Medidata's new GDPR-ready Data Processing Exhibit (DPE)

With Europe's new, comprehensive data privacy law, the General Data Protection Regulation (GDPR), going into effect on May 25, 2018, Medidata is providing a new Data Processing Exhibit (DPE) to help our customers address their GDPR data protection obligations. Our DPE tracks all of the GDPR's requirements for our data processing services to you – see the chart based on GDPR Article 28 below. This Information Sheet describes in greater detail how the GDPR's requirements apply to you and to Medidata, how our DPE addresses specific GDPR requirements relating to our services, 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 EU. Because Medidata has long taken data protection seriously, the GDPR does not change the broad scope of data processing services we provide to you. Instead, the GDPR builds on the existing European data protection laws in a few key ways:

- Accountability and Data Protection Impact Assessments: Controllers must account for how they process and protect personal data; we are responsible for assisting you with this obligation. Medidata provides uniform materials for all of our products and business processes to assist you with your accountability and your data protection impact assessment obligations, namely, our current security certifications and reports (e.g., SOC 1 and SOC 2 audit reports, ISO/IEC 27001:2013 Certification) and our Privacy Shield certification.
- Privacy by Design: The GDPR requires our systems to be designed from the outset based on data protection principles, such as restricting the processing of personal data to only that which is necessary for the purpose of the processing.
- Rights for EU individuals: The GDPR provides expanded rights for EU individuals such as deletion, restriction of processing, and portability of their personal data. Some of these rights (such as the "right to be forgotten") are likely excluded in our clinical trials context; for others, Medidata will assist our customers in complying with data subject requests.
- Security: Medidata's data protection and security standards are confirmed by rigorous third-party compliance audits for security, confidentiality, availability, processing integrity, and privacy controls. Our platform provides encryption in transit (Transport Layer Security (TLS) with minimum key length of 256 bits); encryption at rest for EDC data using AES (256 bit keys) will be in place by May 25th.

GDPR Concepts

The GDPR uses data protection concepts that are mostly similar to those in current EU data protection law – Directive 95/46/EC. Below are the concepts that are most relevant to our services to you.

Our roles – controller and processor
Just as under the Directive, 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
For our services to you, the meaning of personal data under the GDPR is the same as under the Directive. Both your patient data and data about your authorized users are personal data. The GDPR now recognizes pseudonymization as a safeguard that protects personal data – as your clinical patient data is key-coded, this protection is applicable.

Cross-border transfers & data location
Just like the Directive, the GDPR requires a legal basis to transfer your personal data to Medidata's datacenter in the US. Our DPE uses Medidata's Privacy Shield certification (view it on PrivacyShield.gov) and also offers the Standard Contractual Clauses. You may also rely on consent.

Subprocessors
The GDPR introduces a new concept for a data processor's use of subprocessors – a general authorization from you, provided prior notice and the opportunity to object. Medidata's GDPR-ready DPE meets this new requirement with SaaS-industry typical terms.

Breach notification
The GDPR introduces a new, specific timeframe for controllers to alert data protection authorities of material privacy breaches. It also requires processors to alert controllers "without undue delay". Our DPE tracks this GDPR language and assists you in meeting your notice requirement – your clock starts when we alert you of a confirmed breach. *Please make sure to provide us with your preferred incident notice email*.

Data subject rights
The GDPR introduces new rights for data subjects, i.e. the natural persons whose personal data is processed. However, properly consented patients who chose to withdraw consent likely do not have a right to "be forgotten." This is because clinical data provided up to the point of withdrawal is protected under the GDPR. Medidata will help you with data subject rights requests that you may receive.

How our DPE address specific GDPR requirements

We have created the below chart to make it easy for you to review how our DPE addresses the GDPR's requirements that relate to 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, 3.2
Art. 28(3)(b)	Personnel authorized to process data are bound to confidentiality obligations	Sec. 3.3
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. 34 (communicating breach to data subjects)	Sec. 6
Art. 28(3)(f)	Assisting controller in ensuring compliance with Art. 35 (DPIA)	Sec. 7
Art. 28(3)(f)	Assisting controller in ensuring compliance with Art. 36 (Prior Consultation)	Sec. 7
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

Answers to some frequently-asked questions

Where can I find Medidata's DPE and Security Certifications?
Links to Medidata's GDPR-ready DPE, the Standard Contractual Clauses, our independent third-party security reports, as well as our Information Security Whitepaper, are available at https://www.mdsol.com/en/security-certifications. You can also contact your account manager.

Does Medidata's DPE apply to my clinical trials across the globe?
Yes. The Medidata Clinical Cloud optimizes global clinical trials and our DPE supports the data protection requirements for those trials. Because the GDPR is consistent with the world's most stringent data privacy laws, our DPE provides a robust global framework by tracking all of the GDPR's requirements for data processors (see above Chart).

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 already made to prepare for 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 also specific to our services and our MSA. 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 our MSA. For these reasons, we provide our DPE in a PDF format, without the ability to modify.

How can I provide you with my preferred incident notification email?
Please contact us at dataprivacy@mdsol.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.