Security

Overview

DTEN is on a mission to make face to face communication experience. To do that, we need to make sure your data is secure, and protecting it is one of our most important responsibilities. We're committed to being transparent about our security practices and helping you understand our approach.

DTEN uses industry standard encryption to protect your data in transit such as the transport layer security ("TLS") or secure socket layer ("SSL") technology. We will continue to improve our transport security posture to support our commitment to protecting your data.

We monitor the cryptographic industry trend and work promptly to update the service to respond to new cryptographic weaknesses and implement evolving best practices.

More information about AWS security and compliance, see here.

Content and Information Security

You data is safe with us. DTEN will not sell or rent your information. You have the control over who sees your content. We do not have the permission to access to your content unless you agreed to give us permission.

Below are the events that we may disclose your information:

- We share your information with Service Providers who process data on our behalf, such as credit card processors and customer management systems. For example, these Service Providers help us:
    - Operate, develop, and improve the features and functionality of the Service
    - Complete your payment transactions
    - Fulfill your sales and support requests
    - Communicate with you as described elsewhere in this policy
- We also may share information about you with third parties whenever you consent to or direct such sharing. This includes, for example, if you connect your DTEN account with a third-party app.

Email Security

DTEN Note allows you to export DTEN Note note to PDF on the application. Exported PDF can be sent via email to you using a software that DTEN built internally. DTEN email system is secured by HTTPS with AWS security. When you receive an email from DTEN, we want you to be confident that it really came from us and the email from us is legitimate. Every email we send from the following domains:

DTEN:
@dten.com
@mail.dten.com
@cn.dten.com

Displayten:
@displayten.com
@mail.displayten.com
@cn.displayten.com

Activity Logging and Tracking

The DTEN service performs server-side logging of client interactions with our services. This includes web server access logging, as well as activity logging for actions taken through our API. We also collect event data from our client applications.

We use cookies and similar tracking technologies to help us understand how you use our website, our mobile applications, our desktop clients, and our browser extension products. We collect information about the number and type

of devices you use to connect to the Service, as well as information about the operating systems on those devices (e.g., iOS, Android, Windows) to ensure the Service works as expected for you. By providing us with information about how you interact with our Service, these tools help us learn how to make the DTEN experience even better and customize our communications with you. On our website, for example, these technologies can tell us things like how you arrived at the site, if you have visited the site before, how long you stay on the site, and which pages you visit. They also provide us with general information about where in the world you may be located.The following analytics technologies are in use:

- Google Analytics. To learn more about Google Analytics and your privacy, visit the “How Google uses data when you use our partners' sites or apps” page at www.google.com/policies/privacy/partners/. To opt out of being tracked by Google Analytics when using our website, visit http://tools.google.com/dlpage/gaoptout.
- Internal Analytics. AWS Database.

We may use marketing automation services, such as Salesforce Marketing Cloud. Such services use cookies to provide us with information on how you interact with our website and marketing emails to help us refine our marketing efforts and provide more relevant information to you.

Transport Encryption
DTEN uses industry standard encryption to protect your data in transit. This is commonly referred to as transport layer security (“TLS”) or secure socket layer (“SSL”) technology. We plan to continue improving our transport security posture to support our commitment to protecting your data. If your mail service provider supports TLS, your email will be encrypted in transit, both to and from the DTEN service. We protect all customer data flowing between our data center and the AWS Platform using AWS encryption or TLS. Further information about Data transfer and transport encryption via AWS can refer to here.

Encryption at Rest
DTEN uses the Amazon Web Services Platform (“AWS”). Customer data that we store in AWS will be protected using AWSs built-in encryption-at-rest features. More technically, we use AWS' server-side encryption feature with Amazon-managed encryption keys to encrypt all data at rest. You can find additional information on how encryption at rest protects your data here.

Data Retention and Deletion/ Destruction
DTEN will not retain your exported content encrypted on AWS Storage. Encrypted content will be permanently deleted on the AWS Storage server immediately when the meeting session ends.

More information about AWS security and compliance can be found here.

If you have questions, please contact us at legal@dten.com.

DTEN

* Content may be subject to change without notice. Please go to dten.com for the latest information.
* Updated: 2018-08-14