt in) with respect to sensitive data where the processing is:
  - i. In the vital interests of the data subject or another person;
  - ii. Necessary for the establishment of legal claims or defenses;

### 2. The Role of Data Protection Authorities

- a. ESR is committed to cooperate with European Union data protection authorities (“DPAs”) and the FDPIC as described below. ESR commits to employ effective mechanisms for assuring compliance with the Privacy Shield Principles. ESR will provide: (a)(i) recourse for individuals to whom the data relate; (a)(ii) follow up procedures for verifying that the attestations and assertions they have made about their privacy practices are true by providing access; and (a)(iii) will remedy problems arising out of failure to comply with the Principles and accept any consequences.
- b. ESR commits to cooperate with the DPAs by declaring in its Privacy Shield self-certification submission to the Department of Commerce that ESR:
  - i. Elects to satisfy the requirement in points (a)(i) and (a)(iii) of the Privacy Shield Recourse, Enforcement and Liability Principle by committing to cooperate with the DPAs and the FDPIC;
  - ii. Will cooperate with the DPAs and the FDPIC in the investigation and resolution of complaints brought under the Privacy Shield; and
  - iii. Will comply with any advice given by the DPAs or the FDPIC and will take specific action where the DPAs or FDPIC believes that ESR must do so to comply with the Privacy Shield Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken.
- c. Operation of DPA Panels
  - i. ESR acknowledges and accepts that the DPAs and FDPIC may provide information and advice in the following way:
    1. The panel will provide any advice to ESR on unresolved complaints from individuals about the handling of Personal Information that has been transferred from the EU under the Privacy Shield. This advice will be designed to ensure that the Privacy Shield Principles are being correctly applied and will include any remedies for the individual(s) concerned that the DPAs consider appropriate.
    2. The panel will provide such advice in response to referrals from ESR and/or to complaints received directly from individuals against organizations which have committed to cooperate with DPAs for Privacy Shield purposes, while encouraging and if necessary helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer.
    3. Advice will be issued only after both sides in a dispute have had a reasonable opportunity to comment and to provide any evidence they wish. The panel will seek to deliver advice as quickly as this requirement for due process allows. As a general rule, the panel will aim to provide advice within 60 days after receiving a complaint or referral and more quickly where possible.
    4. The panel will make public the results of its consideration of complaints submitted to it, if it sees fit.
    5. The delivery of advice through the panel will not give rise to any liability for the panel or for individual DPAs.
  - ii. ESR has chosen this option for dispute resolution and therefore it must comply with the advice of the DPAs. ESR acknowledges that any failure to fulfill the undertaking to cooperate with the DPAs, as well as failures to comply with the Privacy Shield Principles, will be actionable as a deceptive practice under Section 5 of the FTC Act or other similar statute.

- d. ESR uses Personal Information human resources related data transferred from the EU and commits to cooperate with the DPAs and the FDPIC with regard to such data (see Supplemental Principle on Human Resources Data).

### 3. Self-Certification

- a. Privacy Shield benefits are assured from the date on which the Department has placed the ESR's self-certification submission on the Privacy Shield List after having determined that the submission is complete.
- b. ESR has provided to the Department a Privacy Shield self-certification submission, signed by a corporate officer on behalf of ESR, that contains the following information:
  - i. The name of our organization, mailing address, e-mail address, telephone, and fax numbers;
  - ii. A description of the activities of the organization with respect to Personal Information received from the EU by ESR; and
  - iii. A description of the ESR's privacy policy for such Personal Information, including:
    - 1. ESR's public website address where the privacy policy is available (<http://www.esrcheck.com/Privacy-Policy>);
    - 2. Its effective date of implementation; 07/31/2016
    - 3. A contact office for the handling of complaints, access requests, and any other issues arising under the Privacy Shield;
    - 4. The specific statutory bodies that have jurisdiction to hear any claims against ESR regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the Principles or a future annex to the Principles);
    - 5. Name of any privacy program in of which ESR is a member;
    - 6. Method of verification prescribed in the Supplemental Principle on Verification; and
    - 7. The independent recourse mechanism that is available to investigate unresolved complaints.
- c. ESR wishes its Privacy Shield benefits to cover human resources information transferred from the EU for use in the context of the employment relationship, and the federal Fair Trade Commission (FTC) is the statutory body listed in the Principles or a future annex to the Principles that has jurisdiction to hear claims against ESR arising out of the processing of human resources information. ESR declares its commitment to cooperate with the EU authority or authorities concerned in conformity with the Supplemental Principles on Human Resources Data and the Role of the Data Protection Authorities as applicable and that it will comply with the advice given by such authorities. ESR has provided the Department with a copy of its human resources privacy policy and provided information where the privacy policy is available for viewing by its affected employees.
- d. ESR self-certification submissions will be provided not less than annually; otherwise ESR will be removed from the Privacy Shield List and Privacy Shield benefits will no longer be assured. Both the Privacy Shield List and the self-certification submissions by ESR will be made publicly available. ESR states in its relevant published privacy policy statements that ESR adheres to the Privacy Shield Principles. ESR's privacy policy is available online and ESR provides a hyperlink to the Department's Privacy Shield website and a hyperlink to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved complaints.
- e. ESR's Privacy Principles apply immediately upon certification. Recognizing that the Principles will impact commercial relationships with third parties, ESR certifies that it shall bring existing commercial relationships with third parties into conformity with the Accountability for Onward Transfer Principle as soon as possible, and in any event no later than nine months from the date upon which ERS certifies to the Privacy Shield. During that interim period, where organizations transfer data to a third party, ESR shall (i) apply the Notice and Choice Principles, and (ii) where personal data is transferred to a third party acting as an agent, ascertain that the agent is obligated to provide at least the same level of protection as is required by the Principles.
- f. ESR subjects all personal data received from the EU in reliance upon the Privacy Shield to the Privacy Shield Principles. ESR's undertaking to adhere to the Privacy Shield Principles is not time-limited in respect of personal data received during the period in which the ESR enjoys the benefits of the Privacy Shield. ESR will continue to apply the Principles to such data for as long as ESR stores, uses or discloses them, even if it subsequently leaves the Privacy Shield for any reason.
- g. If ESR ceases to exist as a separate legal entity as a result of a merger or a takeover it will notify the Department of this in advance. The notification will indicate whether the acquiring entity or the entity resulting from the merger will (i)

continue to be bound by the Privacy Shield Principles by the operation of law governing the takeover or merger or (ii) elect to self-certify its adherence to the Privacy Shield Principles or put in place other safeguards, such as a written agreement that will ensure adherence to the Privacy Shield Principles. Where neither (i) nor (ii) applies, any personal data that has been acquired under the Privacy Shield will be promptly deleted.

- h. If ESR leaves the Privacy Shield for any reason, it will remove all statements and marks implying that it continues to participate in the Privacy Shield or is entitled to the benefits of the Privacy Shield.

#### 4. Verification

- a. ESR's follow up procedures for verifying that the attestations and assertions it makes about its Privacy Shield privacy practices are true and those privacy practices have been implemented as represented and in accordance with the Privacy Shield Principles is to obtain a copy of ESR's then current SSAE 16 SOC2 audit report and/or a copy of ESR's Written Information Security Policy.
- b. ESR verifies its attestations and assertions through self-assessment and outside compliance reviews.
- c. ESR's privacy policy regarding Personal Information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible. ESR's privacy policy conforms to the Privacy Shield Principles; individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; ESR has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and ESR has in place internal procedures for periodically conducting objective reviews of compliance with the above. ESR statement verifying the self-assessment is signed by a corporate officer or other authorized representative of the organization no less than once per year and is made available upon request by individuals or in the context of an investigation or a complaint about non-compliance.
- d. ESR's chosen SSAE 16 SOC2 Type 2 annual audits that demonstrate that ESR's privacy policy regarding Personal Information received from the EU conforms to the Privacy Shield Principles, that it is being complied with, and that individuals are informed of the mechanisms through which they may pursue complaints. ESR's completes its outside compliance review once per year and upon completion is signed by the reviewer and a corporate officer of ESR. It is made available upon request by individuals or in the context of an investigation or a complaint about compliance.
- e. ESR maintains its records on the implementation of its Privacy Shield privacy practices and makes them available upon request in the context of an investigation or a complaint about non-compliance to the independent body responsible for investigating complaints or to the agency with unfair and deceptive practices jurisdiction. ESR will respond promptly to inquiries and other requests for information from the Department relating to the organization's adherence to the Principles.

#### 5. Access

- a. The Access Principle in Practice
  - i. Under the Privacy Shield Principles, the right of access is fundamental to privacy protection. In particular, it allows individuals to verify the accuracy of information held about them. The Access Principle means that individuals have the right to:
    - 1. Obtain from ESR confirmation of whether or not ESR is processing personal data relating to them; ESR will answer requests from an individual concerning the purposes of the processing, the categories of personal data concerned, and the recipients or categories of recipients to whom the personal data is disclosed.
    - 2. Have communicated to ESR such data so that they could verify its accuracy and the lawfulness of the processing; and
    - 3. Have the data corrected, amended or deleted where it is inaccurate or processed in violation of the Principles.
  - ii. Individuals do not have to justify requests for access to their personal data. In responding to individuals' access requests, ESR is first guided by the concern(s) that led to the requests in the first place. For example, if an access request is vague or broad in scope, ESR will engage the individual in a dialogue so as to better understand the motivation for the request and to locate responsive information. ESR might inquire about which part(s) of ESR

the individual interacted with or about the nature of the information or its use that is the subject of the access request.

- iii. Consistent with the fundamental nature of access, ESR will always make good faith efforts to provide access. For example, where certain information needs to be protected and can be readily separated from other Personal Information subject to an access request, ESR will redact the protected information and make available the other information. If ESR determines that access should be restricted in any particular instance, it will provide the individual requesting access with an explanation of why it has made that determination and a contact point for any further inquiries.

b. Burden or Expense of Providing Access

- i. The right of access to personal data may be restricted by ESR in only in exceptional circumstances where the legitimate rights of persons other than the individual would be violated or where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question. Expense and burden are important factors and will be taken into account but they are not controlling factors in determining whether ESR providing access is reasonable.
- ii. For example, if the Personal Information is used for decisions that will significantly affect the individual (e.g., the denial or grant of important benefits, such as insurance, a mortgage, or a job), then consistent with the other provisions of these Supplemental Principles, ESR will disclose that information even if it is relatively difficult or expensive to provide. If the Personal Information requested is not sensitive or not used for decisions that will significantly affect the individual, but is readily available and inexpensive to provide, ESR will provide access to such information.

c. Confidential Commercial Information

- i. Confidential commercial information is information that ESR has taken steps to protect from disclosure, where disclosure would help a competitor in the market. ESR may deny or limit access to the extent that granting full access would reveal its own confidential commercial information, such as marketing inferences or classifications generated by ESR, or the confidential commercial information of another that is subject to a contractual obligation of confidentiality.
- ii. Where confidential commercial information can be readily separated from other Personal Information subject to an access request, ESR will redact the confidential commercial information and make available the non-confidential information.

d. Organization of Data Bases

- i. Access can be provided in the form of disclosure of the relevant Personal Information by ESR to the individual and does not require access by the individual to ESR's data base.
- ii. Access will be provided only to the extent that ESR stores the Personal Information. The Access Principle does not itself create any obligation by ESR to retain, maintain, reorganize, or restructure Personal Information files.

e. When Access May be Restricted

- i. ESR will make good faith efforts to provide individuals with access to their personal data, the circumstances in which ESR may restrict such access are limited, and any reasons for restricting access will be specific. As under the Directive, ESR can restrict access to information to the extent that disclosure is likely to interfere with the safeguarding of important countervailing public interests, such as national security; defense; or public security. Other reasons for denying or limiting access are:
  - 1. Interference with the execution or enforcement of the law or with private causes of action, including the prevention, investigation or detection of offenses or the right to a fair trial;
  - 2. Disclosure where the legitimate rights or important interests of others would be violated;
  - 3. Breaching a legal or other professional privilege or obligation;
  - 4. Prejudicing employee security investigations or grievance proceedings or in connection with employee succession planning and corporate re-organizations; or

- 5. Prejudicing the confidentiality necessary in monitoring, inspection or regulatory functions connected with sound management, or in future or ongoing negotiations involving ESR.
  - ii. ESR when claiming an exception has the burden of demonstrating its necessity, and the reasons for restricting access and will provide a contact point for further inquiries to be made by individuals.
- f. Right to Obtain Confirmation and Charging a Fee to Cover the Costs for Providing Access
  - i. An individual has the right to obtain confirmation of whether or not ESR has personal data relating to him or her. An individual also has the right to have communicated to him or her personal data relating to him or her.
  - ii. Although permitted to do so, ESR will not charge a fee for the confirmation or communicating of Personal Information.
- g. Repetitious or Vexatious Requests for Access
  - i. Although permitted to do so, ESR does not set limits on the number of times within a given period that access requests from a particular individual will be met.
- h. Fraudulent Requests for Access
  - i. ESR will not provide access unless it is supplied with sufficient information to allow it to confirm the identity of the person making the request.
- i. Timeframe for Responses
  - i. ESR will respond to access requests within a reasonable time period, in a reasonable manner, and in a form, that is readily intelligible to the individual.

## **6. Human Resources Data**

- a. Coverage by the Privacy Shield
  - i. Where an organization in the EU transfers Personal Information about its employees (past or present) collected in the context of the employment relationship to ESR as an outside service provider, the transfer enjoys the benefits of the Privacy Shield.
- b. Application of the Notice and Choice Principles
  - i. When ESR receives employee information from the EU under the Privacy Shield it will disclose it to third parties only in accordance with the Notice and Choice Principles, and then only for the single purpose the individual has unambiguously consented to in writing. ESR does not reuse or resell Personal Information under any circumstances.

## **7. Obligatory Contracts for Onward Transfers**

- a. Transfers between Controllers
  - i. For transfers between controllers, the recipient controller need not be a Privacy Shield organization or have an independent recourse mechanism. ESR will in all cases enter into a contract with the recipient third-party controller that provides for the same level of protection as is available under the Privacy Shield, not including the requirement that the third party controller be a Privacy Shield organization or have an independent recourse mechanism, provided it makes available an equivalent mechanism.

## **8. Dispute Resolution and Enforcement**

- a. The Recourse, Enforcement and Liability Principle sets out the requirements for Privacy Shield enforcement. ESR satisfies the requirements by compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; and a commitment to cooperate with data protection authorities located in the European Union or their authorized representatives.

- b. In order to help ensure compliance with its Privacy Shield commitments and to support the administration of the program, ESR will provide information relating to the Privacy Shield when requested by the Department. ESR will respond expeditiously to complaints regarding its compliance with the Principles referred through the Department by DPAs and the FDPIIC. The response will address whether the complaint has merit and, if so, how ESR will rectify the problem. The Department will protect the confidentiality of information it receives in accordance with U.S. law.
- c. Recourse Mechanisms

- i. Consumers are encouraged to raise any complaints they may have with ESR before proceeding to independent recourse mechanisms. ESR will respond to a consumer within 45 days of receiving a complaint. As required by the Recourse, Enforcement and Liability Principle, the recourse available to individuals will be readily available and free of charge.
- ii. ESR has chosen the EU Data Protection Authorities (EU DPAs) through The United States Council for International Business USCIB acting as a trusted third party on behalf of the European Union (EU) Data Protection Authorities to serve as an independent recourse mechanism (IRM) for dispute resolution arising from collection, use, and retention of Personal Information transferred from EU member countries to ESR.

ESR has chosen the Swiss Federal Data Protection and Information Commissioner (FDPIIC) to serve as an independent recourse mechanism (IRM) for dispute resolution arising from collection, use, and retention of Personal Information transferred from Switzerland to ESR.

- iii. ESR acknowledges that set forth in Annex I, an arbitration option is available to an individual to determine, for residual claims, whether a Privacy Shield organization has violated its obligations under the Principles as to that individual, and whether any such violation remains fully or partially remedied. This option is available only for these purposes.

## **9. Public Record and Publicly Available Information**

- a. ESR in all cases applies the Privacy Shield Principles of Security, Data Integrity and Purpose Limitation, and Recourse, Enforcement and Liability to personal data from publicly available sources, and to data collected from public records, i.e., those records kept by government agencies or entities at any level that are open to consultation by the public in general.

### **ANNEX I**

Annex I provides the terms under which Privacy Shield organizations are obligated to arbitrate claims, pursuant to the Recourse, Enforcement and Liability Principle. It can be found in its entirety at this Privacy Choice website URL:

<https://www.privacyshield.gov/article?id=ANNEX-I-introduction>.