Epiq Privacy Shield Policy

This Epiq Privacy Shield Policy ("**Policy**") describes how Epiq Systems, Inc. and its subsidiaries and affiliates in the United States ("**US**") ("**Company**," "**we**," "**us**" or "**our**") collect, use, and disclose certain personally identifiable information that we receive in the US from the European Union ("**EU Personal Data**"). This Policy applies to our following US legal entities, subsidiaries and/or affiliates: Epiq Systems, Inc., Epiq Class Action & Claims Solutions, Inc., Epiq eDiscovery Solutions, Inc., Encore Legal Solutions, Inc., Epiq Technology, LLC, Epiq Bankruptcy Solutions, LLC, De Novo Legal LLC, Hilsoft, Inc., Iris Data Services, Inc., and Epiq Systems Acquisition, Inc. This Policy supplements our Privacy Statement located at https:// http://www.epiqsystems.com/privacy-statement, and unless specifically defined in this Policy, the terms in this Policy have the same meaning as in the Privacy Statement.

Epiq recognizes that the EU has established strict protections regarding the handling of EU Personal Data, including requirements to provide adequate protection for EU Personal Data transferred outside of the EU. To provide adequate protection for certain EU Personal Data about consumers, clients, suppliers, business partners, job applicants and employees received in the US, Epiq has elected to self-certify to the EU-US Privacy Shield Framework administered by the US Department of Commerce ("**Privacy Shield**"). Epiq adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement, and Liability.

Epiq complies with the EU-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union to the United States. Epiq has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit https://www.privacyshield.gov/

For purposes of enforcing compliance with the Privacy Shield, Epiq is subject to the investigatory and enforcement authority of the US Federal Trade Commission. For more information about the Privacy Shield, see the US Department of Commerce's Privacy Shield website located at https://www.privacyshield.gov. Further, Epiq is required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

To review Epiq's representation on the Privacy Shield list, see the US Department of Commerce's Privacy Shield self-certification list located at https://www.privacyshield.gov/list.

Personal Data Collection and Use

We may receive the following categories of EU Personal Data in the US: an individual's name, whether or not in combination with an individual's country of birth, marital status, emergency contact, salary information, terms of employment, job qualifications (such as educational degrees earned), address, phone number, email address, user ID, password, and other identification numbers. We process EU Personal Data for the following purposes: to provide our services, including with respect to billing, identification and authentication, to contact and communicate with our clients about our services, to profile prospective clients, to build our mailing list for information distribution (subject to legal requirements including opt-out options), and for employment-related purposes including to process employment-related data in the US and evaluate job candidates. Data subjects whose personally

identifiable information we process include consumers, clients including individuals, law firms, companies and other legal persons, suppliers, business partners, job applicants, independent contractors, and employees.

We will only process EU Personal Data in ways that are compatible with the purpose that we collected it for, or for purposes the individual later authorizes. Before we use your EU Personal Data for a purpose that is materially different than the purpose we collected it for or that you later authorized, we will provide you with the opportunity to opt out. We maintain reasonable procedures to help ensure that EU Personal Data is reliable for its intended use, accurate, complete, and current.

We may collect the following categories of sensitive EU Personal Data: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data covering health or sex life. When we collect sensitive EU Personal Data, we will obtain your opt-in consent where the Privacy Shield requires, including if we disclose your sensitive EU Personal Data to third parties, or before we use your sensitive EU Personal Data for a different purpose than we collected it for or than you later authorized. Certain exceptions to our obligation to obtain affirmative opt-in consent to process sensitive personal data are where the processing is: (i) in the vital interests of the individual or another person; (ii) necessary for the establishment of legal claims or defenses; (iii) required to provide medical care or diagnosis; (iv) carried out in the course of legitimate activities by certain foundations, associations, or other non-profit bodies; (v) necessary to carry out employment law-related obligations; (vi) related to data made public by the individual.

Epiq commits to cooperate with EU data protection authorities (DPAs) and comply with the advice given by such authorities with regard to human resources data transferred from the EU in the context of the employment relationship.

Data Transfers to Third Parties

Third-Party Agents or Service Providers. We may transfer EU Personal Data to our third-party agents or service providers who perform functions on our behalf [as described in our Privacy Statement or in this Policy. Where required by the Privacy Shield, we enter into written agreements with those third-party agents and service providers requiring them to provide the same level of protection that Privacy Shield requires and limiting their use of the data to the specified services provided on our behalf. We take reasonable and appropriate steps to ensure that third-party agents and service providers process EU Personal Data in accordance with our Privacy Shield obligations and to stop and remediate any unauthorized processing. Under certain circumstances, we may remain liable for the acts of our third-party agents or service providers who perform services on our behalf for their handling of EU Personal Data that we transfer to them.

Third-Party Data Controllers. In some cases we may transfer EU Personal Data to unaffiliated third-party data controllers. These third parties do not act as agents or service providers and are not performing functions on our behalf. We may transfer your EU Personal Data to third-party data controllers for the purposes described in our Privacy Statement or this Policy. We will only provide your EU Personal Data to third-party data controllers where you have not opted-out of such disclosures, or in the case of sensitive EU Personal Data, where you have opted-in if the Privacy Shield requires consent. We enter into written contracts with any unaffiliated third-party data controllers requiring them to provide the same level of protection for EU Personal Data the Privacy Shield requires. We also limit their use of your EU Personal Data so that it is consistent with any consent you have provided and with the notices you have received. If we transfer your EU Personal Data to one of our affiliated entities within our corporate group,

we will take steps to ensure that your EU Personal Data is protected with the same level of protection the Privacy Shield requires.

Disclosures for National Security or Law Enforcement. Under certain circumstances, we may be required to disclose your EU Personal Data in response to valid requests by public authorities, including to meet national security or law enforcement requirements.

Security

We maintain reasonable and appropriate security measures to protect EU Personal Data from loss, misuse, unauthorized access, disclosure, alteration, or destruction in accordance with the Privacy Shield.

Access Rights

You may have the right to access the EU Personal Data that we hold about you and to request that we correct, amend, or delete it if it is inaccurate or processed in violation of the Privacy Shield. These access rights may not apply in some cases, including where providing access is unreasonably burdensome or expensive under the circumstances or where it would violate the rights of someone other than the individual requesting access. If you would like to request access to, correction, amendment, or deletion of your EU Personal Data, you can submit a written request to the contact information provided below. We may request specific information from you to confirm your identity. In some circumstances we may charge a reasonable fee for access to your information.

Questions or Complaints

You can direct any questions or complaints about the use or disclosure of your EU Personal Data to us at privacyshield@epiqsystems.com (US). You may also contact our EU affiliate, Epiq Systems, Ltd. (UK), at privacyshield@epiqsystems.co.uk with any questions or concerns. We will investigate and attempt to resolve any complaints or disputes regarding the use or disclosure of your EU Personal Data within 45 days of receiving your complaint. We self-certify with the US Department of Commerce and have engaged with our U.S. - based third party provider for dispute resolution of non-human resources data related complaints. For any unresolved human resources data-related complaints, we agree to cooperate with the EU data protection authorities or authorities concerned in conformity with the Supplemental Principles on Human Resources Data and the Role of the Data Protection Authorities and comply with the advice given by such authorities. If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, then please contact our U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request for further information and assistance.

Binding Arbitration

You may have the option to select binding arbitration for the resolution of your complaint under certain circumstances, provided you have taken the following steps: (1) raised your compliant directly with us and provided us the opportunity to resolve the issue; (2) made use of the independent dispute resolution mechanism identified above; and (3) raised the issue through the relevant data protection authority and allowed the US Department of Commerce an opportunity to resolve the complaint at no cost to you. For more information on binding arbitration, see US Department of Commerce's Privacy Shield Framework: Annex I (Binding Arbitration).

Contact Us

If you have any questions about this Policy or would like to request access to your EU Personal Data, please contact us as follows: privacyshield@epiqsystems.com (US) or privacyshield@epiqsystems.co.uk (EU).

Changes To This Policy

We reserve the right to amend this Policy from time to time consistent with the Privacy Shield's requirements.

Effective Date: August 1, 2016

Last modified: September 13, 2016