Privacy and Security Through APIs

October 9, 2019

DATAGUISE

Agenda

1. How do security and privacy regulations affect businesses?
2. What role does technology play in helping organizations comply with regulations?
3. What APIs can make organizations secure and compliant, and how?

DATAGUISE

New Data Security and Privacy Regulations

1. **GDPR**
2. **CCPA**
3. **HIPAA**
4. **SOX**
5. **PII**
6. **PCIDSS**
7. **Nevada Privacy Law**
8. **Thailand Personal Data Protection**
9. **Mexico Federal Data Protection**
10. **Brazil's LGPD**
11. **Australia Privacy Principle**
12. **Data Privacy Act – Philippines**
13. https://iapp.org/media/pdf/State_Comp_Privacy_Law.pdf

DATAGUISE

How do these regulations affect businesses

Businesses are on the hook to:

1. **Find and keep track of personal data that they store in their repositories**
2. **Use this personal data only if necessary and only for the stated purposes**
3. **Protect personal data (masking, encryption)**
4. **Let customers know what personal data they have about them (when requested) – Right of Access**
5. **Erase customer's personal data upon request (within legal limit) – Right to Erase**

Unlike before, penalties are attached to violations of any of these provisions.

DATAGUISE

Why APIs for Data Security and Privacy?

1. None of these actions – finding the personal data, pseudonymizing it, retrieving data about a particular customer – is easy to program into an application.
2. For example, finding credit card numbers or finding addresses
3. Further, new personal information types are defined as more regulations are passed around the world
4. An API service that already has all this logic built-in, and that gets frequently updated with the latest regulations will keep your applications up-to-date.

Dataguise PoD API

The Dataguise Privacy on Demand API does the following:

1. **Lets you define a policy, consisting of personal data identifiers that you wish to find.**
2. **Finds personal data as defined in your policy**
3. **Optionally protects the personal data at the element level**
4. **Many different protection options available**
   a) **Masking options**
   b) **Encryption**

DATAGUISE

Sample API Usage

```
sampleData = "My ssno is 528679845 and CCNO is 5105105105105100 and my name is John Smith";
DetectionResult dr = DetectionService.detectSensitiveData(sampleData);
List lstdata = dr.getSensitiveDataInfo();
for (SensitiveData sd : lstdata) {
     System.out.println(" Start Index : " + sd.getStartIndex()); System.out.println(" End Index : " +
         sd.getEndIndex());
      System.out.println(" Sensitive Data : " + sd.getToken());
      System.out.println(" Sensitive Type Id: " + sd.getType());
      SensitiveTypesEnum sentype = sd.getSensitiveTypeEnum();
      if (sentype != null) {
             System.out.print(sentype.getValue() + " - ");
              System.out.print(sentype.name());
       } // if
 } // for
```

DATAGUISE

Dataguise PoD API - Availability

Currently in beta
Hosted in Apigee
Check us out at: https://pod-eval-apis.apigee.io/

DATAGUISE

Dataguise Features

Detect

Find sensitive data in structured, unstructured and semi-structured content

- Discover and classify sensitive data
- Inventory identities and requirements
- Process data subject access requests

Protect

Remediate your sensitive data exposure for risk and compliance obligations

- De-identify personal data
- Encrypt at the element level
- Track cross-border transfers
- Track third-party disclosures

Monitor

Track how and where sensitive data is being accessed

- Notify on retention limits
- Alert on compliance violations
- Alert on inappropriate user access