

July 2020

HUMAN RESOURCES PRIVACY POLICY (“Privacy Policy”)

Daniel J. Edelman Holdings, Inc. and its affiliated companies worldwide, which at the time of the Privacy Policy include Daniel J. Edelman, Inc., StrategyOne, Inc. d/b/a Edelman Intelligence, Zeno Group, Inc., Assembly Media, Inc., Matter, Inc., United Entertainment Group Holdings, LLC, Edible, Inc., Edelman Miami Latin America Corp., The H & W Group, Inc. d/b/a SaluTem, The R Group Public Relations Company, Inc. d/b/a Revere, First & 42nd, Inc., and all operating companies and divisions, including such divisions as First At Edifi, BioScience Communications and DJEScience, under the Edelman family of companies (hereinafter referred to as either, “DJEH”, “Company”, “We”, “Us” or “Our”) is an Equal Employment Opportunity/Affirmative Action Employer. The Company adheres to a policy of making all employment decisions without regard to race, color, religion, national origin, age, disability, veteran status, citizenship or any other protected classification which may be applicable under the law of the particular state or locality in which you are employed or applying for employment with the Company. Company will make reasonable accommodation for disabled persons.

Company is committed to protecting the privacy of personal data you may provide Us or that We generate or receive as needed for the Company to perform legitimate Human Resource functions (“HR”) purposes (including information collected pre-employment, from new hires, and from prospective applicants). We believe it is important for you to know how We treat your personal data.

We will comply with all data protection laws in relation to your personal data. These laws say that the personal data We hold about you must be:

- a. Used lawfully, fairly and in a transparent way.
- b. Collected only for valid purposes that We have clearly explained to you and not used in any way that is incompatible with those purposes.
- c. Relevant to the purposes We have told you about and limited only to those purposes.
- d. Accurate and kept up to date.
- e. Kept only as long as necessary for the purposes We have told you about.
- f. Kept securely.

1. What personal data does Company collect about me?

During your employment or application for employment, the Company may collect (in both paper or electronic format) and use personal data about you as needed for HR Purposes (as defined below) where this is allowed by applicable law. Depending on the business need and in accordance with applicable law, such personal data may include but is not limited to: personal contact details, emergency contact details, next of kin and beneficiary information, employment history, employment identification number, government issued identification number, salary and benefits information, job performance information, and other information about you. It could include information that is deemed sensitive or special category personal data (e.g. race, ethnicity, physical or mental health, participation as part of certain affinity groups) under certain

data privacy laws, information about your use of Company resources, administrative information such as your bank account number (e.g. for direct deposit), personal contact details and government issued identification numbers of emergency contacts/beneficiaries, pictures of self and others, travel and travel reimbursement information, and background check information.

Please note that under certain circumstances our clients request background checks relating to employees who work on their premises or their accounts. Under such circumstances, the Company has a legitimate interest in performing such background checks, and they are only performed in accordance with applicable law and in a confidential manner designed to protect the privacy interests of the employee. The results of the background check are not disclosed to the client, and the employee is also given the opportunity to object in advance of the background check in which case it will not be carried out.

2. What does Company do with the personal data collected about an employee?

We will only use your personal data when the law allows us to. Most commonly, We will use your personal data in the following circumstances:

- a. Where We need to perform your employment contract or any other agreement We have with you.
- b. Where We need to comply with a legal obligation.
- c. To defend the legal rights of an individual, Company, its service providers or clients or to obtain legal advice on behalf of Company or its service providers.
- d. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests. Instances where We may process your personal data on this basis are described below.
- e. Where you give your consent to processing (e.g. in an event, affinity group such as Edelman Equal, activity, or contest).

We may also use your personal data in the following situations:

- a. Where We need to protect your interests (or someone else's interests).
- b. Where necessary in the public interest.

Company and its service providers may use/process your personal data for business purposes related to your application for employment, your role and function in the Company, and for human resources management, including but not limited to: complying with legal requirements; recruitment and/or consideration for employment positions within Company; human resources administration, general business organization and governance purposes, and to consider additional employment opportunities; performance management; payroll; training; business continuity; administration of compensation and benefit programs; and facilitating business transactions protecting the Company, its employees or the public against injury, theft, legal liability, fraud, abuse or other misconduct (“**HR Purposes**”).

We may also process your personal data in connection with a lawful request by public authorities, such as a court order, subpoena, government investigation, or other request to meet national security or law enforcement requirements.

We may also share personal data with clients upon request and/or use it for Company branding or marketing purposes, such as listing key employees on our website or social channels. In these instances, the Company has a legitimate interest in communicating such information, for instance regarding key employees' areas of responsibility, expertise and specialties. If you have questions or concerns about such use of your personal information or wish to opt-out of such use, contact the HR Contact noted below.

We may share your personal data with other entities within the Edelman group where this is in accordance with data protection law.

We may process special categories of your personal data in the following circumstances:

- a. with your explicit written consent;
- b. where we need to carry out our legal obligations and in line with this Privacy Policy;
- c. where it is needed in the public interest, such as for equal opportunities monitoring in line with this Privacy Policy.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Note that we may use a number of manual and automated systems/processes to monitor the activities of our employees in the event of suspected inappropriate activities or on a periodic basis in order to ensure ongoing compliance (as permitted by local law), including but not limited to email monitoring, Internet monitoring and video surveillance in and around our premises in order to: prevent and detect crime; protect the health and safety of employees, contingent workers, and visitors on site; manage and protect Company property (including our computer systems and confidential information) and that of employees, contingent workers, and visitors; and where applicable, for quality assurance purposes.

3. With whom does Company share the information?

We only share your personal data where this is permitted by applicable law, including where this is necessary to perform a contract with you or for our legitimate interests or the legitimate interests of a third party and these are not overridden by your fundamental rights and freedoms.

Your personal data is shared only within the Company, its subsidiaries and affiliates (and any other current or future subsidiaries or affiliates) and all service providers who have a need to know and/or process the personal data for the purposes set forth in this Privacy Policy.

In some instances, this may require that your personal data be transferred to, processed, and stored on a cloud and/or central servers in the United States or other locations or sent to

individuals in the United States or elsewhere. The laws regarding data privacy in the United States and other countries outside the European Union may not provide the same degree of protection for the rights and freedoms of individuals than do the laws which apply within the EU. Transfers of personal data from the EU will be made in accordance with applicable law. In addition, your personal information will be processed in accordance with this Privacy Policy no matter where it is transferred and processed.

Company does not sell, rent or loan any personal data regarding employees to unaffiliated third parties who are not service providers for or clients of the Company, and will only transfer, or otherwise disclose any personal data of employees to third parties as set forth in this Privacy Policy.

Because of the nature of electronic mail and business communications, as a matter of course, business contact information is regularly provided to existing and prospective clients, service providers and/or business partners. Also, since We are a client focused organization and our clients and prospective clients often request information regarding the work experience of team members, resumes and relevant business information regarding individual employees' experience may be provided to existing and prospective clients in order to evaluate Company's and team members' capabilities. These disclosures will only be when in the legitimate interests of the Company or otherwise permitted by law.

Company complies with the Privacy Shield Principles for all onward transfers of personal data from the EU, including the onward transfer liability provisions. When it is necessary to provide your personal information to service providers, it is done under a contract which requires the companies to, among other things, use the information only for the limited purposes for which it is provided to them in providing services to Company, not to transfer the information to another party without Company approval, and to agree to hold the information securely and confidentially in accordance with this Privacy Policy, applicable law and the Privacy Shield privacy principles.

If you have any question regarding whether the intended use of your personal data is permitted (including for the Company's legitimate business interests), contact the Company's compliance or privacy teams at Compliance@djeholdings.com.

In addition to adhering to this Privacy Policy and other policies and procedures regarding the privacy of your personal data that Company has in place, when your personal data is transferred from the EU to Company or other entity in another country, we require the recipient entity to enter into a contract regarding the use and processing of that information which incorporates certain standard contractual clauses approved by the Commission of the European Union.

From time to time, Company may make third party activities, events or applications available to you that are managed by third parties not acting as vendors to Company. These third parties (such as social media platforms or other company websites and applications) are responsible for their own privacy practices. If you provide any such third party with your personal data be sure to read the privacy policies, supplemental notices, and settings of all websites or platforms that you visit so you can understand their privacy practices and your options. The Company is not responsible for any personal data that you give to any such third party.

Company also may transfer your personal data to other third-party controllers such as payroll providers, benefit administrators, etc. Company requires third-party controllers to whom it shares or discloses your personal data to contractually agree to process personal data for limited and specified purposes, provide the same level of protection for Personal Data as is required by the Privacy Shield Principles, and notify us and cease processing personal data (or take other reasonable and appropriate remedial steps) if it cannot meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles.

4. Your rights in relation to your personal data?

You have the right to make a complaint in relation to our processing of your personal data to the relevant authorities for your country.

You have rights to obtain a copy of your personal data and in certain situations to obtain correction, erasure and restriction of processing of your personal data. You have a right of data portability. Where processing is based on your consent you have a right to withdraw this at any time.

You are able to opt-out of our processing of your personal data in relation to direct marketing or where we process on the basis that processing is necessary for our or a third party's legitimate interests unless we have compelling legitimate grounds to continue. If you wish to exercise any of these rights, then please notify the HR contact noted below. We will promptly evaluate and respond to your request. Please note, however, that certain personal data may be exempt from such access, modification or deletion rights pursuant to applicable data protection laws.

5. How does Company protect the security of my personal data?

Company uses and/or requires service providers to use administrative, technical, physical and organizational security measures (such as encryption and access controls) which are designed to protect your personal data 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. We safeguard personal data according to established security standards, and periodically assess our methods of protecting information.

If you should become aware of any known or suspected incidents of unauthorized access to, use of or disclosure of any personal data (including without limitation any personal data relating to you, any other employee of the Company or any of the Company's clients), you should report them immediately to the following email address: security@edelman.com. We will investigate all reported incidents.

6. How does the Company assess and audit its own compliance?

As Company's business and technology transforms, so does our privacy ecosystem. Company conducts compliance audits of its privacy practices to verify adherence to this Privacy Policy. All reported breaches or potential breaches will be investigated by appropriate personnel of Company, who will take such action as deemed appropriate based on the results of the investigation. We are open to feedback--see contact information below.

7. Does Company make changes to this Privacy Policy and how are you notified?

We may update this Privacy Policy from time to time. Check the “last updated” date at the top of this Privacy Policy to see the last time it was changed.

If we decide to make changes to this Privacy Policy, we will update this Privacy Policy with the new effective date. If the change is material, we will send an email and/or other notice to effected individuals.

8. How do I contact the Company with questions or concerns?

If you have any further questions or concerns regarding this Privacy Policy and/or the use of your personal data, please email the HR contact noted below. Company will investigate and attempt to resolve complaints and disputes regarding use and disclosure of personal data in accordance with this Privacy Policy, applicable law and any other Company policy. In addition to such investigations, we monitor adherence to this Privacy Policy and investigate suspected infractions. Any employee that is determined to be in violation of this Privacy Policy or misuses personal data will be subject to disciplinary action, up to and including termination where allowable by applicable law.

Notice to California Residents- California Privacy Rights:

While the Company provides comparable rights to all personnel with respect to their personal data, California law specifically requires that we provide notice to California residents that they may request from us information concerning: the categories of information we have collected; the categories of sources from which the personal information is collected; the purpose for which we collect or sell the personal information; the categories of third parties with whom we share personal information; and the specific pieces of personal information we have collected. We will not discriminate against an individual for exercising any of these rights.

If you are a California resident and would like to make such a request, please submit your request in writing to Compliance@djeholdings.com or by using our [CCPA Request Form \[forms.office.com\]](https://forms.office.com).

9. Privacy Shield

Company has self-certified with the U.S. Department of Commerce regarding the collection, use, and retention of personal data from European Union member countries in connection with the Privacy Shield Principles as part of the Privacy Shield program. To learn more about the Privacy Shield program, and to view Company’s certification, please visit <http://www.privacyshield.gov>.

As personal data collected and processed under this Privacy Policy is considered human resources data under the Privacy Shield Framework, Company has agreed to cooperate in investigations by, and comply with the advice of, the appropriate EU data protection authorities (“DPA”) in managing any dispute. Further, Company is also subject to the applicable investigatory and enforcement powers of the U.S. Federal Trade Commission. If you have questions or complaints regarding the use or disclosure of personal data in compliance with the principles of this Privacy Policy, you should contact Company first at the HR Contact noted below. If contacting Company does not resolve your concern or complaint, you may raise your

complaint with the relevant DPA where you live or work (see http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm for contact information) or other applicable regulator. As further explained in the Privacy Shield Framework Annex I, a binding arbitration option is available in the event that residual complaints related to EU compliance are not resolved by any other means.

10. General

This Privacy Policy is governed by the laws of the United States and the state of Illinois unless otherwise specified under applicable law.

This Privacy Policy does not create or confer upon any individual any rights or impose upon Company any rights or obligations outside of, or in addition to, any rights or obligations imposed by the privacy laws applicable to such individual's personal data. Should there be, in a specific case, any inconsistency between this Privacy Policy and such privacy laws, this Privacy Policy shall be interpreted, in respect of that case, to give effect to, and comply with, such privacy laws.

HR CONTACT INFORMATION: Please direct all requests, questions or concerns related to this Privacy Policy or your personal information (with the exception of potential security breaches as noted above) to careers@djeholdings.com.

Company's E.U. Data Processing Representative: The Company's representative (Natalie Butler at compliance@djeholdings.com) should be notified of any issues or concerns raised by data subjects or external data protection supervisory authorities.