EU-US, UK-US and Swiss-US Privacy Shield Privacy Statement- Cisive Entities

Cisive, including its subsidiaries Cisive Driver IQ LLC, Intellicorp Records, Inc., and PreCheck, Inc., all Cisive companies (collectively "Cisive"), participates in the EU/US, UK/ US, and Swiss/US Privacy Shield programs administered by the United States Department of Commerce ("Privacy Shield") and has certified to the Department of Commerce that Cisive adheres to the Privacy Shield Principles for th ese programs. As part of our participation in the Privacy Shield, Cisive has committed to processing all personal data Cisive receives from EU member states, the United Kingdom, and Switzerland, and other participating countries ("from the EU, the United Kingdom, and Switzerland") in accordance with its Privacy Shield commitments and any other relevant standard contractual clauses. This privacy statement applies only to personal data transferred pursuant to the Privacy Shield or other legally valid transfer mechanism. To learn more about the Privacy Shield program, and to view Cisive's certification(s), please visit: https://www.privacyshield.gov/list.

Cisive also complies, where applicable, with U.S. laws, particularly the Fair Credit Reporting Act ("FCRA" 15 U.S.C. §§ 1681 et seq.) and its state counterparts, which provide privacy protections for consumer personal data contained in "consumer reports." In the event of a conflict between this Privacy Shield Privacy Statement and the FCRA or other applicable laws, Cisive will comply with its obligations under the FCRA or other applicable US law. CARCO Group, Inc. dba Cisive as well as Cisive companies and covered entities Cisive Driver IQ, Intellicorp Records, Inc., and PreCheck, Inc. are subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC). Cisive's Privacy Shield Privacy Statement is organized around the following principles:

1. Notice

At Cisive, we notify individuals about the purposes for which we collect and use information about them, the choices they have regarding certain uses and disclosures of their personal data, and how to contact us with inquiries or complaints. We provide this notice either directly, such as through this privacy statement, or through our customers.

Cisive collects personal data for the purpose of providing a variety of information products and services to employers and other Cisive customers. For example, Cisive may collect identification information and information such as information about an individual's employment history, educational qualifications, credit history, or criminal history for the purpose of preparing and providing employment screening services to our customers. Cisive may collect employment application information on behalf of our customers, such as through a customer-branded applicant portal. We also may collect similar information for investigative or due diligence purposes and other non-employment purposes.

2. Choice

In many cases, the reports that we prepare are prepared with the express consent of the individual. For example, the subject of a consumer report issued for employment purposes must provide express authorization ("opt-in"), typically through the employer or prospective employer before Cisive may furnish the report. In other cases, Cisive offers individuals the opportunity to choose (opt-out) whether their personal data is (i) to be disclosed to a third party (other than our service providers performing tasks on Cisive's behalf pursuant to a contract or a customer on whose behalf we are processing it) or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals.

For sensitive information[1], Cisive obtains (directly or through a third party, such as our customer) affirmative express consent (opt-in) from individuals, with certain exceptions permitted by the Privacy Shield program, if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice.

We are committed to providing individuals with clear, conspicuous, and readily available mechanisms to exercise choice. Therefore, in addition to any other mechanisms that may be provided in particular cases, individuals may opt-out by contacting Cisive using the points of contact in the "Contact Us" section below.

---

[1] Sensitive information for purposes of this policy means personal data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, information specifying the sex life of the individual or information designated by the transferring organization as sensitive. In the case of information transferred pursuant to the Swiss Privacy Shield, sensitive information also includes information on social security measures or administrative or criminal proceedings and sanctions, which are treated outside pending proceedings.

3. Accountability for Onward Transfer

Cisive discloses personal data that it collects to its customers for employment screening, due diligence, or similar purposes. Cisive may disclose personal data to its service providers. Cisive also may be required to disclose personal data in response to lawful requests by public authorities, including disclosures to meet national security or law enforcement requirements. Cisive's disclosure of personal data to third parties is governed by the Notice and Choice Principles described above, and, for the purpose of providing consumer reports to third parties, Cisive complies with FCRA requirements.

When transferring personal data to our customers or other third-party controllers (i.e., entities that will control how personal data is processed), we comply with the Notice and Choice Principles as described above. Consistent with Privacy Shield timing requirements for onward transfer compliance, Cisive will enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made, the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.

As noted above, Cisive also may transfer personal data to service providers acting on its behalf. In such cases, consistent with Privacy Shield timing requirements for onward transfer compliance, Cisive will:

- transfer such data only for limited and specified purposes;
- ascertain that the service provider is obligated to provide at least the same level of privacy protection as is required by the Privacy Shield Principles or any relevant standard contractual clauses;

- take reasonable and appropriate steps to ensure that the service provider effectively processes the personal data transferred in a manner consistent with Cisive's obligations under the Principles or any standard contractual clauses;
- require the service provider to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles or any standard contractual clauses;
- upon notice, including from the service provider, take reasonable and appropriate steps to stop and remediate unauthorized processing; and
- provide a summary or a representative copy of the relevant privacy provisions or relevant standard contractual clauses from its contract with that service provider to the Department of Commerce upon request.

4. Security

Cisive takes reasonable and appropriate measures to protect personal data from loss, misuse, and unauthorized access, disclosure, alternation, and destruction, taking into account the risks involved in the processing and nature of the personal data.

5. Data Integrity and Purpose Limitation

Cisive limits the personal data it collects to information that is relevant for the purposes of processing. Cisive does not process personal data in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, Cisive takes reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. In the case of consumer reports, Cisive meets this obligation by complying with FCRA requirements, including a requirement that consumer reporting agencies follow reasonable procedures to ensure maximum possible accuracy.

Cisive takes reasonable and appropriate measures to retain personal data only for as long as Cisive has a legitimate legal or business need to do so, such as customer service, compliance with legal or contractual retention obligations, retention for audit purposes, security and fraud prevention, preservation of legal rights or other reasonable purposes consistent with the purpose of the collection of the information. Cisive will adhere to the Principles for as long as it retains personal data transferred in accordance with the Privacy Shield Principles.

6. Access

It is Cisive's policy to provide individuals with access to personal data about them that Cisive holds about them and provides them with a means to request the correction, amendment, or deletion of that information where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Many Cisive products are governed by the FCRA. Where applicable, Cisive provides access and correction rights in accordance with FCRA requirements. The FCRA specifies the rights of consumers to obtain a disclosure of the contents of the consumer reporting file that Cisive maintains about them, if any. The FCRA also provides consumers with rights to dispute the contents of their file and, if warranted, to have the contents corrected or deleted.

Of course, whether the consumer personal data is covered by the FCRA or by our Privacy Shield Principles, Cisive requires that an individual provide reasonable verification of their identity before we provide access to personal data. To access your Cisive file and obtain any of the remedies discussed in this section please contact Cisive using the points of contact in the "Contact Us" section below.

7. Recourse, Enforcement and Liability

Cisive internally monitors and assesses our compliance with our Privacy Shield Privacy statement and our Privacy Shield obligations. Under the Privacy Shield Principles, Cisive may be liable in the event that a service provider to whom Cisive transfers personal data such personal data in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage. An individual with an inquiry or complaint may contact us using the mailing or email address below.

In the case of human resources data from the EU, Cisive has agreed to cooperate with a panel of European Data Protection Authorities created for that purpose. In the case of human resources data transferred from Switzerland, Cisive has agreed to cooperate with the Swiss Federal Data Protection and Information Commissioner. In the case of human resources data transferred from the United Kingdom, Cisive will cooperate with the EU Panel of Data Protection Authorities or the UK Information Commissioner's Office, as appropriate.

In compliance with the Privacy Shield Principles, Cisive commits to resolve complaints about our collection or use of your personal information. EU, UK and / or Swiss individuals with inquiries or complaints regarding our Privacy Shield policy should first contact Cisive at:

CARCO Group, Inc.
disputes@carcogroup.com
(855) 881-0716
Individuals also may be able to invoke binding arbitration, under certain circumstances where permitted by the Privacy Shield program, if the individual believes there has been a violation of Privacy Shield requirements that has not been appropriately addressed by Cisive.

Cisive's compliance with its Privacy Shield obligations also is subject to investigation and enforcement by the U.S. Federal Trade Commission. Cisive also is required by the Privacy Shield program to respond promptly to inquiries and requests for information from the U.S. Department of Commerce.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

8. Public Record and Publicly Available Information

In accordance with Privacy Shield, in cases where Cisive discloses public records or publicly available information from the EU, United Kingdom, and Switzerland without combining that information with non-public information, our general policies on Notice, Choice, and Accountability for Onward Transfer may not apply.

9. Contact Us

If you have any inquiries or complaints regarding this policy or our privacy practices, contact us at 5000 Corporate Court, Suite 203, Holtsville, NY, 11742 or privacypolicy@cisive.com.

10. Policy Changes

Cisive reserves the right to change their policy from time to time, consistent with the Privacy Shield Principles.

Effective 01/01/2018
Last Updated 10/6/2020