BEST PRACTICES FOR DATA PROTECTION

AESC

PURPOSE OF THESE BEST PRACTICE GUIDELINES

AESC is the exclusive global association representing only the highest quality firms in our profession worldwide. After meeting our rigorous membership criteria, our members agree to abide by the AESC Code of Professional Practice. By virtue of selecting an AESC Member, clients can be secure in their choice of consulting firm and can reap the benefits that only a trusted advisor can deliver.

AESC Members always respect any confidential information entrusted to them by clients and candidates. Each of our members respect the confidence placed upon them. These Best Practices improve transparency and accountability, provide some level of mitigation against enforcement actions, and improve AESC member firm standards by establishing best practices.

We encourage the adoption and use of a consistent set of privacy standards for the protection of personal data in the context of executive search and leadership consulting services, with the aim of improving the protection afforded to individuals and fostering trust in the profession as a whole.

Only AESC Members can announce their commitment to these Best Practices. Under no circumstances may any organization that is not an AESC Member Firm use these Best Practices or claim adherence to these guidelines. These guidelines are the intellectual property of AESC.

SCOPE OF THESE GUIDELINES

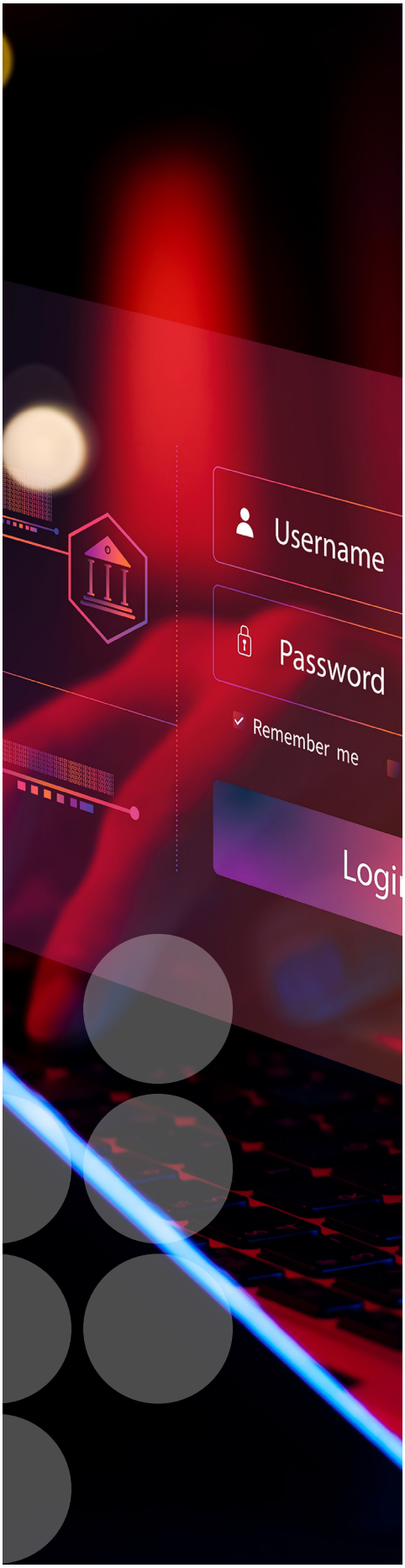
AESC Data Protection Guidelines are designed specifically to cover:

- **CLIENTS:** any individual managing or involved in the hiring process for a Client**;**
- **CANDIDATES:** any candidate, or potential candidate, for a position with a Client;
- **PARTICIPANTS:** any individual who participates in any assessments provided as part of any Executive Search or Leadership Advisory Services; and
- **SOURCES:** any person that provides any view or opinion regarding the qualities or abilities of any Candidate or Participant, for any purpose, including but not limited to the suitability of a Candidate or Participant for a particular role with a Client.

Member Firms may also process other personal data that doesn't fall within these categories, for example, a Member Firm is likely to process the personal data of its own Personnel or of individuals working for suppliers. While not within the scope of these Guidelines, applicable data protection laws continue to apply to the processing of personal data of individuals who fall outside the scope of these Best Practice Guidelines.

COLLECTION OF RELEVANT PERSONAL DATA

Member Firms may collect or obtain Relevant Personal Data in a variety of ways. While conducting recruiting assignments for Clients, a Member Firm may proactively contact Candidates in its research and networking efforts.



While providing Leadership Advisory Services, Member Firms may receive Relevant Personal Data from the Client that commissioned these services.

PRINCIPLES AND PURPOSES OF PROCESSING

Member Firms, acting as a controller, shall only process Relevant Personal Data in accordance with the following principles:

- Relevant Personal Data shall be processed in a fair, lawful and transparent manner, in accordance with these Best Practice Guidelines and applicable data protection laws.
- Relevant Personal Data shall only be collected and further processed for one or more specified purposes, and shall not be processed for further, incompatible, purposes.
- Each Member Firm shall ensure that it has a legal basis, in accordance with applicable data protection laws, for processing Relevant Personal Data.
- Relevant Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are being processed.
- Member Firms shall take reasonable measures to ensure, as far as is practicable, that Relevant Personal Data that they process are kept accurate and up-to-date.
- Relevant Personal Data shall not be retained in an identifiable format for longer than is necessary in connection with the purposes for which they are being processed.
- Member Firms shall ensure appropriate security for Relevant Personal Data.
- Member Firms shall retain sufficient records to demonstrate compliance with these Best Practice Guidelines, and applicable laws relating to the processing of Relevant Personal Data.

OBLIGATION TO PROVIDE NOTICE

Member Firms shall ensure that they provide a public-facing privacy notice that is made readily available. This notice must be concise, transparent, intelligible and easily accessible using clear and plain language.

Where the legal basis for the processing of Relevant Personal Data is legitimate interests, AESC members must provide a clear explanation of the legitimate interests pursued by the Member Firm.

APPOINTMENT OF PROCESSORS

Member Firms shall only engage processors that provide sufficient guarantees to implement appropriate technical and organizational measures

in such a manner that processing of Relevant Personal Data will meet the requirements of these Best Practice Guidelines and applicable Privacy Laws.

DISCLOSURE OF RELEVANT PERSONAL DATA

Member Firm controller entities may disclose Relevant Personal Data to their own authorized Personnel to the extent that those Personnel have a legitimate business reason to process those Relevant Personal Data.

A Member Firm may disclose Relevant Personal Data to processors and third parties including other entities within their organization and with clients. When the AESC member firm discloses information to a client, the Member firm does so as a controller not as a processor.

ELECTRONIC DIRECT MARKETING

It is likely that Member Firms will engage in electronic direct marketing to Relevant Data Subjects from time to time. When done, it is important to comply with the requirements of applicable law regarding electronic direct marketing to ensure that there is a valid legal basis for doing so and that provision is made to opt out or unsubscribe from any marketing lists upon request.

USE OF ARTIFICIAL INTELLIGENCE

In guiding Member Firms' adoption of AI, these Best Practices Guidelines recommend that any AI technology used should maintain the Member Firm's ethical standards, Candidate privacy protections, Client confidentiality, and uphold the integrity of its processes. Member Firms must:

- Implement AI responsibly and in accordance with applicable law;
- Ensure AI decisions are fair and transparent; and
- Preserve human judgment in the decision-making process, ensuring that AI supports rather than replaces the nuanced expertise of search professionals.

RIGHTS OF RELEVANT DATA SUBJECTS

Relevant Data Subjects (i.e. candidates, participants and sources) have rights guaranteed by law in many jurisdictions in which Member Firms operate. Accordingly, Member Firms shall give effect to the following rights:

- Opt-outs from electronic direct marketing Access to Relevant Personal Data
- Correcting errors or inaccuracies in Relevant Personal Data
- Erasure, restriction of processing and objections to processing
- Data portability
- Withdrawal of consent Complaints to Data Protection Authorities

INTERNATIONAL DATA TRANSFERS

Member Firms recognize that applicable data protection laws in many of the jurisdictions in which they operate may restrict international transfers of Relevant Personal Data. Member Firms should seek to rely on these legal grounds for transferring Relevant Personal Data in the order in which they are set out above.

SECURITY AND CONFIDENTIALITY OF RELEVANT PERSONAL DATA

Member Firms should ensure that they:

- implement appropriate technical and organizational security measures to protect Relevant Personal Data;
- keep Relevant Personal Data confidential at all times;
- anonymize or pseudonymize Relevant Personal Data as appropriate, to limit the risk of harm to Relevant Data Subjects;
- regularly review the risks posed to Relevant Personal Data by the Member Firm's processing activities; and
- implement any specific security measures or standards required by applicable law or best practice.

DATA RETENTION

Member Firms shall retain Relevant Personal Data only for as long as those data are needed in connection with the purposes for which they are processed plus the applicable limitation period which considers:

- Duration of the relationship
- Applicable limitation period
- Requirements of Engagement Agreement

ABOUT THE ASSOCIATION OF EXECUTIVE SEARCH AND LEADERSHIP CONSULTANTS

Since 1959, AESC has set the quality standards for the executive search and leadership consulting profession. AESC Members represent 16,000+ trusted professionals in 1,200+ offices, spanning 70+ countries. AESC Members are recognized experts providing consulting services in the areas of leaders, teams and culture to the world's leading organizations. They leverage their access and expertise to place more than 100,000 executives each year in board of directors and C-level positions across industry sectors. Dedicated to strengthening leadership together, AESC and its members share a deep commitment to the highest quality standards in executive search and leadership consulting—for the benefit of clients and the profession. We Shape. Connect. Educate. Innovate. Learn more about us at aesc.org For AESC's career services, visit bluesteps.com

AESC | *Strengthening Leadership Together*