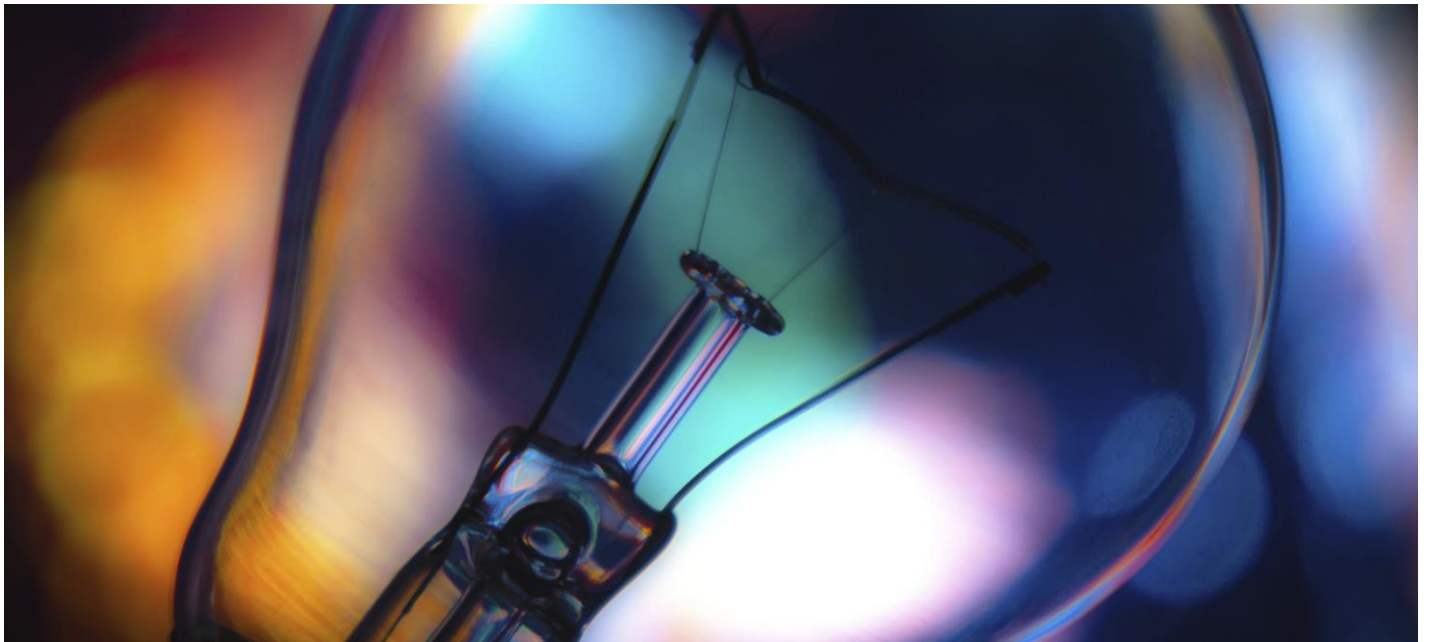


# Ensono, LP

## EU-US Privacy Shield Policy



# Document Version Control

**Intended Distribution:** All Ensono, LP Associates and interested parties  
**Effective Date:** 01/24/2019

## Review & Approval History

Version Number	Date	Reviewed By
v1.0	9/29/2016	Audit & Compliance, Corporate Legal
	11/17/2016	Audit & Compliance, Corporate Legal
	11/23/2016	Audit & Compliance, Corporate Legal
	02/15/2017	Global Assurance & Advisory, Corporate Legal
	01/24/2019	Global Assurance & Advisory

# Table of Contents

Document Version Control .....	2
Ensono Privacy Shield Policy .....	4
1. Purpose and Scope .....	4
2. Applicability and Enforcement .....	4
3. Definitions .....	5
4. Notification & Choice .....	5
5. Accountability for Onward Transfers .....	5
6. Data Security, Integrity and Purpose Limitation.....	6
7. Annual Verification and Certification .....	6
8. Individual Rights to Access, Review and Update Personal Data .....	7
9. Questions or Complaints .....	7
10. Independent Recourse Mechanism .....	7
11. EU-US Privacy Shield Policy Updates.....	7

# Ensono Privacy Shield Policy

## 1. Purpose and Scope

It is the policy of Ensono, LP (“Ensono” or the “Company”) to comply with applicable laws and regulations protecting the privacy of personal information in the jurisdictions in which the Company operates. Ensono respects and protects personal information collected or maintained by or on behalf of the Company, regardless of the form, format, location or use, in support of its business operations, including, without limitation, human resources and commercial operations.

Ensono 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. Ensono 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 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>.

This policy establishes a framework for privacy of nonpublic personal information (“NPI”) (as defined in Section 3.0 below, and consistent with the Privacy Shield definition of “personal data” or “personal information”), including but not limited to personal data, personal financial information and personal health information (“PHI”). Protecting NPI requires keeping it confidential wherever it is collected and stored in digital form or otherwise. The principal objectives of the Policy are to:

- Ensure the confidentiality and integrity of NPI;
- Protect against unauthorized access to or use of NPI;
- Prevent harm to individuals due to identity theft, fraud, or any other act that would violate an individual’s right to privacy.

This policy governs all Ensono employees, contractors, and temporary staff (“Ensono Associates”) as defined in Section 3 below) with respect to the protection of NPI. Every Ensono Associate has the obligation to play his or her role in protecting the NPI of fellow Ensono Associates, clients, business partners, and other individuals with whom Ensono has business interactions in compliance with all applicable laws, regulations, and other Ensono policies and procedures.

## 2. Applicability and Enforcement

Ensono is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC), an agency of the US Department of Commerce, under the EU-US Privacy Shield Framework. In exercising its monitoring and enforcement responsibilities under the Framework, the US Department of Commerce works cooperatively with European Union Data Protection Authorities (EU DPAs).

Ensono also assures compliance with this EU-U.S. Privacy Shield Policy and the EU-U.S. Privacy Shield Framework by fully investigating and attempting to resolve any complaint or dispute regarding the use and/or disclosure of personal data in violation of this Policy.

### 3. Definitions

For purposes of this Policy, the following definitions apply:

- **“Ensono Associate”** means any employee, contractor, agent, or temporary staff member of the Company, to the extent such individual handles, processes or has access to NPI.
- **“Nonpublic personal information” (“NPI”)** means:  
Consistent with the Privacy Shield definition, personal data or personal information are data about an identified or identifiable individual that are within the scope of the Directive, received by an organization in the United States from the European Union, and recorded in any media or format. It includes information that identifies or may be used to identify an individual and the protection of which is governed by applicable data protection laws (including statutes, regulations, orders, etc.), and does not consist solely of information that is lawfully obtained from public sources, publicly available information, or from federal, state or local government records lawfully made available to the general public. NPI may include, but is not limited to: (1) an individual’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual: Social Security number, driver’s license number, other government-issued identification number, biometric identifier, medical coverage number, or financial account number or credit card/debit card number that would permit access to the individual’s financial account, and (2) health information together or in association with an identifier of an individual (such as initials, an e-mail address, birth date, or any other identifying number or code). NPI also includes information that is deemed “protected health information” (“PHI”) under the Health Insurance Portability and Accountability Act (“HIPAA”).  
NPI does not include anonymized data, such as aggregated data, so long as the aggregation is sufficient to prevent identification of an individual from that data either itself or in combination with publicly available data.
- **“Third Party”** means any person, company or organization (e.g., a vendor or business partner), public authority/agency, or other entity outside of the Company that provides or receives or processes NPI from or on behalf of Ensono.

### 4. Notification & Choice

The publication of this policy constitutes Ensono’s notification to clients and individuals about its privacy practices and adherence to the EU-US Privacy Shield and other data protection regulations.

Ensono collects and processes HR data of Ensono Associates for the fulfillment of employment law, administration of employment benefits, promotions and other similar employment decisions.

Ensono may collect, use or disclose personal information controlled by or belonging to clients in order to deliver services and or fulfil contractual obligations. Such uses or disclosures will conform to this policy and to the Privacy Shields Principles. Secondary uses of personal information for purposes that are not consistent with the original purpose for which such information was collected, are prohibited, unless the data subjects opt-in to such uses or disclosures and unless authorized by the Corporate Legal department.

### 5. Accountability for Onward Transfers

Except as otherwise provided herein, Ensono discloses personal data only to third parties who reasonably need to know such data only for the scope of the original intent for which the data was collected and not for other purposes. All disclosures of personal information must be reviewed and authorized by Corporate Legal.

Ensono does not use or disclose personal data for marketing purposes, including to promote, advertise, or suggest the benefits or quality of any Ensono product or service, if the individual to whom the information pertains has not consented to such uses or disclosures or has opted out of such use.

Ensono may provide personal data to third parties that act as agents, consultants, and contractors to perform tasks on behalf of and under our instructions. Such disclosures would be made pursuant to a written agreement providing that the third party agrees, prior to accessing any personal information, to protect the information as set forth in the data privacy and security provisions of Ensono's template agreements for contracts with third parties. Any variance from the template data protection provisions must be approved by Corporate Legal.

Transfers or disclosures may not be made to a third party prior to receipt by Ensono of duly executed legal agreements assuring Ensono they would comply with the Privacy Shield principles or another mechanism permitted by the applicable EU data protection law(s) for transfers and processing of personal data.

Ensono may also disclose personal data for other purposes or to other third parties when a data subject has consented to or requested such disclosure. Please be aware that Ensono may be required to disclose an individual's personal information in response to a lawful request by public authorities, including to meet national security or law enforcement requirements. Ensono is liable for inappropriate onward transfers of personal data to third parties.

## 6. Data Security, Integrity and Purpose Limitation

In order to assure the security, integrity and limitation of use or disclosure to the original purpose for which data was collected, Ensono has developed and implemented appropriate standards and policies. The Company's Information Security Policy (ISP) is the foundation of Ensono's data protection policy. It provides classifications of data and guidelines for protection, and includes guidelines concerning acceptable use, access and cryptographic controls, data destruction as well as management of security incidents.

Ensono requires that its Associates understand the data security protection requirements of sensitive data. Identification of sensitive data is the responsibility of the information owner as defined in the ISP. Ensono Associates who, as part of the job role, collect, store, and/or maintain such data must comply with the security controls.

## 7. Annual Verification and Certification

Ensono will renew its EU-US Privacy Shield certification annually, unless it subsequently determines that it no longer needs such certification or if it employs a different adequacy mechanism. As part of the recertification process, Ensono will perform the verification process to ensure that its attestations and assertions with regard to its treatment of personal data are accurate and that the company has appropriately implemented these practices.

As part of the verification process, Ensono will undertake the following:

- A. Review this Privacy Shield policy to ensure it accurately describes the practices regarding the processing of personal data
- B. Ensure that the publicly posted privacy policy provides sufficient notice of Ensono's participation in the EU-US Privacy Shield
- C. Ensure that this policy continues to comply with the Privacy Shield Principles
- D. Confirm that individuals are informed of the processes for addressing complaints and any independent dispute resolution process (such as the IRM noted in section 10)
- E. Review its processes and procedures for training Associates about Ensono's participation in the EU-US Privacy Shield program and the appropriate handling personal data

Ensono will prepare an internal verification statement on an annual basis.

## 8. Individual Rights to Access, Review and Update Personal Data

Individuals have the right to access the personal information about them that Ensono holds and to be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Privacy Shield Principles. The exercise of these rights are subject to the Supplemental Principles of the Framework.

## 9. Questions or Complaints

In compliance with the Privacy Shield Principles, Ensono commits to resolving complaints about our collection or use of your personal information. European Union individuals with inquiries or complaints regarding our Privacy Shield policy should first contact Ensono at: [privacy@ensonocom](mailto:privacy@ensonocom).

## 10. Independent Recourse Mechanism

Ensono has further committed to cooperating with [EU data protection authorities \(EU DPAs\)](#) with regard to unresolved Privacy Shield complaints concerning human resources data transferred from the EU in the context of the employment relationship. If you do not receive timely acknowledgment of your complaint from us, or if we have not addressed your complaint to your satisfaction, please contact the EU DPAs for more information or to file a complaint. The services of EU DPAs are provided at no cost to you.

Finally, as a last resort and in limited situations, EU individuals may seek redress from the Privacy Shield Panel, a binding arbitration mechanism.

## 11. EU-US Privacy Shield Policy Updates

Ensono's Global Assurance & Advisory function has primary responsibility for the administration of this policy. In fulfilling that responsibility, it shall consult regularly with the Corporate Legal function, Information Security, Human Resources ("HR"), and other internal stakeholders.

Global Assurance & Advisory shall review this policy periodically and ensure that it is updated and revised as appropriate. It shall monitor updates in applicable data protection laws to ensure that this policy reflects Ensono's legal obligations with respect to personal information, in addition to measures implemented to fulfil such obligations. Ensono Associates, clients and EU individuals will be notified of changes to this policy via our privacy website.