ENTRUST

IDENTITY ESSENTIALS

PRIVACY STATEMENT

Contents

Identity Essentials Privacy Statement

Last Updated: May 26, 2021

Identity Essentials (Formerly SMS Passcode)

This product privacy notice describes how Identity Essentials collects and processes personal data pursuant to applicable data privacy laws.

Description

Identity Essentials is a multi-factor authentication (MFA) solution for companies seeking a fast, cost-efficient solution to secure worker identities and enable their remote workforce. Identity Essentials is an on-premises MFA solution that can be extended to the cloud with Identity as a Service.

Personal Data Collection and Processing

Personal Data Type	Mandatory/Optional	Purpose for Processing
Audit information (user actions such as authentication times, self-management actions)	Mandatory	User authentication
Custom Attributes (as designed by customer)	Optional	User authentication
Email Address	Optional	User authentication
IP Address	Optional	User authentication, Auditing
Name	Optional	User authentication
OTP, Hardware Token, Soft Token, Email	Optional	User authentication
Password	Optional	User authentication
Phone Number	Optional	User authentication
User ID	Mandatory	User authentication

Retention Period

The personal data captured by Identity Essentials is kept until the user is deleted by an administrator. Any other retentions periods are set by the Customer.

Use of Sub-Processors

For the current list of sub-processors, visit https://www.entrust.com/legal-compliance/privacy/sub-processors.

International Data Transfers

Identity Essentials is an on-premise solution which allows customers to elect where to store or transfer data.

An optional component of Identity Essentials is available for Customers who would like to use Entrust Cloud Dispatch. This optional component uses Microsoft Azure to dispatch one time passwords (OTPs) to the application via SMS or voice. Customers can select to have their data hosted in either the United States or the Netherlands. If the Customer is located in a different country than the one they have selected for hosting, there may be cross-border transfers of personal data. Any cross-border transfers of personal data associated with this optional component are made in accordance with relevant data privacy law requirements (e.g., the Standard Contractual Clauses for EU personal data transferred out of the EU).

Data Protection Measures

For more information on how Entrust processes personal data collected by this product, please refer to Schedule 2, Appendix 2 of our standard customer data processing agreement (DPA) found here.

Data Privacy Rights

The Customer is the data controller for all personal data collected by Identity Essentials. Entrust Corporation, as the data processor, will assist the Customer, to the extent reasonable and practicable, in responding to verified data subject access requests the Customer receives with respect to Identity Essentials.

Amendments to this Privacy Statement

We reserve the right to amend this Product Privacy Statement from time to time as our business, laws, regulations and industry standards evolve. Any changes are effective immediately following the posting of such changes to https://www.entrust.com/legal-compliance/data-privacy/product-privacy-notices. We encourage you to review this statement from time to time to stay informed.

Contact Information

For questions about this product privacy notice, please contact privacy@entrust.com. For Entrust Corporation’s general privacy notice, please click here.