EU-U.S. and Swiss-U.S. Data Privacy Framework Program

Cerner has been acquired by Oracle and will soon transition to the Oracle Privacy Policy. Click here to view the Oracle Privacy Policy. Please note that the provisions of Cerner's Privacy Policy below will remain active until the policy transition is complete.

Cerner publicly commits to comply with the EU-U.S. and Swiss-U.S. Data Privacy Framework Program through self-certification.

General

Cerner Corporation and its subsidiaries, listed below, ("Cerner") are committed to protecting the privacy and security of its clients, partners, and associates and, therefore, operate under a set of strict privacy principles. Cerner is required to comply with certain legal requirements in respect of any personal data it collects, holds and/or processes from the European Economic Area ("EEA") the United Kingdom, and Switzerland. These requirements are set out in the European Data Protection Directive, the European General Data Protection Regulation and the local laws of each country.

To the extent that Cerner's business operations require that personal data collected in the EEA, the United Kingdom, and Switzerland be processed in the United States of America (U.S) Cerner complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Cerner has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. Cerner has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) Program, and to view our certification, please visit https://www.dataprivacyframework.gov/. These Privacy Guidelines set forth the privacy principles Cerner follows with respect to any transfer of personal data from the EEA, the United Kingdom and Switzerland to the U.S. These Privacy Guidelines apply to all personal data received from the EEA, the United Kingdom, and Switzerland by Cerner regardless of the medium or format in which the information is stored. EEA member countries, the United Kingdom and Switzerland are hereinafter referred to collectively as 'Europe'.

Cerner is subject to the investigatory and enforcement power of the U.S. Federal Trade Commission ("FTC") relative to the Data Privacy Framework Principles.

Covered Cerner Subsidiaries

The following Cerner Corporation subsidiaries receive personal data from the EEA and adhere to the Data Privacy Framework Principles:

Cerner Health Services Inc.

Cerner's Data Processing Roles, the Types of Personal Data Cerner Receives and the Purposes for which it Processes Personal Data from the Europe:

Cerner has two separate roles when processing personal data transferred from the Europe:

First, as a data controller Cerner determines the purposes for which and the manner in which it collects, stores and processes the relevant personal data.

Cerner, as a data controller, collects and processes personal data relating to its clients, vendors, partner and associates. Personal data collected from clients, vendors and partners and processed by Cerner is limited to what is necessary in the business relationship, e.g. name, contact details, payment records, contracts and business correspondence. Where Cerner, as a data controller, receives, holds, and processes personal data from employees of Cerner's wholly-owned European subsidiaries, which are transferred to Cerner Corporation in the U.S. for purposes of human resource administration the processing of such data is subject to Cerner's HR Privacy Policy.

In addition, Cerner's goal is to provide its global clients, partners and associates with a personalized Internet experience and an Internet-based online information and communication service that delivers the information, resources and services that are most relevant and helpful to its users. In order to achieve these goals, Cerner collects and processes personal data from users during visits to its Web sites and, in particular, during a user's visits to cerner.com and/or ucern.com. As a consequence, Cerner may process personal data from European clients, partners and associates also while providing website services such as an Internet based communication platform for professionals to connect to each other. Cerner's collection and use of personal data varies based on the website services requested by the users and the users' choice of privacy options within the relevant website services. For European users of Cerner's website, the principles set out in Cerner's Privacy Policy also apply: www.cerner.com/Privacy.

Second, as a "data processor" Cerner processes personal data for its clients who are data controllers. In this capacity, Cerner does not own or determine the purposes for which it processes the personal data. Cerner's clients, as data controllers, collect the data and determine the purpose for which it is processed. Cerner receives and processes personal data for and at the instruction of its client, and in such circumstances, Cerner has no direct relationship with the individuals to whom such personal data relates. As a data processor acting on behalf of a Cerner client who is the data controller, Cerner is required to perform its services in accordance with the Data Privacy Framework Principles and its contract with the client together with any data

privacy protections incorporated therein. Cerner, however, is otherwise dependent upon its client, the data controller, to comply with applicable data protection laws at the time that the personal data is originally collected or received by the client.

As a manufacturer of clinical and management information systems, Cerner assists its clients worldwide in the implementation and support of Cerner solutions in their healthcare institution(s). Since Cerner provides implementation and support for different healthcare institutions, Cerner may receive, hold, and process personal data from European clients, including client employee name, work role, email, telephone number, work address, etc. and any patient data provided by clients for the purpose of troubleshooting specific computer system hardware and software problems and issues in accordance with business and/or service agreements. Cerner also provides managed services such as remote hosting, remote system monitoring, disaster recovery, data warehousing and application management services, in which it may act as the custodian of patient health information for certain clients. With these offerings, Cerner not only has access to provider-based personal health information, but also performs many of a provider's custodial duties as well.

These Privacy Guidelines are to be read subject to this distinction.

Notice

When Cerner, as the data controller, transfers data to a third-party, or uses the data for a different purpose than originally authorized, Cerner will notify the individual data subject in accordance with the Notice and Choice Principles of the Data Privacy Framework. Cerner informs individuals for whom it is a data controller that it participates in the Data Privacy Framework; the purpose and use of the personal information; about how individuals can contact Cerner with any inquiries or complaints; the types of third parties to which it discloses the information; the purpose for which it discloses; individuals right to access their personal data; the choices and means Cerner offers for limiting use and disclosure of the information; Cerner's independent dispute resolution body; possibility for binding arbitration; Cerner may be required to disclose personal information in response to lawful request by public authorities, including to meet national security or law enforcement requirements; and Cerner's potential liability in onward transfers to third parties.

In the event Cerner is processing personal data in the U.S. from individuals for a European client, Cerner processes the personal data in accordance with the client's instructions and informs the client that it participates in the Data Privacy Framework. The client, as the data controller, is responsible for ensuring that the personal data is processed in accordance with the rights and requirements of the individuals concerned under European data protection law.

Choice

Cerner, as a data controller, will offer individuals the opportunity to choose (through an 'opt out' choice and unless otherwise required by law) whether their personal data is (l) to be disclosed to a third party controller or (2) to be used for a purpose other than the purpose for which it was

originally collected or subsequently authorized by the individual. Individuals may opt-out by using the contact information listed below.

For sensitive personal data (that is personal data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, ideological views or activities, trade union membership or information specifying the sex life of the individual, information on social security measures, administrative or criminal proceedings and sanction which are treated outside pending proceedings, or other personal data that Cerner receives from a third party which the third party identifies as sensitive personal data), Cerner will obtain affirmative express consent (unless otherwise permitted or required by contract or law) from individuals (through an 'opt-in' choice) if such information is to be (l) disclosed to a third party controller or (2) used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt-in choice.

Accountability for Onward Transfer

Cerner does not share personal data with third party data controllers without the individual's consent, unless the requirement to disclose personal information is in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. Subject to the above, Cerner 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 Cerner 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.

Personal Data controlled by Cerner may be disclosed to service providers for processing personal data on behalf of Cerner and subject to Cerner's instruction. Cerner limits the data transferred to a service provider to data that is necessary to carry out the function Cerner has contracted with the third party data transferee to perform. Cerner will first ascertain that the third party is obligated to provide at least the same level of privacy protection as is required by the Framework Principles. Cerner will enter into a written contract with the third party, which also puts in place adequate safeguards to ensure a sufficient level of data protection, e.g. by using only service providers acting as data processors that are based within Europe or are certified under the Data Privacy Framework. Cerner will take reasonable and appropriate steps to ensure that the third party effectively processes the personal information transferred in a manner consistent with Cerner's obligations under the Principles. If Cerner learns that a third party is using or disclosing personal data in a manner contrary to these Privacy Guidelines, Cerner will take all reasonable and appropriate steps to prevent or stop the use or disclosure and remediate unauthorized processing. Third parties are also required to notify Cerner if they can no longer meet its obligation to provide the same level of protection as is required by the Framework Principles. Cerner will provide a summary or a representative copy of the relevant privacy provisions of its contract with that third party to the Department upon request.

Cerner also 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. In cases of onward transfer to third parties of data of European individuals received pursuant to the Data Privacy Framework, Cerner is potentially liable.

Data Security

Cerner takes all reasonable and appropriate measures to protect personal data from loss, misuse and unauthorized access, disclosure, alteration and/or destruction, taking into due account the risks involved in the processing and the nature of the personal data. Cerner accordingly has put in place appropriate physical, electronic and managerial security measures to safeguard and secure any personal data under Cerner's control from loss, misuse and unauthorized access, disclosure, alteration and / or destruction.

Data Integrity and Purpose Limitation

Cerner processes personal data only in a way that is compatible with and relevant to the purpose for which it was collected or subsequently authorized by the client data controller or individual. To the extent necessary for those purposes, Cerner takes reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. Cerner will adhere to this Principle for as long as it retains such information.

Access

Cerner acknowledges that, subject to certain legal limitations, individuals have the right to access the personal information/data that we maintain as a controller about them. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data held by Cerner as a data controller, should direct his query to the contact information listed below. Cerner will respond to such request within a reasonable timeframe. When acting as a data processor, Cerner supports any access request addressed to a Cerner client.

Recourse, Enforcement and Liability

Cerner uses a self-assessment approach to verify compliance with the Data Privacy Framework Principles and periodically conducts objective reviews that its published privacy policies regarding personal information received from Europe are accurate, comprehensive for the information intended to be covered, prominently displayed, completely implemented and accessible, and in conformity with the Framework Principles. Cerner periodically trains employees on its privacy policies regarding personal information during implementation and disciplines them for failure to follow the policy.

In compliance with the EU-U.S. and Swiss-U.S. Data Privacy Framework Principles, Cerner commits to resolve complaints about privacy and collection or use of personal information. EEA or Swiss individuals with inquiries or complaints regarding this privacy policy should first

contact Cerner using the contact information provided below before proceeding to independent recourse mechanisms. Cerner will investigate and attempt to resolve any complaints and disputes regarding use and disclosure of personal data in accordance with the Framework Principles. Cerner will respond to complaints within 45 days of receiving a complaint, as required by the Framework Principles.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Cerner commits to refer unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF to BBB EU PRIVACY FRAMEWORK, a non-profit alternative dispute resolution provider located in the U.S. and operated by the Council of Better Business Bureaus, an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit https://bbbprograms.org/programs/all-programs/dpf-consumers for more information or to file a complaint. The services of BBB are provided at no cost to you.

Should your complaint remain fully or partially unresolved after a review by Cerner, BBB EU and the relevant DPA, you may be able to, under certain conditions, seek arbitration before the Data Privacy Framework Panel. For more information, please visit https://www.dataprivacyframework.gov.

An individual who decides to invoke this arbitration option must take the following steps prior to initiating an arbitration claim: (l) raise the claimed violation directly with Cerner and afford Cerner an opportunity to resolve the issue within 45 days of receiving the complaint; (2) make use of the independent recourse mechanism, BBB EU PRIVACY; and (3) raise the issue through their EU DPA, the United Kingdom Information Commissioner's Officer or the Swiss Data Protection and information Commissioner to the Department of Commerce and afford the Department of Commerce an opportunity to use best efforts to resolve and respond to the DPA within 90 days.

Human Resources Data

Cerner, as a data controller, also commits to cooperate with the EU data protection authorities, the United Kingdom Information Commissioner's Office and the Swiss Federal Data Protection and Information Commissioner ("FDPIC") with regard to human resource data transferred from European the context of the employment relationship. Where an organization in Europe transfers personal information about its employees (past or present) collected in the context of the employment relationship, to Cerner, the collection of the information and its processing prior to transfer is subject to the national laws of the European country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected. When receiving employee information from Europe, under the Data Privacy Framework Cerner may disclose it to third party data controllers or use it for different purposes only in accordance with the Notice and Choice Principles.

If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed by Cerner, and your inquiry or complaint involves human resource data, you may have your complaint considered by an independent recourse mechanism: for EU/EEA Data Subjects, a panel established by the EU data protection authorities ("DPA Panel"), and for Swiss Data Subjects, the Swiss FDPIC. To do so, you should contact the state or national data protection or labor authority in the jurisdiction where you work. Cerner agrees to cooperate and comply with the decisions of the DPA Panel and FDPIC.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Cerner commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Swiss Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of human resources data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF in the context of the employment relationship.

Contact Information

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Cerner commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU and UK individuals and Swiss individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF should first contact Cerner at:

In Europe:

Cerner HS Deutschland GmbH
Email: PrivacyOffice@cerner.com

In US:

Cerner Corporation
Email: PrivacyOffice@cerner.com

Amendments

These Privacy Guidelines may be amended from time to time consistent with the requirements of the Data Privacy Framework. We will post any revised policy on this website.

Revised Date: August 30, 2023