INFORMATION SHEET

Medidata’s GDPR Data Processing Exhibit (DPE) with the EC’s Standard Contractual Clauses (SCCs)

Medidata is pleased to provide its Data Processing Exhibit (DPE), incorporating the European Commission’s (EC’s) latest approved Standard Contractual Clauses (SCCs) (under Commission Implementing Decision (EU) 2021/914 of 4 June 2021). The SCCs have long been an important legal means to transfer your personal data from the EEA to Medidata’s US-based hosting. Our DPE meets the SCCs requirements, while continuing to track all of the GDPR’s requirements for our services (see the chart on next page). This Information Sheet describes how the SCCs and ongoing GDPR requirements apply to you and to us, explains how our DPE addresses these requirements, and answers some frequently asked questions.

How the GDPR applies to you and to Medidata

The GDPR applies to your use of the Medidata Clinical Cloud® for clinical trials having patients, employees or site users located in the EEA. Medidata is the industry leader in data protection and maintains a robust GDPR compliance program in alignment with the current SCCs. Below are some of the ways that Medidata helps you meet key GDPR requirements:

- “Transfer Impact Assessment”: The latest SCCs require both our customers and Medidata to conduct a Transfer Impact Assessment (TIA), in line with the EDPB’s “Guidance on the Essential European Guarantees for surveillance measures”. Our TIA provides assurance that the transfer of your data to the Medidata Clinical Cloud - hosted in the United States - meets the new SCC standards. Our TIA (included within our DPE) along with our Transfer Impact Whitepaper (available at our Trust & Transparency Center, www.medidata.com/trust) provides you with the necessary information to conduct your own TIA, as required by the new SCCs.
- Additional safeguards for sensitive data: The current SCCs require Medidata to provide “additional safeguards” where use of our services requires the transfer of sensitive data to us, namely your clinical trial data. As set out in our new DPE, these safeguards include that your clinical trial data is pseudonymized and that we encrypt it both at rest and in transit.
- Privacy by Design: As the GDPR requires, our services are designed from the outset based on data protection principles, e.g., restricting personal data processing to only what is necessary for the processing purpose.
- Rights for EU individuals: The GDPR provides expanded rights for EU individuals such as deletion, restriction of processing, and portability of their personal data. While some of these rights are inapplicable in our clinical trials context, Medidata assists our customers in complying in full.
- Security: Medidata’s data protection and security standards are confirmed by rigorous third-party compliance audits and penetration testing. Our platform provides encryption in transit (with Transport Layer Security) and encryption at rest for EDC data (with AES-256 encryption).

GDPR Concepts

Our roles – controller and processor
Medidata is the data processor of your personal data. You are the data controller, and your instructions to us for processing your personal data are our MSA, Sales Orders, and the DPE.

Personal data and pseudonyimzation
Both your patient data and data about your authorized users are personal data. The GDPR recognizes pseudonyimzation as a safeguard that protects personal data – as your clinical patient data is key-coded, this protection is applicable for the new SCCs.

Subprocessors
Through the DPE we receive a general authorization from you, provided there is prior notice and the opportunity to object. Medidata’s GDPR-ready DPE meets subprocessor requirements with SaaS-industry typical terms.

Medidata Security Certifications & Standards

Medidata has a long history of successful independent certification and attestation for security, confidentiality, availability, processing integrity, and privacy controls.

Visit our Trust & Transparency Center at www.medidata.com/trust to review our reports and certifications in detail.

SOC 2 Type 2: Medidata publishes a Service Organization Controls 2 (SOC 2) report conducted in accordance with SSAE 16 and the ISAE 3402 professional standards. The SOC 2 report audit attests that Medidata control objectives are appropriately designed and operating effectively, including in compliance with the AICPA **Privacy Trust Services Criteria,** an *industry first.*

ISO Certification: Medidata maintains International Standards Organization (ISO) certifications addressing security and privacy management best practices and comprehensive controls:

- **ISO 27001:2013**
  Information Security Management
- **ISO 27018:2014**
  Privacy of Personal Data in the Cloud
- **ISO 27701:2019**
  Privacy Information Management

How our DPE addresses the GDPR and SCC requirements

The below chart demonstrates how our DPE addresses GDPR and SCC requirements for our services to you.

GDPR/SCC	Topic	Medidata's DPE
Art. 28(3)	Subject-matter, duration, nature and purpose of the processing	Sec. 2.1-2.3
Art. 28(3)	Type of personal data, categories of data subjects	Sec. 2.4
Art. 28(3)(a)	Processing only on controller's instructions	Sec. 3.1, 3.3
Art. 28(3)(b)	Personnel authorized to process data are bound to confidentiality obligations	Sec. 3.4
Art. 28(3)(c)	Taking measures required by Article 32 (security)	Sec. 4.1
Art. 28(3)(d)	General authorization for engaging subprocessors	Sec. 5.1
Art. 28(3)(e)	Assisting controller with appropriate technical and organizational measures, insofar as possible, with controller's data subject request responsibilities	Sec. 6
Art. 28(3)(f)	Assisting controller in ensuring compliance with Art. 32 (security)	Sec. 4.3, 10.2
Art. 28(3)(f)	Assisting controller in ensuring compliance with Art. 33 (breach notification to supervisory authority)	Sec. 7.2
Art. 28(3)(f)	Assisting controller in ensuring compliance with Art. 35 (DPIA)	Sec. 7.1
Art. 28(3)(f)	Assisting controller in ensuring compliance with Art. 34 (communicating breach to data subjects)	Sec. 7.2-7.3
Art. 28(3)(g)	Deletion or return of personal data	Sec. 8
Art. 28(3)(h)	Making available information to demonstrate compliance with Article 28, including inspections and audits	Sec. 9
SCC Clause 8.7	"Additional safeguards" applied by the data importer where the transfer involves sensitive data	Attachment B
Art. 46(2)(c)	Appropriate safeguard for data transfer by means of standard data protection clauses adopted by the European Commission (Standard Contractual Clauses)	Attachment C
SCC Clause 14(d)	Transfer Impact Assessment (TIA): *SCC requirement for a documented assessment of the relevant laws and practices of the importing country to satisfy that the data importer will be able to fulfill its obligations under the SCCs*	Attachment D

Answers to some frequently-asked questions

Where can I find Medidata's DPE, certifications, and learn more about Medidata's data protection program?

Please visit medidata.com/trust for links to our GDPR-ready DPE and SCCs, our Transfer Impact and Information Security whitepapers, and our industry-leading SOC2+ attestation and ISO certifications. You can also contact your account manager.

Why use Medidata's DPE, and not my company's?

We understand the criticality of meeting the GDPR's rigorous data protection requirements and the efforts many of our customers have made related to the GDPR, including creating their own vendor-facing data processing terms. However, Medidata's DPE not only addresses all of the GDPR's requirements (see the chart above), but it is specific both to our services and to our MSA with you. Our approach of relying on one DPE is consistent with Software-as-a-Service (SaaS) providers across different industries. In addition, our DPE explicitly avoids any modification of the commercial terms in our MSA with respect to data protection, such as representations, warranties, liability or indemnification – these are addressed in the MSA.

Why is Medidata's DPE set up to be automatic and acceptable?

Medidata's ability to provide a consistently high level of service across its entire customer base relies on the standardization of processes for data privacy and security. Medidata has gone to great lengths to create and benchmark a contract and contracting process that is customer-friendly in order to reduce the amount of time and effort needed to finalize agreements. We have taken our customers' common requests and objections and proactively addressed them in our standard DPE. Notably, the terms in our DPE do not change any liability limitations or other significant terms in our MSA (Medidata only takes on additional responsibilities and obligations).

Can we attach our own security/privacy exhibits to the DPE?

No, Medidata’s ability to provide a consistently high level of service relies on the standardization of our processes, including security and data privacy methodologies. Thus, our customers adopt Medidata’s description of our security / privacy controls. Medidata is transparent upfront with our controls (see Medidata’s Security Exhibit, DPE, SOC-1 and SOC-2 audit reports, etc.) and contractually commits that in no event shall Medidata materially diminish the protections provided by its controls.

What personal data is in scope of the DPE?

In its role as processor, Medidata only processes key-coded clinical trial data (pseudonymised) in its provision of services to customers.

What are the required “additional contractual measures” for third-country transfers and does Medidata satisfy them?

The additional contractual measures recommended by the EDPB mainly require: (i) that the data importer and exporter assess and warrant that the laws of the importing country will prevent the importer from fulfilling its GDPR obligations; and (ii) that the data importer notify, to the extent legally possible, the data exporter of any binding requests from public authorities, and follow instructions to object. These measures are satisfied in the current SCCs, in Clauses 14 and 15, respectively. By adopting the current SCCs, no further “additional contractual measures” are required.

Is Medidata compliant with the Data Privacy Framework (DPF)?

Medidata complies with and is certified to the EU-U.S. DPF, along with the UK Extension and Swiss-U.S. DPF. Medidata has a long history of compliance with EU-US data transfer frameworks; including compliance with Safe Harbor, then Privacy Shield, and now the DPF. While we enter into the SCCs with all of our customers, our DPE states that in cases where a transfer is covered by a suitable framework, such as the DPF, then the framework will apply over the SCCs.

Why use a Subprocessor General Authorization approach?

Medidata uses the written general authorization process to ensure it can efficiently add new services and subprocessors to all of its 2,000+ customers. This process provides timely prior notice and opportunity to object to our customers before a subprocessor begins processing of their data. Medidata’s current subprocessor list can be viewed here.

What happens to my data at termination or expiration of the Agreement?

Medidata’s customers own their data at all times. In compliance with ICH GCP and other regulatory requirements that apply to the Services, clinical trial data will be retained by Medidata for 25 years after the end of the applicable clinical trial.

How can I provide you with my preferred incident notification email?

If not previously provided or updated, please contact us at dataprivacy@medidata.com with the email at which your company prefers to be notified in the event of a data protection incident. You can also contact your account manager.