

# Medidata's updated GDPR Data Processing Exhibit (DPE) with the EC's new Standard Contractual Clauses (SCCs)

Medidata is pleased to provide its updated Data Processing Exhibit (DPE), incorporating the European Commission's recently approved Standard Contractual Clauses (SCCs). The SCCs have long been an important legal means to transfer your personal data from the EEA to Medidata's US-based hosting. The new SCCs build on existing GDPR data protections by requiring Trial Impact Assessments (TIAs) by both Medidata and our customers, as well as the use of "additional safeguards" for sensitive data. Our new DPE meets these requirements, while continuing to track all of the GDPR's requirements for our services – see the GDPR Article 28 chart below. This Information Sheet describes how the new 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 already in alignment with the new SCCs. Below are some of the ways that Medidata helps you meet key GDPR requirements:

- **New "Transfer Impact Assessment":** The new 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 with our DPE) along with our Transfer Impact Whitepaper (available at our Trust & Transparency Center, [www.medidata.com/trust](http://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 new 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 pseudonymization

Both your patient data and data about your authorized users are personal data. The GDPR recognizes pseudonymization 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](http://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 new SCCs requirements

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

GDPR	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): <i>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 fulfil its obligations under the SCCs</i>	Attachment D

## Answers to some frequently-asked questions

### 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 newly approved SCCs, in Clauses 14 and 15, respectively. By adopting the new SCCs, no further "additional contractual measures" are required.

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

Please visit [medidata.com/trust](https://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 providing a 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.

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

If not previously provided or updated, please contact us at [dataprivacy@medidata.com](mailto: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.