Last Updated January 2018

Privacy Policy

This is the Privacy Policy of Inventus Solutions, Inc. ("Inventus," "we," "us," or "our"). By accessing or otherwise using any service or website we provide, you agree to this Privacy Policy. This privacy policy covers the information we collect online (1) from or on behalf of our clients or (2) from visitors to our websites generally.

1. Processing of Client Data

We process data our clients submit to us or instruct us to process on their behalf in connection with our services ("Client Data"). While our clients decide what data to submit, Client Data typically includes communications between individuals and other information that may be subject to discovery in legal proceedings. We process Client Data to provide our services pursuant to our agreements with the relevant clients, including to prevent or address service or technical problems, to respond to client support matters, to follow the instructions of our client who submitted the data, and to fulfill other contractual requirements with our clients.

2. Processing of Website Data

We also may receive certain information when people (such as clients and prospective clients) visit our corporate website(s), including the website on which this Privacy Policy is posted. In addition to information you provide us when visiting or otherwise accessing our website, we also may automatically collect information about the computer or devices you use to access our website. We also may combine any of the foregoing information, or link any of the foregoing information to a unique "cookie" identifier, as described below.

We may use the information collected to understand how visitors interact with our websites and to understand more about those visitors. We may use online technologies such as cookie identifiers and web-pixels to targets advertising to you when you visit other websites or use other web services.

If you choose to provide us with your contact information on an online registration form, we may use it to contact you via email, telephone, direct mail or other communication formats to provide you with information about our services (such as emails about our products, or invitations to events), or to provide you other information and services that you have requested. Should you no longer wish to be contacted by us, please select the "Unsubscribe" button at the bottom of the applicable email or send an email to the address listed on the bottom of this policy.

If you choose to submit your resume/CV, we will collect information about you, such as your name, location and email address. If you supply a resume/CV, then you may also choose to provide us with details of your career history and other information such as address, telephone number, gender and nationality.

We may otherwise use information collected through our websites for the purposes for which you provided it, to provide our services, for internal research and reporting, to improve the content of our websites or other services or develop new services, and to enforce the legal terms that govern our services.

We may aggregate and/or de-identify any information collected through our websites. We may use de-identified and/or aggregated data for any purpose, including without limitation for research and marketing purposes, and may also share such data with any third parties.

Our websites use "cookie" technology. A cookie is a small file that a website can read or write on your browser. We use cookies to operate our websites. We may also use cookies (and sync with or help deploy third party cookies) to help us advertise to you – for instance, to show you ads for our products or invite you to events when you visit other web pages and services. This is called "targeted" or "retargeted" advertising, and if you don't wish to receive these ads you can "opt out" of many companies that facilitate it by going to the website of the , or a similar European DAA site.

You may configure web browser to reject certain types of cookies, or to alert you when certain types of cookies are being sent. However, if you block or otherwise reject our cookies, certain websites (including ours) may not function properly.

We do not recognize or respond to browser-initiated Do-Not-Track signals, as the Internet industry is currently still working toward defining exactly what Do-Not-Track means, what it means to comply with Do-Not-Track, and a common approach to responding to Do-Not-Track.

We refer to the information described in this Section 2 as "Website Data."

3. Disclosures of Information

Subject to limitations in our client agreements, we may disclose any information we collect (through our websites or otherwise), in the following circumstances:

- To Perform Services for a Client: We may disclose Client Data with non-affiliated third parties based on a Client's request, or as required to perform services requested or contracted by a Client, or as otherwise described in this Privacy Policy.
- With Service Providers: We likewise may provide information to service providers who perform services for us or on our behalf. Depending on the data and the context of its collection, this may include, for instance, third parties who perform marketing, email delivery, billing, hosting, supporting, data enhancement, event management, or other services related to our business.
- Protection of Us and Others: We may access, preserve and disclose Client Data or Website Data if required to do so by law or in a good faith belief that such access, preservation or disclosure is reasonably necessary to: (a) comply with legal process (including to meet national security or law enforcement requirements); (b) enforce our Terms of Service, this Privacy Policy, or other contracts; (c) respond to claims that any content violates the rights of third parties; (d) respond to your requests for customer service; and/or (e) protect the rights, property or personal safety of us, our agents and affiliates, our users and/or the public. We may also disclose information to law enforcement agencies in emergency circumstances, where the disclosure of such information is consistent with the types of emergency disclosures permitted or required by law.
- Business Transfers: We reserve the right to disclose and transfer all of your information, including your contact information, in connection with a proposed or actual merger, acquisition, transfer of control, or sale of all, or components, of our business, to the extent permitted by applicable law.

4. Security

We have implemented physical, electronic, and administrative safeguards to help prevent unauthorized access to the data that we maintain. However, no security protocols are 100 percent secure. Thus, we cannot guarantee that the information you submit or that we hold will not be intercepted or accessed by others.

5. EU-US Privacy Shield

As a business subject to the enforcement and investigatory powers of the Federal Trade Commission, Inventus Solutions, Inc. has certified our compliance with the EU-US Privacy Shield Framework with respect to the personal Client Data we receive from the relevant European countries,

effective as of the date our certification is posted at https://www.privacyshield.gov/list. You can learn more about the Privacy Shield program at https://www.privacyshield.gov.

We may also process personal data our clients in the EU submit via other compliance mechanisms, including data processing agreements based on the EU Standard Contractual Clauses.

As of the date we applied for Privacy Shield certification, we did not use third-party service providers to process information subject to the Privacy Shield. However, if we receive information under the Privacy Shield and then transfer it to a third-party service provider acting as an agent on our behalf, we have certain liability under the Privacy Shield if both (i) the agent processes the information in a manner inconsistent with the Privacy Shield and (ii) we are responsible for the event giving rise to the damage.

Accessing Your Data: European residents have certain legal rights to access certain personal data and to obtain its correction, amendment, or deletion. You may contact us at the contact information below to request access, correction, amendment, or deletion. Because our personnel have a limited ability to identify and access an individual user's personal data that our client has submitted to us, and because we process it on behalf of our clients, if you wish to request access, to limit use, limit disclosure, or request corrections, we may first refer you to the client who submitted your data, and we will support them as needed in responding to your request. Please note that the rights described in this paragraph are subject to important exceptions and restrictions, including under laws designed to protect the integrity of legal proceedings.

In compliance with the EU-US Privacy Shield Principles, Inventus, Solutions, Inc. commits to resolve complaints about your privacy and our collection or use of your personal information. If you have and concerns or complaints, please contact us as described at the end of this policy, and we will work with you to resolve your issue.

Inventus Solutions, Inc. has further committed to refer unresolved privacy complaints under the EU-US Privacy Shield Principles to the JAMS Privacy Shield Program, which is described on the JAMS website at **https://www.jamsadr.com/eu-us-privacy-shield.** JAMS is an alternative dispute resolution provider located in the United States. Assistance from JAMS will be provided at no cost to you. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please contact or visit the JAMS website at https://www.jamsadr.com/eu-us-privacy-shield for more information or to

file a complaint. The services of JAMS are provided at no cost to you. If your complaint is not resolved through these channels, a binding arbitration option may be available before a Privacy Shield Panel in limited circumstances. To be eligible for binding arbitration under this option, a resident of a European country participating in the Privacy Shield must first: (1) contact us and afford us the opportunity to resolve the issue; (2) seek assistance from JAMS, our independent dispute resolution provider; and (3) contact the U.S. Department of Commerce (either directly or through a European Data Protection Authority) and afford the Department of Commerce time to attempt to resolve the issue. If such a resident invokes binding arbitration, each party shall be responsible for its own attorney's fees. Please be advised that, pursuant to the Privacy Shield, the arbitrator(s) may only impose individual-specific, non-monetary, equitable relief necessary to remedy any violation of the Privacy Shield Principles with respect to the resident.

6. Updates

We may update this Privacy Policy to reflect changes in the law or in our practices. Your continued use of the services or website following the posting of changes to this Privacy Policy on our website will mean you accept those changes.

7. Contact Us

To exercise your rights, or to provide us with questions or complaints, please contact us at:

Inventus Solutions, Inc.
Attn: Legal Department
500 W Madison Street #1210
Chicago, IL 60661
legal@inventus.com

Local Addendum to the Privacy Policy for Data Subjects in the European Union

1. Scope of application

This local addendum to the Privacy Policy for data subjects in the European Union ("EU Addendum") supplements sections 1 to 7 of the Privacy Policy above and applies in addition to the these sections to any processing of personal data relating to data subjects (as defined below) in the European Union, where the processing activities are related to (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the European Union or (ii) the monitoring of their behavior, as far as their behavior takes place within the European Union.

"Personal data", where used in this EU Addendum, shall mean any information relating to an identified or identifiable natural person ("data subject'"; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Within its scope of application this EU Addendum shall take precedence over any conflicting or deviating terms in sections 1 to 7 of the Privacy Policy.

2. Controller

Controller in the meaning of Article 4 no. 7 of the Regulation (EU) 2016/679 ("GDPR") in relation to the processing of personal data subject to this EU Addendum is

Inventus Solutions, Inc
Attn: Legal Department
500 W Madison Street #1210
Chicago, IL 60661
legal@inventus.com

3. Processing of Website Data

When we collect information about the computer or devices you use to access our website, track your use of our website to improve the website and provide targeted advertisement as outlined in paragraph 1, 2 and 7 of

section 2 of the Privacy Policy above, we do so to pursue our legitimate interest in providing relevant advertisement to you and improve our service. We collect such information only on the basis of anonymized or pseudomized data. You may object to the collection of pseudomized data by sending us a notice through this opt-out link.

In this case we will place an opt-out cookie on your device to identify the device and be able to prevent future tracking. Legal basis as of 25. May 2018 for this collection and processing of data is Art. 6 para. 1 lit. f) GDPR.

When we aggregate and/or de-identify any information collected through our websites. to process such aggregated or de-identified data for any purpose, including without limitation for research and marketing purposes or share such data with third parties we will do so as of 25. May 2018 on the basis of Art. 6 para. 1 lit. f) GDPR.

When we process (i) your contact information provided on an online registration form, to contact you and to provide you with information about our services or to provide you other information and services that you have requested, or (ii) your resume/CV you provided in the context of a job application, or (iii) other information through our websites for the purposes for which you provided it, we do so as of 25. May 2018 on the basis of the permission set out in Art. 6 para. 1 lit. b) GDPR.

Where we process personal data to comply with legal obligations or legal processes we do so on the legal basis of Art. 6 para. 1 lit. c) GDPR. Legal basis for the processing of personal data for the purposes listed in section 3 lit. b), c) and e) of the Privacy Policy is Art. 6 para. 1 lit. f) GDPR.

4. Transfer to third countries

Personal data processed by us in the United States will be processed in compliance with our Privacy Shield certification. The European commission concludes that the United States ensure an adequate level of protection for personal data transferred under the EU-U.S. Privacy Shield from the Union to self-certified organisations in the United States.

5. Your rights as a data subject

To enforce the following rights as a data subject granted in the GDPR, please contact us as described in section 7 of the Privacy Policy above. Please bear

in mind that we may ask you to identify yourself as a data subject (e.g. by presenting a copy of your identity card) to be able to verify whether you are the data subject and to prevent misuse of your personal by others.

a. Right of Access

As a data subject you have the right of access to your personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations;

and starting from 25 May 2018 according to Art. 15 GDPR also:

(d) the envisaged period for which the personal data will be stored, or, if not possible the criteria used to determine that period;

(e) where the data are not collected from the data subject, any available information as to their source;

(f) and the rights of the data subject, explained hereinafter.

b. Right of Rectification

We as a data controller are required to rectify inaccurate personal data. As of 25 May 2018 you as an affected data subject shall have the right to obtain from us the rectification of inaccurate personal data and the completion of incomplete data relating to you.

c. Right to Erasure or restriction of processing

As of 25 May 2018 you as a data subject have the right to obtain from us the erasure of personal data concerning you, if the conditions described Art. 17 para 1 GDPR are fulfilled, and provided none of the exceptions specified in Art. 17 para 3 GDPR apply. As from 25 May 2018 according to art. 17 para 2 GDPR, you as a data subject have a right to be forgotten if

we as a data controller have made the personal data public and are obliged pursuant to Art. 17 para 1 GDPR to delete the personal data.

d. Right to object

Where we process your personal data on the basis of Art. 6 para 1 subpara (f) GDPR to pursue our legitimate interest, you have the right - starting from 25 May 2018 - to object to such processing (Art. 21 GDPR). If you object to processing, we will review our balancing of interests.

e. Retention of data

Personal data may be stored only as long as necessary. According to Art. 17 para 1 DS-GVO, personal data that are no longer necessary for the purpose for which they were collected or otherwise processed, must be deleted by the data controller. We will retain your personal data collected through our websites for so long as it is required to complete the purpose for which you provided us with your data. We will retain Client Data for the period agreed in the separate agreement with the particular client.

f. Right to lodge a complaint with a supervisory authority

You may lodge a complaint with the competent data protection supervisory authority, if you consider that the processing of personal data relating to you is unlawful.