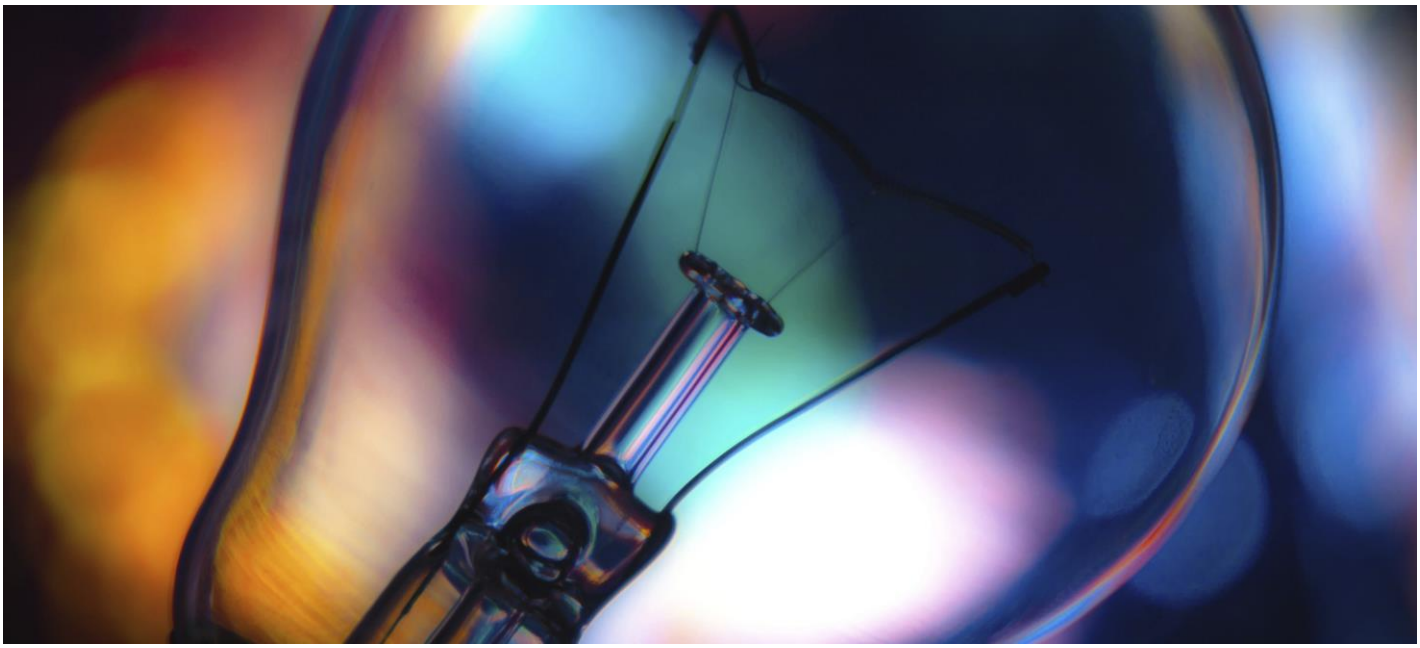
Ensono Global Data Protection & Privacy Policy



Document Version Control

Classification: *Internal & Public Use*
Intended Distribution: *All*
Issue Date: *09/29/2016*
Revision: *1.0*
Last Revision Date: *May 21, 2018*
Approved By: *Ensono, LP Corporate Legal and Global Assurance & Advisory*

Revision History

Version Number	Date	Performed By
v1.0	9/29/2016	Assurance & Advisory, Corporate Legal
	11/17/2016	Assurance & Advisory, Corporate Legal
	11/23/2016	Assurance & Advisory, Corporate Legal
	02/15/2017	Assurance & Advisory, Corporate Legal
	05/21/2018	Assurance & Advisory
	10/15/2018	Assurance & Advisory
	12/13/2019	Assurance & Advisory

Table of Contents

Introduction

Ensono, LP ("**Ensono**", "**we**", "**us**," or "**our**") is committed to conducting its business in accordance with all applicable data protection laws and regulations, and in line with the highest standards of ethical conduct. This document outlines our data protection and privacy policy and the expected conduct of data users, concerning the collection, use, retention, transfer, disclosure, destruction or other processing of personal data.

Recognizing that personal data is subject to certain legal safeguards and other regulations, such as the GDPR, which impose restrictions on how organizations may process such information, we are committed to implementing and maintaining appropriate measures to safeguard the privacy and security of personal data.

As a data controller and data processor, Ensono is responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose the company to complaints, litigation risks, regulatory actions, fines and/or reputational damage. All Associates and third-party service providers are required to comply with this policy.

Ensono's leadership is fully committed to ensuring continued and effective implementation of this policy and requires all data users to share in this commitment.

1. About This Policy

This policy applies to all our data users, regardless of location, who process personal data for or on behalf of Ensono, including without limitation for the purposes of:

- Human resource management.
- Business operations.
- The provision or offer of products and services.
- Monitoring the preferences of visitors to our websites, by using data processing techniques such as web browser cookies to best direct them to relevant content, products or services.

Data users have the obligation to assist in protecting the personal data for which Ensono is responsible (including personal data of Ensono colleagues, clients, business partners, and other data subjects with whom we have business interactions), in compliance with all applicable laws, regulations, and other Ensono policies and procedures.

Any breach of this policy by a data user will be taken seriously and may result in disciplinary or enforcement action, up to and including termination of employment, working relationship or contract (as applicable). It may also be the case that such conduct is unlawful and, if so, we reserve the right to inform the appropriate authorities. Data users should also note that in some cases, they may be personally liable for their actions in respect of the processing of personal data.

This policy establishes a baseline standard for the processing and protection of personal data by our data users. Where national law imposes a requirement, which is stricter than imposed by this policy, the requirements in national law must be followed. Furthermore, where national law imposes a requirement that is not addressed in this policy, the relevant national law must be adhered to. If there are conflicting requirements in this policy and national law, please consult with privacy@ensono.com for guidance.

2. Definitions

For the purposes of this policy, the following definitions apply:

- **"consent"** means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to her or him.
- **"data controller"** means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **"data processor"** means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of a data controller.
- **data users** include Ensono, all Ensono entities, their respective Associates, contactors, agents or temporary staff members, together with all third parties and their subcontractors, in each case to the extent they handle, process or have access to personal data for or on behalf of Ensono or any Ensono Entity. Data users must protect the personal data they handle in accordance with this policy and any other of our applicable data security procedures and policies at all times.
- **Ensono entity** means any establishment, including subsidiaries and joint ventures over which Ensono exercises management control.
- **GDPR** means the European General Data Protection Regulation ((EU) 2016/679).
- **Non-covered jurisdictions** mean countries or regions deemed not to have adequate data protection regulations, nor other legal transfer mechanisms. This also includes countries such as China and Russia, which have restrictive regimes against the use of cryptographic controls for non-military purposes (such as on Ensono laptops and personal mobile devices).
- **personal data** means, any information relating to an identified or identifiable natural person (a "**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. personal data can be factual (e.g. a name, address or date of birth) and can also include any expression of opinion, or any indication of the intentions of a data controller or any other person, in respect of an individual.
- **"processing", "process" and any derivations thereof** means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. Operations performed may include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Sensitive personal data** is a sub-set of personal data and includes: (i) information about: a person's racial or ethnic origin; political opinions; religious, philosophical or similar beliefs; or trade union membership; (ii) genetic data; (iii) biometric data for the purpose of uniquely identifying a person; (iv) data concerning the physical or mental health or condition of a person; (v) information regarding a person's sexual life and/or orientation; or (vi) information about the commission of, or proceedings for, any offence committed or allegedly committed by a person, or the disposal of or sentences relating to such proceedings. Under certain regulations, such as the GDPR, Sensitive personal data can only be processed if at least one of a number of strict conditions has been complied with, for example, a condition requiring the express permission of the person concerned or where the processing is required for compliance with certain legal obligations.

- **"third-party"** means a natural or legal person, public authority, agency or body other than the data subject, data controller, data processor and persons who, under the direct authority of the data controller or data processor, are authorized to process personal data.

3. Data Protection Principles

Ensono has adopted the principles outlined below, to govern its collection, use, retention, transfer, disclosure, destruction and other processing of personal data. All data users must comply with these principles when processing personal data for or on behalf of Ensono.

3.1 Principle 1: Lawfulness, Fairness and Transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means that Ensono must inform Data Subjects what processing will occur (transparency), the processing must match the description given to Data Subjects (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

3.2 Principle 2: Purpose Limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means Ensono will specify what the personal data collected will be used for and limit the processing of that personal data to the minimum necessary to accomplish the original intent for which the data were collected.

3.3 Principle 3: Data Minimization

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means Ensono must not store any personal data beyond what is required to meet the original intent for which the data were collected.

3.4 Principle 4: Data Accuracy

Personal data shall be accurate and kept up to date. This means Ensono will establish processes for identifying and addressing out-of-date, incorrect and redundant personal data.

3.5 Principle 5: Storage Limitation

Personal data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed. This means Ensono must, wherever possible, store personal data in a way that limits identification of the Data Subject or forensically erases such data upon the termination of the data processing activity.

3.6 Principle 6: Integrity and Confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing, and against accidental loss, destruction or damage. Ensono must use appropriate technical and organizational measures to ensure the integrity and confidentiality of personal data is maintained always.

3.7 Principle 7: Accountability

Ensono must implement adequate measures and be able to demonstrate compliance with the applicable data protection regulations, in relation to the processing of all personal data for which it is responsible. Such measures shall include adequate records that document the privacy program, compliance activities, consent lifecycle management, disclosures, notice of privacy practices, data processing activities and corresponding legal bases, secure development lifecycle, oversight of third parties, periodic risk assessments and any other such activities required by applicable data protection regulations.

3.8 Principle 8: International Transfers

Where personal data is subject to protection under the GDPR, Ensono will only transfer such personal data to a third country or international organization if adequate protection for the personal data is ensured (this also applies to onward transfers of personal data from the third country or international organization).

4. Lawfulness, Fairness and Transparency

Except as otherwise provided in this policy, Ensono collects and processes human resource data for the fulfillment of employment law, administration of employment benefits, promotions and other similar employment decisions. Ensono also collects, uses and may disclose personal data of clients to deliver services and or fulfil contractual obligations. Such uses or disclosures will conform to this policy, in accordance with clients' instructions and applicable law. Secondary uses of personal information for purposes that are not consistent with the original purpose for which such information was collected, are prohibited, unless data subjects opt-in or consent to such uses or disclosures.

Ensono will not process personal data in any of the use cases outlined above unless at least one of the following requirements is met:

- The data subject has consented to the processing of their personal data for one or more specific purposes.
- The processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract.
- The processing is necessary for compliance with a legal obligation to which Ensono is subject.
- The processing is necessary to protect the vital interests of the data subject or of another natural person.
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Ensono.
- The processing is necessary for the purposes of the legitimate interests pursued by Ensono or by a third-party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject).

As a data controller, Ensono will only process sensitive personal data if at least one of an additional set of conditions is met. These conditions include, for example, that:

- The relevant individual has given explicit consent to the processing for one or more specified purposes (unless applicable law prohibits this).
- The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of Ensono or of the data subject in the field of employment and social security and social protection law.
- The processing is necessary to protect the individual's vital interests or those of another person if the individual is physically or legally incapable of giving consent.

- The processing relates to sensitive personal data which have obviously been made public by the relevant individual.

When processing personal data as a data controller in the course of our business, we will ensure that appropriate conditions to justify our processing are met.

5. Purpose Limitation

In the course of business, Ensono may collect and process the personal data set out in our various privacy notices and data protection and privacy policies (together our "**Data Protection and Privacy Policies**"). This may include data we receive directly from data subjects (e.g. when they complete forms or correspond with us by mail, phone, email or otherwise) and also data that we receive from other sources (e.g. business partners, sub-contractors, credit reference agencies and others).

Data users must only process personal data for the specific purposes set out in our Privacy Policies, unless otherwise required by applicable data protection legislation. We will disclose those purposes to the relevant Data Subjects when we first collect data about them or as soon as possible afterwards.

When Ensono acts as a data processor on behalf of its clients, all data users must only process personal data for which our clients are responsible in accordance with our clients' instructions and the applicable service agreements.

6. Notifying Data Subjects

At the point of collecting personal data from data subjects, or soon after collecting personal data from third-party business partners, Ensono will generally provide the data subject its Privacy Policies, and other relevant information including:

- Our identity and contact details;
- The contact details of our data protection officer or privacy representative, if any;
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- Where the processing is based on Ensono's legitimate interests or a those of a third-party, the legitimate interests pursued by Ensono or by a third-party on its behalf;
- The recipients or categories of recipients of the personal data;
- Where applicable, the fact that Ensono may transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by relevant data protection authorities;
- The period for which your personal data will be stored, or if that is not possible, the criteria used to determine that period;
- The existence of the right to request from Ensono, access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- Where the processing is based on consent, the existence of the right for the data subject to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

- The right to lodge a complaint with a supervisory data protection authority;
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- The existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

In addition to these disclosures, the following information shall be provided, within one month of obtaining personal data, or at least, at the time of first communication, where Ensono obtained personal data from a source other than the data subject:

- The categories of personal data concerned;
- Details of the sources from which the personal data originated, and if applicable, whether it came from publicly accessible sources.

These notifications shall be performed to the extent data subjects do not already have the information.

Data users must not collect, use or otherwise process personal data in any way not provided for in our Privacy Policies. If any data user is unclear about what personal data they are permitted to process or for what purposes, they must consult with privacy@ensono.com for guidance.

7. Data Quality

Ensono will only collect personal data that is adequate, relevant and not excessive and to the extent that it is required for the specific purposes notified to the relevant data subjects. Ensono operate a clear "need to know" approach (only collecting the categories of personal data needed for business purposes). If any data user is concerned that the personal data they are processing is not adequate, relevant or may be excessive, they must consult with privacy@ensono.com.

Ensono will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data. If any data user is concerned that the personal data they are processing is not adequate or up to date, they must consult with privacy@ensono.com.

As a data controller, Ensono will not keep personal data longer than is necessary for the purposes for which it was collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required Record Retention Policy. We will also review regularly, data subjects' personal data that we hold to ensure that it is only kept for an appropriate time.

As a data processor, when Ensono has completed its provisions of services to its data controller clients, Ensono and its data users must comply with the instructions of the relevant data controller with regard to the return or destruction of the personal data for which they are responsible.

8. Processing in Line with Data Subjects' Rights

In Ensono's capacity as a data controller, we will process all personal data in line with data subjects' rights, including those set out below, to the extent required by and in accordance with applicable law (including, without limitation, in accordance with any applicable time limits and requirements regarding charges). We require all data users to respect these rights. If any data user has any questions or concerns regarding these rights, or if any data user receives a request in relation to any data subject right, he or she should consult privacy@ensono.com for guidance. Data users should under no circumstances, respond to a request from a data subject with respect to their personal data without prior authorization from privacy@ensono.com.

In Ensono's capacity as a data processor, if any data user receives a request from a data subject in relation to personal data for which an Ensono client is responsible, he or she must forward the request to privacy@ensono.com immediately. As above, under no circumstances should any data user respond to such a request without prior authorization.

Access. We will confirm to data subjects whether or not we are processing and using personal data about them at their request and, if so, provide them with access to and a copy of such personal data and the other details to which they are entitled under applicable law.

Rectification. We will correct any inaccurate personal data and complete any incomplete personal data (including by providing a supplementary statement) that we hold about individuals without undue delay at their request.

Erasure. Subject to certain exceptions, we will erase a data subject's personal data at their request without undue delay in certain circumstances, including among other things, if their personal data is no longer needed for the purposes for which it was collected or otherwise used.

Restriction. We will restrict the processing of data subjects' personal data in certain circumstances, (e.g. among other things, if they believe that their personal data held by us is inaccurate), if requested by them to do so.

Data Portability. We will respect data subjects' rights to receive personal data about them that they have provided to us in a structured, commonly used and machine-readable format and to transmit such personal data to another data controller without hindrance from us in certain circumstances.

Right to Object. We will respect data subjects' rights to object to the processing of their personal data in certain circumstances to the extent required by and in accordance with applicable law.

Right to Object to Marketing. We will respect data subjects' rights regarding the use of their personal data for direct marketing purposes. In particular, we will not begin, or we will cease processing any personal data of data subjects for particular direct marketing purposes, including profiling if it is related to such direct marketing, if at any time data subjects ask us not to do so. We will usually inform data subjects (before collecting their data) if we intend to use their data for such purposes or if we intend to disclose their information to any third-party for such purposes. Data subjects can exercise their right to prevent such processing by checking clearly labeled boxes on the forms we use to collect their data, or otherwise at any time by contacting us.

Automated Individual Decision-Making, Including Profiling. We will respect data subjects' rights (which are subject to certain exceptions) not to be subject to decisions which are based solely on automated processing of their personal data, including profiling, especially where such processing has legal or other significant effects on them. We inform data subjects about any such decisions and, subject to certain exceptions, we will usually obtain the relevant data subjects' explicit consent before making any decisions based solely on automated processing activities and put in place appropriate safeguards to protect their rights, freedoms and legitimate interests. Among other things, we ensure that data subjects can always obtain a review by one of our data users of any automated decisions and are able to express their points of view and contest any such decisions.

We will not make any automated decisions based on sensitive personal data unless we have obtained explicit consent from data subjects to do so, or this is otherwise necessary for substantial public interest reasons based on applicable law.

Scientific or Historical Research Purposes or Statistical Purposes. If relevant, we will respect data subjects' rights to object to our processing of their personal data for scientific or historical research purposes, or statistical purposes, unless this is necessary to perform tasks carried out for substantial public interest reasons.

9. How We Protect Personal Data

To safeguard the confidentiality, integrity and availability of personal data, Ensono has adopted a risk-based approach to information security. Leveraging industry-leading practices, we have implemented controls to prevent the loss, misuse, alteration, unauthorized access, or unlawful or unnecessary processing of personal data we handle, whether as a data controller, or as a data processor on behalf of our clients.

Data users must comply with all personal data security controls and procedures at all times, including those described in this policy, and any other relevant Ensono policies.

We maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

a) ***Confidentiality*** means that only data users who are authorized to process data can access such data.
b) ***Integrity*** means that personal data should be accurate and suitable for the purpose for which it is processed.
c) ***Availability*** means that authorized data users should be able to access the data if they need it for authorized purposes.

Security procedures include, without limitation:

a) ***Access controls***. Measures by which we prevent unauthorized logical or physical access to personal data or information assets. This helps ensure that only those who have a legitimate need to access personal data are able to do so.
b) ***Network security***. This includes technical controls we have implemented to safeguard the integrity of our communication networks.
c) ***Physical and environmental controls.*** Measures by which we safeguard secure-areas and ensure infrastructural stability. Such areas include data centers, and record storage locations, which are protected by layers of detective and preventive controls.
d) ***Data security***. The application of cryptographic and/or other compensating controls to protect the confidentiality and integrity of data.

e) ***Secure disposal.*** Measures by which we ensure that data storage media (including paper records) are securely disposed of when no longer needed.
f) ***Equipment.*** Measures (such as anti-malware, encryption, patching, etc.) by which we safeguard the security of our computing devices, including the secure use of such devices for data processing.
g) ***Secure storage.*** Data storage devices, including paper records are kept in a secure environment.
h) ***Password protection***. Personal data held on computers and computer systems are protected by the use of secure passwords which, where possible, have forced changes periodically, degree of complexity and length requirements. Data users are not to share their passwords with unauthorized individuals.
i) ***How We Protect Personal Data***: We undertake several industry-leading security and privacy certifications, and perform recurring validation of the operating effectiveness of controls implemented to safeguard our information assets, and to meet ISO 27001, PCI DSS, SOC 1 & SOC 2 Type II requirements.

Further details of our security procedures in respect of which all data users must comply are set out in information security policy.

10. How We Disclose and Share Personal Data

10.1 Disclosure within Ensono's group of undertakings

Ensono is a global company headquartered in Downers Grove, Illinois, in the United States of America. The personal data we collect for employment, administrative or service delivery purposes may be transferred or accessed by Ensono Entities on a need-to-know basis. For example, personal data may be transferred to, processed and stored in, the United States or any other country in which Ensono Entities maintain facilities. We will protect the privacy and security of the personal data that we collect in accordance with the terms of this policy and applicable data protection regulations. To enable transfers between the EU and the US, Ensono is certified under the EU-US Privacy Shield framework.

10.2 Disclosure to Third-Parties

To the extent that we use data processors, or any other third-parties, that have access to any personal data that we collect and/or use, we take steps to select and retain data processors capable of maintaining the privacy, security, integrity and confidentiality of any personal data to which they may have access. We will also require all data processors, by appropriate written contracts, to implement appropriate safeguards designed to protect personal data and to otherwise comply with (and ensure compliance by us with) all applicable data protection laws and all applicable provisions of this policy.

All relevant third-parties (including, without limitation, all contractors, agents, persons or entities working for us and on our behalf) must ensure that they and all their staff who process personal data on our behalf are aware of this policy and are fully trained in and are aware of their duties and responsibilities under all applicable data protection laws, this policy and any contracts or other agreements with us.

Further details of our procedures with respect to data processors are set out in our Third-Party Risk Management Policy.

10.3 Transferring Personal Data Outside the EEA

The personal data that we process may be transferred to and stored or otherwise processed at destinations outside the European Economic Area ("**EEA**"), provided that one of a number of conditions is complied with. These include, for example, conditions that:

a) The country to which the personal data is transferred has been deemed by the European Commission to provide adequate protection for the relevant individuals' rights and freedoms;
b) The relevant data subjects have given their explicit consent to the transfer, having been informed of the possible risks;
c) The transfer is necessary for one of the reasons set out in the GDPR, including the performance of a contract between us and the relevant individuals, or to protect the relevant individuals' vital interests;
d) The transfer is necessary on important public interest grounds or for the establishment, exercise or defense of legal claims;
e) EU Commission-approved standard contractual clauses have been put in place between us and the recipient; or
f) The recipient has certified to the EU-US Privacy Shield, or other legal transfer mechanism recognized by the EU Commission.

10.4 Processing from Non-Covered Jurisdictions

Unless otherwise approved by the Assurance & Advisory and Corporate Legal functions, and except as may be allowed under applicable legal transfer mechanisms secured by Ensono, there shall be no processing of EU or US personal data from Non-Covered Jurisdictions as defined in section 2 of this policy. All travels to countries with inadequate data protection regulations, practices, and or to countries that have restrictive control regimes on the use of cryptographic controls in non-military computing devices (such as Ensono laptops and or personal mobile devices), must be cleared by the Culture & People Experience function.

10.5 Disclosure to Lawful Authorities

We may disclose personal data in response to lawful requests by public authorities, in accordance with legal obligations, including to meet national security or law enforcement requirements, or requests from courts of law. To be considered, such requests have to be in writing, reasoned and lawful.

10.6 Transfer of personal data as part of Business Transfers:

As we continue to develop our business, we might sell or buy businesses or services. In such transactions, personal information generally is one of the transferred business assets, but remains subject to regulatory requirements and to the promises in any pre-existing Privacy Notice (unless, of course, the individual consents otherwise).

11. Data Protection by Design, Impact Assessments, Awareness and Training

To ensure data protection requirements are identified and addressed, the design of new systems or processes and/or changes to existing systems or processes, shall follow Ensono's secure development lifecycle. In addition, a data protection impact assessment (DPIA) must be conducted, by the Assurance & Advisory function or designee, for all new and/or revised systems or processes.

The subsequent findings of the DPIA must then be submitted to the Director of Assurance & Advisory for review and approval. Where applicable, the Information Technology (IT) function, as part of its IT system and application design review process, will collaborate with the Assurance & Advisory and Information Security functions, to assess the impact of any new technology uses on the security of personal data.

All data users are required to undergo data protection/privacy awareness and training upon intake, and thereafter, at yearly intervals. New data users must complete required training prior to being granted access to information systems other than systems required to access and complete the training.

12. Personal Data Breaches

Data users are responsible for reporting any security or other incidents involving personal data immediately to privacy@ensono.com.

A personal data breach includes any breach which results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed. If a breach occurs, we will notify impacted client(s), relevant Supervisory Authorities and any affected individuals, by and in accordance with applicable law.

13. Handling Personal Data Access Requests

Data users who receive any request, either from an individual for or about the information we hold about them, or from a third-party, should forward it to privacy@ensono.com immediately for processing in accordance with our Subject Access Request Process.

When responding to access requests, we will only disclose personal data we hold if we are able to validate the requester's identity, to ensure that information is only given to a person who is entitled to it.

Data users should refer requests to the Culture People Experience function at Associatequestions@ensono.com or to privacy@ensono.com for assistance in difficult situations. Data users should not be made to feel pressured into disclosing personal data.

14. Accountability and Records

We are responsible for and must be able to show that our data processing activities comply with all applicable data protection laws, including the GDPR. We put in place appropriate technical and organizational measures in order to achieve this, among other things by implementing and complying with appropriate data protection policies (such as this policy) and procedures.

The Global Assurance & Advisory function monitors compliance with applicable data protection laws and our data protection and privacy policies.

As a data controller, we create and maintain written internal records of all our personal data processing activities, as required by applicable law. Such records include details of: (i) our name and contact details (as data controller); (ii) the purposes of the processing; (iii) details of the data subjects and the types of personal data involved; (iv) the types of recipients that we have disclosed, or will disclose, personal data to; (v) transfers of personal data to

countries or international organizations, if relevant, including details of the countries/organizations concerned and, in certain cases, details of how adequate protection for such personal data will be ensured; (vi) time limits for erasing the relevant personal data, where applicable; and (vii) the technical and organizational security measures that we have put in place in respect of the relevant personal data.

As a data processor, we also create and maintain written internal records of all our personal data processing activities on behalf of our clients, as required by applicable law. Such records include details of: (i) the name and contact details of each data controller on whose behalf we act, and where applicable, the name and contact details of any joint data controller, and the data controller's representative and data protection officer; (ii) the categories of processing carried out on behalf of each data controller; (iii) transfers of personal data to third countries or international organizations, if relevant, including details of the countries/organizations concerned and, in certain cases, details of how adequate protection for such personal data will be ensured; and (iv) the technical and organizational security measures that we have put in place to secure the personal data.

15. Anonymization and Pseudonymization

We will anonymize personal data wherever this is necessary, considering the purposes for which the personal data was collected. We also will pseudonymize personal data where appropriate in order to help comply with all our applicable data protection obligations.

Data users are expected to consider whether anonymization or pseudonymization of personal data is possible and appropriate at all times when processing personal data.

16. Client-Hosted Data

As a hybrid technology service provider, Ensono provides and or manages computing infrastructure for clients – usually business or commercial entities, who in turn may host their commercial data (including their customers' personal data) with us. Our clients use our products and services to host, transmit or process data (including personal data) on our hosted systems ('Client-Hosted Data').

Ensono does not, and no data user shall review, share, distribute, nor reference any such Client-Hosted Data except as provided in the agreement that we have in place with the client, or as may be required by law. Nothing contained in this policy shall be construed to alter specific terms and conditions applicable to our products or services.

At all times, Ensono provides its services under the direction of its clients and has no direct relationship with the data subjects whose personal data our clients process.

17. How You Can Contact Us with Questions or Complaints

Any questions about the operation of this policy or any concerns that this policy has not been followed should be referred in the first instance to: privacy@ensono.com.

18. Governance & Policy Updates

18.1 Program Oversight

Ensono's Assurance & Advisory function is responsible for the company's data protection and privacy program. The Corporate Legal function provides legal counsel and support. In fulfilling this responsibility, the Assurance & Advisory

function shall consult regularly with the Corporate Legal function, and as appropriate, the Information Security and the Culture & People Experience functions, and other internal stakeholders.

18.2 Policy Maintenance & Regulatory Vigilance

The Assurance & Advisory and the Corporate Legal functions shall review and update this policy periodically. It is also necessary to monitor the evolution of data protection regulations in jurisdictions where Ensono does business, to ensure that this policy sufficiently articulates Ensono's position and control framework with respect to the protection of personal data.