Castle

GDPR Automation Solution

This is an extension to the GDPR API project delivered in 2019, allowing for an alternative delivery method for User Data Access Requests. The new method will give customers a more programmatic way of downloading GDPR subject access data.

Proposed solution

The main motivation for the original approach (using a trusted email like privacy@example.com for delivery), is to limit access of this feature so that not everyone with dashboard and API access is able to extract sensitive user data in bulk.

In order to preserve this behavior, we've created a special GDPR webhook endpoint which will be configured manually by a Castle representative, upon request of the Customer. As with the current GDPR functionally, this endpoint will **not** be configurable through the dashboard.

Setup flow

1. The customer reaches out to Castle and requests enabling of the GDPR webhook
2. Castle will ask a trusted contact to provide a URL for receiving the webhooks, with the possibility to use different ones for each environment that the customer has created. The customer should explicitly list which environments and URLs should be configured, with App IDs matching the ones in the dashboard settings
3. Castle enables the webhook(s) for each requested environment
4. A confirmation email is manually sent back to the trusted contact, confirming that the URL(s) has been configured.

Request Flow

1. Customer sends a subject access request to the GDPR API endpoint
2. Upon receiving a request, Castle will compile records pertaining to the associated user
3. When the data compilation is completed, Castle will send the data as follows:
    a. If a privacy email is configured: An email will be sent to your privacy email address on file. The email will contain a data download link that will expire after 48 hours.
    b. If a GDPR webhook is configured: A webhook will be sent to the URL destination that was provided. A signature will be sent in the X-Castle-Signature header of the outgoing request exactly the same way as for the standard webhooks.

Sample webhook contents:

```
{
    "api_version": "v1",
    "app_id": "382395555537961",
    "type": "$gdpr.subject_access_request.completed",
    "created_at": "2019-12-01T19:38:28.483Z",
    "data": {
        "id": "test",
        "download_url": "https://url/user.zip"
        "download_url_expires_at": "2020-12-12T00:00.00Z"
        "user_id": "2",
        "user_traits": {
            "id": "2",
            "email": "email@example.com"
        }
    }
}
```