SPENCER STUART
DATA PROTECTION STANDARDS

The Spencer Stuart Group ("Spencer Stuart") is the leading firm of choice in the provision of executive search, leadership advisory, human resources and employee engagement services among top companies seeking guidance and counsel on their senior leadership and organisational needs.

Given the importance of safeguarding your Personal Data and ensuring that its processing in the context of our service offerings is done in a fair, accurate and transparent way, we have committed ourselves to protecting your privacy. These are legally binding on all Spencer Stuart participating entities and employees, and Spencer Stuart must integrate the requirements within our business practices. This means that all Spencer Stuart entities and employees have a duty to ensure that these Binding Corporate Rules are respected and adhered to across the Firm. The following describes our Firm's policy regarding the collection, use, and transfer of your Personal Data as well as your rights.

1. Definitions, Objective & Scope

The purpose of the Data Protection Standards (the "**Standards**" or "**BCRs**") is to provide consistent safeguards for the processing of the Personal Data of all individuals whose information is processed by Spencer Stuart in the context of the provision of its services including data subjects affected by data transfers, or sets of transfers, performed by Spencer Stuart in the provision of its services. The following terms are used in these BCRs:

- *Applicable Data Protection Laws* means data protection laws in force in the territory from which an Entity initially transfers Personal Data under these BCRs. Where a European Entity transfers personal data under these BCRs to a non-European Entity, the term applicable data protection laws shall include the European data protection laws applicable to that European Entity (including the GDPR).

- *Data Transfers* pertains to the transfer of Personal Data to countries included in Appendix 2.

- *Exporter* means a Spencer Stuart Entity who processes personal data subject to the GDPR as a controller on behalf of the Group and transfers this personal data to another Entity outside Europe (the Importer) for further processing.

- *Importer* means a Spencer Stuart Entity outside Europe who receives personal data from the Exporter with a view to further processing this personal data as a controller.

- *Individual* is any individual whose information is processed in the provision of Spencer Stuart's services and internal business purposes. This includes but is not limited to candidates, assessed individuals, business contacts, sources, referees, and personnel.

- *Nature* and *Categories of Personal Data* pertain to the type of Personal Data that Spencer Stuart may collect in its provision of its professional services, which is included in Appendix 2

- *Personal Data* shall have the same meaning as in Directive 95/46/EC of 24 October 1995 and the General Data Protection Regulation (2016/679).

- *Processing* or *Process* refers to any manual, or automated action performed on Personal Data by Spencer Stuart. This includes, but is not limited to collecting, using, adapting,

structuring, retrieving, recording, organising, storing, modifying, disseminating, transferring, disclosing, deleting, and sharing such data among the Spencer Stuart group in accordance with Spencer Stuart's policies.

- *Spencer Stuart Entity (or Entity)* means a Spencer Stuart Entity listed in Appendix 1.

- *Supervisory Authority (or SA)* means the supervisory data protection authority that is competent for the exporter of personal data.

- *Third party* means a natural or legal person, public authority, agency or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data

2. Spencer Stuart Global Standards & Local Laws

Spencer Stuart currently operates multiple offices throughout the world, locations being available at www.spencerstuart.com/locations. Regardless of the jurisdiction, each office and Entity of Spencer Stuart is required to abide by these Standards through the creation of an Intra-Group Agreement binding all Spencer Stuart Entities. Doing so protects the Personal Data processed by Spencer Stuart in countries that possess less rigorous protection mechanisms than those contained in these Standards. Spencer Stuart will ensure that any new Entities formed after the creation of these Standards will abide by the protections described herein. Of course, where certain countries or supranational Entities in which Personal Data is processed employ more stringent regulations than those contained in these Standards, Spencer Stuart will naturally comply with those more stringent regulations. For jurisdictions outside the EEA, Spencer Stuart will carry out prior data transfer impact assessments ('TIAs') to ascertain whether the applicable laws, regulations, and practices of the third country destination do not prevent it from fulfilling its obligations under the Standards. These assessments will consider, amongst other factors:

- the specific circumstances of the transfer and of any envisaged onward transfers to a country outside the EEA or within that same country, including but not limited to: categories and format of data, the type and purpose of processing, types of Entities involved in the processing, sector in which the transfer occurs, location of the processing (including storage), and transmission channels of processing;

- the adequacy of our contractual, technical, and organizational measures for safeguarding data including measures applied during transmission and to the processing of the personal data in the country of destination;

- whether the level of protection required by EU law is respected by the laws and practices of the relevant country outside the EEA such as those compelling the disclosure of data to public authorities or authorising access by such authorities, including during the transit of data;

- whether any legislation therein could interfere with fundamental data subject rights (including the possibility of lawful access requests); and

- whether Spencer Stuart should enact supplementary measures to ensure a level of protection equivalent to European requirements.

Where this is the case, the Entity in question seeking to enact these safeguards should inform Spencer Stuart International Ireland, who shall be involved in the assessment and any other Entities involved. The assessment, along with its conclusion and any relevant supplementary measures to be implemented, will be appropriately documented and made available to the SA

upon request. Where any safeguards in addition to those envisaged under the BCRs should be put in place, the entity, and the DPO will be informed and involved in such assessment. The Standards will only be used as a protection mechanism where these assessments have occurred. Spencer Stuart Entities will communicate the results and decisions arising from these assessments within the group. Spencer Stuart exporting Entities will monitor developments, on an ongoing basis, and where appropriate, in collaboration with Spencer Stuart importer Entities, the laws and practices of third countries that could have an impact on the rights of data subjects after the initial assessment has occurred and accordingly make decisions on such transfers. If, as a data importer, a Spencer Stuart Entity receives a lawful access request from a third-country authority, these rules require the relevant Entity to use all legal, organisational, and technical measures at its disposal to limit the data which can be accessed in order to support the protection of data subjects' rights. Spencer Stuart currently employs technical measures which ensure personal data is protected in the event of such access requests. Furthermore, additional contractual commitments to ensure continued protection bind all Spencer Stuart affiliated Entities.

The Standards require any Spencer Stuart Entity to notify its counterparts if it has reason to believe that it has become subject to laws or practices that would prevent it from fulfilling its obligations under the Standards. Upon verification of this, the appropriate persons responsible for data protection shall promptly identify appropriate technical and/or organisational measures to adopt in order for the Entity to fulfil its obligations under the Standards. Where no such appropriate safeguards can be ensured, or where the SA instructs, the transfer of data to this country outside the EEA or any other transfers for which it can be concluded would lead to the same consequences, will be suspended. Transfers of data will end completely if the Spencer Stuart Entity cannot comply with these BCRs or if it is not restored within one month of suspension. Any data transferred prior to suspension should, at the choice of the Spencer Stuart Entity, be returned or destroyed.

Conversely, if the importer ceases to be bound by these BCRs for a different reason other than that mentioned above, it may keep, return, or delete the personal data received under the BCRs. If the data exporter and data importer agree that the data may be kept by the data importer, protection must be maintained in accordance with Chapter V GDPR.

3. Spencer Stuart's Obligations

Spencer Stuart's Standards require the following with regard to processing Personal Data:

3.1 Personal Data is processed fairly and lawfully.

3.2 Data Subjects are informed (for example, in a data privacy notice or privacy statement) to explain how their data will be processed by Spencer Stuart to ensure fair and lawful processing.

3.3 Personal Data is processed on the basis of legitimate interest, or other legal grounds (such as consent) where required by applicable local legislation, provided that the processing of such information is not overridden by an Individual's own privacy interests, or their rights and freedoms as provided by law.

3.4 Personal Data is processed for lawful purposes associated with Spencer Stuart's business ("Purposes").

3.5 Personal Data is not processed in any manner incompatible with these Purposes.

3.6 Personal Data is always adequate, relevant, and limited to what is necessary in relation to the purposes for which the Personal Data is processed. If we intend to process Personal

Data for a purpose which is incompatible with the purpose for which the Personal Data was originally collected, we may only do so if such further processing is permitted by applicable law or we have the individual's consent. In assessing whether any processing is compatible with the purpose for which the personal data was originally collected, we take into account:

a. any link between the purposes for which the Personal Data was originally collected and the purposes of the intended further processing;

b. the context in which the Personal Data was collected, and in particular the reasonable expectations of the individuals whose Personal Data will be processed;

c. the nature of the Personal Data, in particular whether such information may constitute special categories of data;

d. the possible consequences of the intended further processing for the individuals concerned; and

e. the existence of any appropriate safeguards that we have implemented in both the original and intended further processing operations.

3.7 Special Categories of Data (e.g., personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) will only be processed only with the data subject's consent.

3.8 Personal Data is only used by Spencer Stuart and is not sold or shared for related or unrelated purposes to non-licensed third parties unless otherwise stated at the time of collection or as required by law.

3.9 Personal Data is processed and maintained in a manner that assures reasonable accuracy.

3.10 Personal Data that is inaccurate is corrected, updated, or deleted within a reasonable time of the discovery of the inaccuracy.

3.11 Personal Data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which Spencer Stuart processes the Personal Data.

3.12 Personal Data is protected by all necessary and appropriate protective measures – both technological and legal.

3.13 Personal Data will not be automatically processed in any manner which will have a significant effect on the data subject except where authorised by a law which also safeguards the data subject's legitimate interests; and

3.14 Personal Data will not be transferred to third parties without adequate protections in place unless an exception permitting such transfers, as found in European data protection laws, applies. Such protections include contractual terms imposed on the service provider that require it:

a. to act only on our instructions when processing that information, including with regard to international transfers of personal data;

b. ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c. to have in place appropriate technical and organizational security measures to safeguard the personal data;

d. Where it engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR;

e. to assist us in ensuring compliance with our obligations as a controller under applicable data protection laws, in particular with respect to reporting data security incidents and responding to requests from individuals to exercise their data protection rights;

f. to return or delete the personal data once it has completed its services; and

g. to make available to us, as Controller, all information necessary to demonstrate compliance with the obligations laid down in the GDPR and allow for and contribute to audits, including inspections, conducted by us or another auditor mandated by us.

3.15 Personal Data transferred outside the EEA, to processors or controllers not bound by these BCRs, is covered under a different appropriate safeguard, such as an adequacy decision, standard contractual clauses or otherwise that a data transfer derogation in line with Article 49 of GDPR applies and a Transfer Impact Assessment (as described in Section 2 above) has been conducted where necessary.

3.16 Spencer Stuart will implement appropriate technical and organisational measures as detailed in these Standards in order to comply with data protection principles. Such measures will ensure a level of security appropriate to the risk. These measures may include the following, as appropriate in light of the risk:

a. the pseudonymisation or encryption of Personal Data;

b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3.17 Spencer Stuart will maintain a written record of categories of all processing activities carried out. This confidential record of processing activities will be maintained in writing, including in electronic form, and be made available to SAs upon request. Activities likely to result in a high risk to the rights and freedoms of data subjects will be subject to a data protection impact assessment. When a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller, it will consult an SA.

a. Where a TIA indicates that processing would, in the absence of supplementary measures taken by us to mitigate the risk, result in a high risk to the rights of the data subject, the SA shall be consulted.

3.18 **Personal Data Breaches**: Spencer Stuart has policies, procedures, and protocols in place for managing and responding to personal data breaches, understood as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. All instances of suspected or known breaches where there may have been inappropriate access to, or an unauthorized disclosure of personal data must be reported immediately

to the Information Security team. All employees are required to follow our security instructions. As part of our incident response processes there are procedures for informing without undue delay, any personal data breaches to our crisis management team, which includes members of senior leadership, Data Privacy Officer (DPO), Information Security Officer (ISO), the liable BCR member, other Entities affected by the incident and relevant members of the Legal team of the incident and where required, notifying the supervisory authorities without undue delay, not later than 72 hours after becoming aware of the breach. In addition, where required, Spencer Stuart will notify individuals without undue delay where the breach is likely to cause significant risks to the rights and freedoms of individuals. There are also procedures for notifying other relevant bodies about breaches when legally required to do so in certain jurisdictions or when Spencer Stuart considers it appropriate. Spencer Stuart maintains a record of personal data breaches which includes details about the breach incident, the effects (if any) on individuals, Spencer Stuart or any other party, and remedial action necessary to resolve the breach. Spencer Stuart will make these records available to the relevant supervisory authority in accordance with applicable laws.

3.19 Spencer Stuart honours the rights of data subjects, as further detailed in Section 7, below.

3.20 All Entities must comply with and be able to demonstrate compliance with these Standards and applicable data privacy laws.

4. Purposes for Personal Data Processing

Spencer Stuart processes Personal Data only for the Purposes and in accordance with applicable law. Such Purposes include:

- **Executive, Board and Management Search Services**: Spencer Stuart processes Individual Personal Data in order to match individuals who may be qualified for a particular position with client organisations.

- **Leadership Advisory Services**: Spencer Stuart processes Individual Personal Data in order to evaluate individuals' ability to perform, fit and make an enduring impact in critical leadership roles, provide in-depth data and insights to inform selection decisions for senior leadership roles, coaching individuals and advise our clients in regard to team culture, performance and development.

- **Market Intelligence**: Spencer Stuart processes Individual Personal Data for research, benchmarking, and analytics in order to provide, improve and develop our services and intellectual capital and remain aligned with market standards for our industry. Additionally, Spencer Stuart processes Individual Personal Data to share intellectual capital and thought leadership it has published or for marketing our services and/or events.

- **Business Purposes**: Spencer Stuart processes Individual Personal Data for business purposes including, but not limited to, audit procedures, security processes, maintenance of systems and infrastructure, tests of our services, and other short-term uses.

- **Personnel Purposes**: Spencer Stuart processes Personal Data of personnel as necessary to comply with its legal obligations as an employer and to ensure the performance of its contractual obligations.

5. Security, Confidentiality and Compliance

Spencer Stuart will take all necessary and appropriate protective measures to prevent unauthorised access, loss, or damage to Personal Data and ensure any processing of Personal Data is done in accordance with these Standards, as well as maintaining compliance with these standards Those measures include:

- **Employee Contracts and Policies**: Spencer Stuart's policy is to keep all Personal Data confidential. All employees of Spencer Stuart are required to sign and abide by the following:
    - ***The Code of Conduct***: All employees of Spencer Stuart sign Spencer Stuart's Code of Conduct outlining the values and commandments of the company. The Code of Conduct requires strict adherence to the confidentiality and integrity of Personal Data.
    - ***Employment Contract***: All employees of Spencer Stuart sign employment contracts that contain robust confidentiality clauses.
    - ***Confidentiality Agreement***: In addition, all employees of Spencer Stuart are required to sign a separate and extensive confidentiality agreement.
- **Spencer Stuart Group Agreements**: All Spencer Stuart Entities have contractually agreed to implement appropriate security measures, including respecting these Standards, to protect Personal Data as mandated by Spencer Stuart.
- **Training**: In alignment with these BCRs, Spencer Stuart has instituted appropriate and up to date training focused exclusively on privacy training, our BCRs, and their application in the context of executive search and leadership consulting. Training is provided to employees that have permanent or regular access to personal data, who are involved in the collection of data or in the development of tools used to process personal data.
    - ***Orientation and Annual Refreshers***: All Spencer Stuart employees will participate in an introductory training session upon joining the firm and are required to complete annual refresher courses. These sessions cover key aspects of our BCRs, data protection principles, and their practical application in our day-to-day operations, including procedures for managing requests for access to personal data by public authorities.
    - ***Role-Specific Guidance***: The Data Protection Officer and the Legal team partner with HR and IT teams, who will receive additional, tailored guidance and direction as it relates to the handling of sensitive Personal Data. This focuses on the responsibilities and best practices specific to their roles, emphasizing the importance of vigilance and compliance in all data processing activities.
    - ***Access and Resources***: Comprehensive documentation on our BCRs, including relevant guidelines, procedures, and policies, will be made available on Spencer Stuart's corporate intranet. This ensures that all employees have unfettered access to vital information necessary for informed compliance.
    - ***New Employee Integration***: Integral to our onboarding process, new employees will be granted immediate access to all privacy-related training resources. They will be required to complete the foundational privacy training

program, ensuring they understand and can adhere to our data protection standards from their first day.

- ***Verification of Understanding***: Following the completion of any privacy training program, employees must pass a knowledge check. This certification process confirms their understanding and ability to apply our privacy standards effectively in their roles.

- ***Cyberbreach Training***: The Spencer Stuart Crisis Management Team that includes executive management conducts annual cybersecurity and breach tabletop exercise. The Board of Directors of the Spencer Stuart Group are informed of the results of the tabletop. These exercises are designed and facilitated by an external third party with expertise in mitigating cyberattacks.

- ***Continuous Improvement***: Reflecting our commitment to excellence and adaptation to evolving privacy landscapes, our privacy training programs will be regularly reviewed and updated. This task is undertaken in coordination with Spencer Stuart's leadership team and in consultation with its Legal and Privacy team, ensuring that training remains comprehensive, current, and effective. If required to do so, Spencer Stuart will provide the supervisory authorities with examples of our training program.

- **Access Security**: Personal Data is securely stored and can only be accessed via Spencer Stuart's proprietary software. Personal Data is only accessible by Spencer Stuart employees from Spencer Stuart computers and only through Spencer Stuart's private network. Access is continually monitored and restricted to employees of Spencer Stuart and is secured by appropriate physical, electronic, and managerial security procedures to prevent unauthorised access, loss, or damage to the Personal Data.

- **Contractor Obligations**: Contractors performing services for Spencer Stuart must undergo a due diligence procedure and execute a written service contract. Beyond business terms, these service contracts include confidentiality and security obligations and data protection provisions and provide enforcement mechanisms through all available legal remedies. Vendors with access to personal data are required to undergo a security assessment.

  Spencerstuart.com Safeguards: To safeguard all Personal Data that is submitted via spencerstuart.com, appropriate physical, electronic, and managerial security procedures have been put in place to prevent unauthorised access, maintain the accuracy of data and ensure proper use of information via spencerstuart.com. Our safeguards include sufficient protections to guard against any onward transfer of data to controllers or processors which are not part of the BCR.

- **Compliance with these BCRs**: No transfer shall be made to an Entity acting as an importer unless such Entity is effectively bound by these BCRs and can deliver compliance.

  - An Entity acting as importer shall promptly inform the exporter if it is unable to comply with these BCRs, for whatever reason
  - Where an importer is found to be in breach of these BCRs or is unable to comply with it, the Entity acting as an exporter shall suspend the transfer to such importer.

- An Entity acting as an importer should, at the choice of the exporter, immediately return or delete all personal data in its possession that has been transferred under these BCRs (including any copies thereof) if:
    - the exporter has suspended the transfer and compliance with these BCRs is not restored within a reasonable time, and in any event within one month of the suspension; or
    - the importer is in substantial or persistent breach of these BCRs; or
    - the importer fails to comply with a binding decision of a competent court or competent supervisory authority regarding its obligations under these BCRs.
- The importer should certify the deletion of the personal data to the exporter.
- Until all personal data is either deleted or returned, the importer shall continue to comply with the terms of these BCRs.
- In case of local/national laws in the country of the importer that prohibit the return or deletion of the transferred personal data, the importer shall warrant that it will continue to ensure compliance with these BCRs and will only process the personal data to the extent and for as long as required under the local/national laws of such third country.

6. Required Processing

In the event that a Spencer Stuart Entity is subject to a legal requirement arising in a country outside the EEA that is likely to have a substantial (adverse) effect on the guarantees provided by the Data Protection Standards and/or a Spencer Stuart Entity has reasons to believe that the applicable legislation prevents the company from fulfilling its obligations under the Standards, the Spencer Stuart Entity shall, without undue delay; (i) inform Spencer Stuart International Ireland Ltd. ("Spencer Stuart Ireland"), (ii) inform the relevant Privacy Officer as applicable, and (iii) report the existence of such a risk to the competent SA. In such a case, the Spencer Stuart Entity shall clearly inform the competent SA about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure. This includes any legally binding requests for disclosure of Personal Data by a law enforcement authority, state security body and any situations where Personal Data must be disclosed as a matter of law. However, there may be situations where the Spencer Stuart Entity is otherwise prohibited from notifying, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

If Spencer Stuart is prevented from being able to make the necessary notifications, the Spencer Stuart Entity shall use its best efforts to waive this prohibition to communicate as much information in as timely a manner as possible, and furthermore, demonstrate its compliance with this section of the Standards. In any case, the Spencer Stuart Entity will use its best efforts to resist lawfully, limit, or delay disclosure and ensure that it only provides the necessary Personal Data relevant to the request and will provide at regular intervals, as much information as possible to the corresponding exporter Entity. Spencer Stuart commits to refrain from undertaking disclosures that are massive, disproportionate, and indiscriminate in a manner that would go beyond what is necessary for a democratic society. If the Spencer Stuart Entity is unsuccessful in the above measures, despite exercising its best efforts, it shall, on an annual basis, provide the competent SA with general information concerning the requests (e.g., number of applications for disclosure, type of data requested, requester if possible, etc.).

7. Third-Party Beneficiary Rights of Access, Rectification, Objection, Restriction, and/or Deletion

Any individual may, at any time, in accordance with local law, contact Spencer Stuart and exercise their rights in respect to their data, including but not limited to those detailed below:

Right of Access to Personal Data:
An individual has the right to request access to their personal data which has been processed by us. When Spencer Stuart receives such a request, we will take reasonable steps to:

- identify the individual making the request;
- determine whether we are processing or have processed their personal data; and
- ask for certain information to help locate that data.

We will provide the individual with the following information:

- whether data is held and if so, its relevant purpose, together with an indication of the source of the data if known;
- the categories of personal data;
- the recipients of the data, including recipients located in countries outside the EEA and details of the appropriate safeguards in place for the transfer of their data to other countries; and
- how long the data will be retained or the retention criteria.

Spencer Stuart will provide a copy of this information within one month of receiving an individual's request, or within any specific period that may be required by local law in any country.

Notwithstanding any local laws or requirements, we may refuse to provide an individual with information where disclosure would reveal information about another individual. In this case, we will provide as much of the information as possible without revealing information about the other individual. It may be reasonable to provide the information without the other individual's agreement, or it may be necessary to obtain their consent to release the information.

Where we refuse to comply with a request, we will explain our reasons for doing so to the individual and inform them of their right to complain to a SA and/or seek judicial remedy within one month of receiving our refusal to comply with the request.

Right of Rectification:
An individual may request that Spencer Stuart rectify their personal data if the data is inaccurate or incomplete.

If the data is incorrect or incomplete, we will delete, correct, or amend the data. If the data is not incorrect or incomplete, we will inform the individual and explain their right to complain to a SA and/or to seek judicial remedy. We will keep a record that the individual considers the data to be inaccurate or incomplete.

If we have disclosed the data, we will inform the recipient of the request where feasible to do so. An individual may request information about the recipients from us.

Right to Data Erasure:
Spencer Stuart will abide by a request from an individual to erase their personal data under the following conditions:

- the personal data is no longer necessary for the purpose for which it was collected or otherwise processed;
- an individual withdraws their consent and there are no other legal grounds for processing;

- an individual objects to the processing and we have no overriding legitimate interests in continuing to process their data;
- the personal data is being unlawfully processed; or
- the data must be erased to comply with a legal obligation.

There are circumstances in which we can refuse an erasure request, including:

- exercising the right of freedom of expression and information;
- complying with a legal obligation as a data controller or for the performance of a public interest task or exercise of official authority;
- for public health reasons or for purposes in the public interest;
- for archiving purposes in the public interest, scientific research, historical research, or statistical purposes; or
- for the establishment, exercise, or defence of legal claims.

Within the legally required timeframe we will inform any recipients of the erasure request unless this would require a disproportionate effort. Where we have made the data public, we will take reasonable steps to inform other recipients to erase links, copies, or replicas.

Right to Restrict Processing:
Spencer Stuart will agree to restrict the processing of an individual's data when one of the following applies:

- Until the accuracy of the data can be verified where an individual contests its accuracy.
- The processing is unlawful and the individual requests a restriction of use rather than erasure of their data.
- We no longer need to process the personal data, but the individual requires the data to establish, exercise or defend a legal claim.
- In circumstances where an individual has objected to the processing and it must be considered whether our interests override those of the individual, where the processing was done on the basis of public or legitimate interest.

If there is a restriction on processing, we have the right to retain the data and we may continue to use the data for legitimate purposes. We will inform any recipients of the personal data about the restriction unless it is disproportionate to do so. If we lift the restriction on processing, the individual will be informed.

Please note: In addition, Spencer Stuart shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with this rule to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. We must inform the individual about those recipients if the individual requests it.

Right to Object to Processing:
An individual has the right to object to the processing of their data under certain circumstances. Spencer Stuart will abide by any valid request from an individual who objects to the processing of their data by us. In some cases, there may be grounds for continued processing where we can demonstrate a legitimate interest in the processing which overrides the rights of a data subject.

These rights, as well as any information on how an individual's data will be processed will be notified to the individual within a reasonable timeframe. The information provided will include:

- the identity and details of the data controller, or where applicable, its representative;

- the contact details of the designated privacy contact, or where applicable, Data Protection Officer;
- the purpose for which Spencer Stuart intends to use such data, including the legal basis for processing;
- the recipients or categories of recipients, if any; and
- where applicable, any relevant information about international transfers of the data.

Where Spencer Stuart has already provided this information, it will not continually be provided as part of each subsequent interaction with the individual, save where failure to do so would infringe the data subject's rights. With regards to determining the retention period for data, subjects can view the relevant criteria at https://www.spencerstuart.com/privacy-policy.

Right not to be subject to decisions based solely on automated processing, including profiling:
An individual has a right to not be subject to a decision based solely on automated processing, including profiling. If such request is made, we will ensure the individual is exempted from such processes, unless such decision is: (i) necessary for entering into, or performing, a contract between Spencer Stuart and that individual; (ii) authorized by applicable law (which, in the case of personal data about individuals in Europe, must be European Union or Member State law); or (iii) based on the individual's explicit consent. In the (i) and (iii) cases above, we must implement suitable measures to protect the individual's rights and freedoms and legitimate interests, including the right to obtain human intervention, to express his or her view and to contest the decision. We must never make automated individual decisions about individuals using their special categories of data unless they have given explicit consent or another lawful basis applies.

How To Exercise These Rights:
Such requests as detailed above can be made to any Spencer Stuart employee or via email to privacy@spencerstuart.com. All such requests will promptly be honoured by the Legal Department, and unless otherwise noted in the request, will apply to all forms of processing by Spencer Stuart. These Standards expressly confer rights on data subjects to enforce the Standards as third-party beneficiaries. Furthermore, the Standards expressly grant, to the data subjects, the right to judicial remedies and the right to obtain redress and, where appropriate, compensation in case of any breach of one of the Standards' enforceable elements subsequently outlined. Under the Standards, data subjects have the right not to be subject to decisions based solely on automated processing, including profiling.

8. Enforcement Rights and Mechanisms

The Spencer Stuart Group has appointed Spencer Stuart Ireland to accept responsibility for and take the necessary steps to remedy the actions of any member of the Spencer Stuart Group, including those members established outside the EEA. Spencer Stuart Ireland shall therefore be responsible for ensuring data subject's rights are enforced and in the event of any proven violations, pay compensation for any resulting material or non-material damages. For the avoidance of doubt, this procedure applies where Spencer Stuart is a data controller and to all Spencer Stuart entities which are signed up to Spencer Stuart's Binding Corporate Rules.

If an Individual wants to exercise any of the rights described in Section 7 or believes their Personal Data is being processed in contravention of these Standards, they can contact Spencer Stuart via email at privacy@spencerstuart.com or by mail with their request sent to Spencer Stuart, Attn: Legal Department, Block C, 2nd Floor Whitaker Court, Sir John Rogerson's Quay, Dublin, D02 W529, Ireland. As a department with an appropriate level of independence in the exercise of its functions, the Spencer Stuart Legal Department shall respond to the requesting individual without undue delay. If the request is justified, the Legal Department will instruct the relevant department or function to correct, complete, restrict or erase the data. Furthermore, Spencer Stuart shall resolve

such a request within thirty (30) days from the date of receipt of the access request. Spencer Stuart may extend the time limit by a further two months if the request is complex or if Spencer Stuart receives several requests from the same data subject. Individuals will be made aware of Spencer Stuart's delayed response time and the reasons why as soon as Spencer Stuart becomes aware of a delay.

There may be exceptions within applicable privacy/other laws where Spencer Stuart has legal grounds to reject or only partially comply with a request. For example:

- the information requested is subject to legal proceedings or is part of an ongoing law enforcement investigation and Spencer Stuart is prohibited from disclosing the information, or
- Spencer Stuart has received a request to erase an individual's information, but Spencer Stuart is obliged to retain the information in compliance with overriding legal requirements such as employment or tax law.

The Individual may also choose to bypass contacting Spencer Stuart and may lodge a complaint before the competent SA and enforce these Standards as a third-party beneficiary against Spencer Stuart Ireland, before the Irish courts, or the courts of the jurisdiction in which the Spencer Stuart Entity in the EEA responsible for exporting such data is established, or before the courts of the EEA jurisdiction where the data subject either has their habitual residence or their place of work, or before the courts of the EEA jurisdiction of the place of the alleged infringement in which case the individual may be represented by a not-for-profit body, organisation, or association if certain conditions as set out in the GDPR are met.

Where an Individual can demonstrate that they have suffered damage and can establish facts which show that it is likely that the damage has occurred because of a breach of these Standards, Spencer Stuart Ireland will have the burden of proof to demonstrate that a Spencer Stuart Entity is not liable for the breach or to show that no such breach took place.

As part of its review, the CPO may arrange to meet the parties to the dispute in an attempt to resolve it. If, due to the complexity of the dispute, a substantive response cannot be given within one (1) month of its escalation, the CPO will advise the complainant accordingly and provide a reasonable estimate for the timescale within which a response will be provided which will not exceed three (3) months from the date the dispute was escalated.

3.1.6. If the complaint is upheld, the CPO will arrange for any necessary steps to be taken as a consequence. If the complaint is rejected, the CPO will notify the individual within the timescales set out above.

9. Internal Oversight Procedures

Spencer Stuart ensures enforcement of these Standards through its Legal Department (including Data Protection Officers where required) who monitor the processing of Personal Data and conduct data protection compliance audits, which include all aspects of these Binding Corporate Rules, on a regular basis. It is not mandatory to monitor all aspects of the privacy program each time a Spencer Stuart entity member is audited, as long as all aspects of the Binding Corporate Rules are monitored at appropriate regular intervals for that entity. The Legal Department (including Data Protection Officers where required) is further responsible for investigating any claims related to data processing and may coordinate with the IT Department to analyse the scope of the alleged violation. In addition, employees will self-police their actions and the actions of peers regarding the processing of Personal Data. Employees are required to immediately report any violation to their direct superior who will notify and work with the Legal Department (including Data Protection Officer where relevant) to investigate the claim.

Audit Function:

Data protection audits shall cover all aspects of the BCRs and all related policies, procedures or guidelines, including methods of ensuring that corrective measures will take place. Different aspects of our auditing program address data privacy compliance. Audits will generally be carried out at regular bi-annual intervals but also by exception, where there is a particular need to conduct an audit outside of the regular schedule. Audits are planned by the Risk Committee of the Board and conducted by the Legal Department independent of its Data Protection Officer if there is a potential conflict of interest.

All Entities agree to be audited by the Supervisory Authorities if required to do so. During the audit, each Spencer Stuart Entity shall cooperate with the auditor and shall disclose to the auditors any and all information or documents as may be required for the accomplishment of the auditor's objectives, subject to compliance with local laws and regulations. The results of all the audits relating to the processing of personal data shall be made available to executive leadership, the Legal Department, the Data Protection Officer, the board of Spencer Stuart's ultimate parent company, and any other relevant Spencer Stuart function. Upon request, the results will be made available to supervisory authorities. Audit follow up procedures will include a corrective action plan based on the audit findings and procedures for ensuring the corrective action is implemented.

Data Protection Officer (DPO):

Spencer Stuart has appointed an individual who is responsible for compliance with applicable data protection laws and the BCRs. This individual reports directly to the Chief Legal Officer and executive leadership and can inform them if any questions or problems arise during the performance of their duties. The DPO does not have any tasks that could result in conflicts of interest. The DPO is responsible for:

- informing and advising Spencer Stuart employees who carry out processing of their obligations pursuant to applicable data protection laws and the BCRs;
- when the privacy team within the Legal Department conducts data protection impact assessments, offering support and guidance.
- monitoring compliance with data protection regulations, the policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff at a local level involved in processing operations, and the related audits;
- providing advice where requested as regards the data protection impact assessment and monitoring its performance;
- cooperating with the competent supervisory authority;
- handling local complains from data subjects;
- reporting major privacy issues to the competent supervisory authorities as well as on issues relating to processing, including prior consultation, and consulting, where appropriate, with regard to any other matter.

Spencer Stuart's DPO and the Legal Department's Privacy Team can be directly contacted at privacy@spencerstuart.com or by writing to Spencer Stuart Legal Department, Block C, 2nd Floor Whitaker Court, Sir John Rogerson's Quay, Dublin, D02 W529, Ireland.

10. Communication of Standards

These Standards will be published at www.spencerstuart.com/privacy as well as privately for Spencer Stuart employees on its intranet. Employees are trained to adhere to these Standards and to follow the appropriate protocol. Additionally, a copy of these Standards will be distributed to any Individual who requests one. Upon request, an Individual may also obtain a copy of the Intra-Group Agreement which binds the Spencer Stuart group of companies to these Standards and a current

list of such Entities by reporting to their contact at Spencer Stuart, to any Spencer Stuart employee, or via email to privacy@spencerstuart.com.

11. Modification of Standards

Spencer Stuart reserves the right to modify these Standards as needed in cooperation with the Data Protection Commission of Ireland. Where local law requires a higher standard for Personal Data it will take precedence over these Standards.

The Legal Department shall communicate any changes to the Standards without undue delay to all Spencer Stuart Entities. The changes will be promulgated throughout the Firm via an email announcement or a posting of the revised Data Protection Standards to the intranet and training in accordance with any legal requirements. Individuals will be informed going forward and have access to the updated Data Protection Standards at www.spencerstuart.com/privacy. Likewise, the Legal Department shall report any changes without undue delay to the relevant SAs, via the competent SA, with a brief explanation of the reasons justifying the update. Spencer Stuart may update the Standards, or the list of Spencer Stuart Entities bound by the Standards without reapplying for approval from the SA. The Legal Department commits to maintaining a fully updated list of the Entities bound by the Standards and keeping track of any updates to the rules and providing the necessary information to the data subjects or SA upon request. The Legal Department shall refrain from transferring any data to a new Entity under the Standards until the new Entity is effectively bound by, and entirely compliant to, the BCRs. If Spencer Stuart undertakes any change to the Standards, it shall report once a year to the relevant SAs, via the competent SA, with a brief explanation of the reasons justifying the update. Consequently, where such a modification may affect the level of protection afforded by the Standards or significantly affect the Standards, Spencer Stuart shall promptly communicate this fact to the relevant SA via the competent SA. Finally, Spencer Stuart commits to providing confirmation of its assets at each annual update to the competent SA, and remains responsible to keep the Spencer Stuart Entities up-to-date and in compliance with Article 47 GDPR and the EDPB recommendations.

12. Obligations to Data Protection Authorities

Spencer Stuart will cooperate and respond diligently and appropriately to all requests from data protection authorities located in the EEA regarding these Standards, including consenting to requests by a competent Data Protection Authority located in the EEA to audit and inspect Spencer Stuart's compliance with these Standards, including where necessary, on-site. Spencer Stuart will take into account the advice of such relevant EEA Data Protection Authorities on any issues related to the interpretation and application of Spencer Stuart's Data Protection Standards, and abide by decisions of these Data Protection Authorities on any issue related to these BCRs. Upon request, such Data Protection Authority located in the EEA shall receive a copy of any compliance audits conducted by Spencer Stuart regarding these Standards and Spencer Stuart will further comply with requests by the relevant EEA Data Protection Authorities for additional review of company-wide compliance. Spencer Stuart agrees to submit themselves to the jurisdiction of the courts of the relevant EEA Data Protection Authority in question. A current list of the Spencer Stuart companies bound by these Standards shall be provided, as required, to the Data Protection Authorities.

Appendix 1

Spencer Stuart Entities – Updated as of 1 June 2024

Please note that the email address for each of the following Entities is privacy@spencerstuart.com. Our Privacy inbox is handled and accessible by our global legal team by directing incoming emails to the appropriate regional legal team.

Exporters

Spencer Stuart International B.V. Company Number: 30118706	**Netherlands**
Spencer Stuart (Scandinavia) A.B. Company Number: AB 556271-2884	**Sweden**
SS Management Consulting GmbH Company Number: FN 58957 b	**Austria**
Spencer Stuart Start Austria GmbH Company Number: FN 506349g	**Austria**
Spencer Stuart Star Hungary Kft. odštěpný závod Company Number: 08055114	**Czech Republic**
Spencer Stuart & Associates B.V. Company Number: CH-112.805.382	**Netherlands**
Spencer Stuart Poland sp z.o.o. Company Number: KRS 58478	**Poland**
Spencer Stuart Star Poland sp. z.o.o. Company Number: 0000743861	**Poland**
Spencer Stuart & Associates GmbH **Company Number: HRB 7184**	**Germany**
Spencer Stuart Star Germany GmbH Company Number: HRB 254152	**Germany**
Spencer Stuart Star Hungary Kft. Company Number: 01-09-337809	**Hungary**
Spencer Stuart Italia S.R.L. Company Number: MI-1098093	**Italy**
Spencer Stuart International P/S Company Number: 32304761	**Denmark**
Spencer Stuart International ApS Company Number: 32304761	**Denmark**

Spencer Stuart S.A.S. Company Number: 672030574	**France**
Spencer Stuart Consejeros de Dirección S.A. Company Number: A-28/555910	**Spain**
Spencer Stuart Star Spain S.L.U. Company Number: 639392	**Spain**
Spencer Stuart Management Consultants N.V. Company Number: 0406-981-316	**Belgium**
Spencer Stuart International AS Company Number: 915692672	**Norway**
Spencer Stuart International Ireland Company Number: 565616	**Ireland**
Spencer Stuart Star Ireland Ltd. Company Number: 639392	**Ireland**
Merc Partners Ltd. Ireland Company Number: 326397	**Ireland**
Spencer Stuart PLC Company Number: 734766	**Ireland**

Importers

Spencer Stuart Switzerland AG Company Number: CHE-183.474.494	**Switzerland**
Spencer Stuart Management Consultancy Ltd. Company Number: 804608	**Turkey**
Spencer Stuart South Africa (Pty.) Ltd. Company Number: 1993/01515/07	**South Africa**
Spencer Stuart India (Private) Ltd. Company Number: U74140MH2005PTC157008	**India**
LDHR Services India Limited Company Number: AAO-8767	**India**
Spencer Stuart & Associates (Singapore) PTE Limited	**Singapore**

Company Number: 19-9603520-M	
Spencer Stuart Star Singapore PTE Ltd. Company Number: 201906833C	**Singapore**
Spencer Stuart (Middle East) Ltd. Company Number: CL0450	**U.A.E.**
Spencer Stuart Star Consulting (DIFC) Limited Company Number: CL 3219	**U.A.E.**
Spencer Stuart & Associates Ltd. Company Number: 20/04792780	**Hong Kong**
Spencer Stuart Professional Consulting (Beijing) Co., Ltd. Company Number: 9111010579755101XY	**P.R.C. Beijing**
Beijing Branch of Spencer Stuart Star Enterprise Management (Shanghai) Co., Ltd. Company Number: 9111010MA01KBTU7F	**P.R.C. Beijing**
Spencer Stuart Human Resources Consultancy (Shanghai) Co., Ltd. Company Number: 310103681008242 913100006810082426	**P.R.C. Shanghai**
Spencer Stuart Star Enterprise Management (Shanghai) Co., Ltd. Company Number: 91310000MA1FPEAJ61	**P.R.C. Shanghai**
Esaress Australia Pty, Ltd. Company Number: ABN 12000824313	**Australia**
Spencer Stuart Star Australia Pty, Ltd. Company Number: 2 163 1522 408	**Australia**
Spencer Stuart Star Australia Pty. Ltd. Company Number: 7511596	**New Zealand**
Spencer Stuart Star Malaysia SDN. BHD. Company Number: 1315772-U	**Malaysia**
Spencer Stuart Star (Thailand) Co., Ltd. Company Number: 0105562086530	**Thailand**
Kincentric (Thailand) Co., Ltd. Company Number: 0105556000394	**Thailand**
Spencer Stuart Japan Ltd. Company Number: 69-172-7291	**Japan**
Spencer Stuart Star Japan GK Company Number: 0104-03-020407	**Japan**
Spencer Stuart & Associates (Canada) Ltd.	**Canada**

Company Number: 768237-9	
Spencer Stuart Star Canada Inc. Company Number: 11223976-7	**Canada**
Esaress International Group, Inc. Company Number: 0098663	**U.S.**
Spencer Stuart Star USA Inc. Company Number: 4229669	**U.S. & Puerto Rico**
SSI (U.S.) Inc. Company Number: 2138518	**U.S.**
Spencer Stuart S.de R.L. de C.V. Company Number: SST000524L57	**Mexico**
Spencer Stuart Star Management Mexico S. de R.L. de C.V. Company Number: SSS190315KP9	**Mexico**
Spencer Stuart Star Management Mexico, S. De R. L. De C.V. Sucursal Company Number: 03114395	**Colombia**
Spencer Stuart International Ltda. Company Number: 21480	**Chile**
Spencer Stuart Star Chile SpA Company Number: 59.282.240-7	**Chile**
Spencer Stuart Consultores Gerenciais Ltda. Company Number: 35219327768	**Brazil**
Spencer Stuart Star Consultoria em Gestao Empresarial Brasil Ltda. Company Number: 190006752941	**Brazil**
Spencer Stuart Argentina S.A. Company Number: 10841	**Argentina**
Spencer Stuart Andina S.A.S. Company Number: 67203057400038	**Colombia**
LLC Spencer Stuart International Company Number: 1137746734905	**Russia**
Spencer Stuart & Associates Ltd. Company Number: 703962	**U.K.**
Spencer Stuart Star UK Ltd. Company Number: 11805666	**U.K.**
Spencer Stuart Star Saudi Ltd. Company Number: 1010625503	**Saudi Arabia**

Spencer Stuart Peru SAC **Peru**
Company Number: 1158955

Appendix 2 - Categories of individuals, categories of personal data and processing, purposes, recipients, countries

These tables set out the types of individuals we may process personal data about, the categories of personal data we may process about them, and the purposes for which we process personal information. These tables are intended to be a generic summary. It does not mean we process this data about all these types of individuals. Our data privacy notices and data privacy statements are where we provide specific information to individuals, for example, our privacy statement on the Spencer Stuart website.

Candidates, Assessment Participant (Participant), Referees

Type	Explanation
Exporters of Personal Data described in this section	Spencer Stuart Entities located in Europe (Appendix 1: Exporting Entities)
Importers of Personal Data described in this section	Spencer Stuart Entities located outside of Europe (Appendix 1: Importing Entities)
Categories of Data Subjects	• Prospective executive Candidates ("Candidates") • Candidate Referrals • Client employees undergoing an assessment ("Participants")
Categories of Personal Data transferred	• Contact information (name, e-mail address, home address, telephone number); • Applications, transcripts, cover letters, interview notes, and resumes; • Career and education history; • Language skills; • Immigration, right-to-work and residence status; • References; • Job-related information, such as years of service, work location, work record, and contracts; • Individual capabilities and preferences; • Professional views and opinions; • Recruitment and performance-related data, such as objectives, ratings, comments, feedback results, work equipment, career and succession planning, skills and competencies, appraisals, performance reviews, performance improvement plans and related correspondence, and other work-related qualifications; • Photographs, audio and/or video recordings, such as those related to coaching; • Information needed for compliance and risk management, such as background check reports, and security data; • Payroll and payment or benefits-related information, such as salary, bonus, pension, allowances, reimbursement records; • references and feedback, and connection to Candidates
Categories of Special	• Equal opportunities monitoring and sensitive information where required by law, such as racial or ethnic origin,

Personal Data transferred	membership of political parties or trade unions, and general health status such as medical statements. • Government-issued identification numbers, such as national ID or social security number; • Identification data (civil/marital status, gender, nationality, date of birth);
Type of processing and purpose	• providing our Services • maintaining our business relationship, including contacting these individuals about an assignment, verifying profile details, identifying, assessing and evaluating individuals, and/or presenting insights, analysis or reports to Clients. • Conducting a press check or background check, including; verification of educational or professional credentials; • Supporting and improving our business operations (e.g. interview transcription (if applicable), audit procedures, security processes, document storage, maintenance of our systems and infrastructure, data analytics, benchmarking, statistics, creating knowledge pieces, determining the effectiveness of our Services); • Sharing marketing and promotional materials (e.g., intellectual capital, thought leadership pieces, etc.); • Inviting candidates to industry and/or role-specific event (e.g., forum, charity event, etc.); • Working with partners, sponsors and vendors • maintaining business records, including those related to our Services; and • Responding to requests from law enforcement or government authorities where necessary to comply with applicable law, including to a subpoena or court order or discovery request, and to otherwise satisfy legal and regulatory obligations
Locations where Personal Data is processed in this section	Personal data is processed at all Spencer Stuart Entity locations listed in Appendix 1.
Lawful bases for processing of Personal Data described in this section	Processing is necessary for the legitimate interests pursued by the controller: • providing our Services • maintaining our business relationship, including contacting these individuals about an assignment, verifying profile details, identifying, assessing and evaluating individuals, and/or presenting insights, analysis or reports to Clients. • Supporting and improving our business operations (e.g. interview transcription (if applicable), audit procedures, security processes, document storage, maintenance of our systems and infrastructure, data analytics, benchmarking, statistics, creating knowledge pieces, determining the effectiveness of our Services);

	• Sharing marketing and promotional materials (e.g., intellectual capital, thought leadership pieces, etc.); • Inviting candidates to industry and/or role-specific event (e.g., forum, charity event, etc.); • Working with partners, sponsors and vendors, including third-party travel agencies; • maintaining business records, including those related to our Services; and Processing is necessary to a legal obligation to which the controller is subject: • Responding to requests from law enforcement or government authorities where necessary to comply with applicable law, including to a subpoena or court order or discovery request, and to otherwise satisfy legal and regulatory obligations Processing of special data is based on explicit consent provided by the data subject for one or more specific purposes • Conducting a press check or background check, including; verification of educational or professional credentials; Other exemptions that allow for the processing of special categories of data include: • Processing is necessary for employment, social security, and social protection obligations/rights as authorized by law or collective agreement. • Processing of data manifestly made public by the data subject. Necessary for the establishment, exercise, or defense of legal claims or judicial capacity actions.

Client Personal Data

Type	Explanation
Exporters of Personal Data described in this section	Spencer Stuart Entities located in Europe (Appendix 1: Exporting Entities)
Importers of Personal Data described in this section	Spencer Stuart Entities located outside of Europe (Appendix 1: Importing Entities)
Categories of Data Subjects	• Individual contacts, including employees, officers, agents and consultants of former, current and prospective corporate customers • Website visitors' data and prospects' data
Categories of Personal Data transferred	• Name • Associated company/employer • Spencer Stuart Client Portal account login details

	• Job title/role • Language/Preferred language for communication purposes • Phone number • Physical address • Email address • Country of residence • Nationality • Data related to previous interactions • Financial details, including credit card and bank account details • Information received relating to regulatory monitoring and reporting obligations • Customer records (engagement history, after services surveys, beta participation) • Website interactions and other event-related data (interest and/or attendance at a conference or webinar) • Usage data (username, IP address, general location information, communications metadata, log files data, usage information)
Categories of Special Personal Data transferred	n/a
Type of processing and purpose	• Managing relationships with actual and prospective corporate customers; • Administering webinars, conferences and other events • Complying with applicable legal obligations, including responding to a subpoena, court order, or discovery request and complying with "Know Your Client" obligations; • Providing, optimizing and maintaining services purchased or requested; • Storing input and opinions on prospective candidates • Managing customer accounts, including invoicing, management of payments, related accounting and tax administration (includes financial accounting, invoices and management of payments and open items (e.g., accounts payable and accounts receivable)); • Managing quality assurance and customer service and support activities; • Detecting, preventing and investigating security incidents, fraud, spam and other abuse or misuse of Client Portal; and
Locations where Personal Data is processed in this section	Personal data is processed at all Spencer Stuart Entity locations listed in Appendix 1.
Lawful bases for processing of Personal	Processing is necessary for the legitimate interests pursued by the controller: • Managing relationships with actual and prospective corporate customers;

Data described in this section	• Administering webinars, conferences and other events • Providing, optimizing and maintaining products and services purchased or requested • Detecting, preventing and investigating security incidents, fraud, spam and other abuse or misuse of Spencer Stuart Client Portal; Processing is necessary to a legal obligation to which the controller is subject: • Complying with applicable legal obligations, including responding to a subpoena, court order, or discovery request and complying with "Know Your Client" obligations; • Identity verification, necessarily processed in order to receive telephone number assignments or otherwise provide services Processing is necessary to the performance of a contract to which the controller is a party: • Managing customer accounts, including invoicing, management of payments, related accounting and tax administration (includes financial accounting, invoices and management of payments and open items (e.g., accounts payable and accounts receivable)); • Managing quality assurance and customer service and support activities;

Please note that these Standards do not apply to any Personal Data that has been anonymised and used in aggregate form such as compiling industry and employment statistics where such data does not involve personal identifying information and individuals are not able to be identified from it.