{databrackets cybersecurity • audit • compliance}

# GDPR Report - Demo

databrackets

June 5, 2020

Prepared By:
Srini Kolathur

In Consultation With:
Joe Mitch - Director - Company 1

{databrackets} cybersecurity · audit · compliance

# Contents

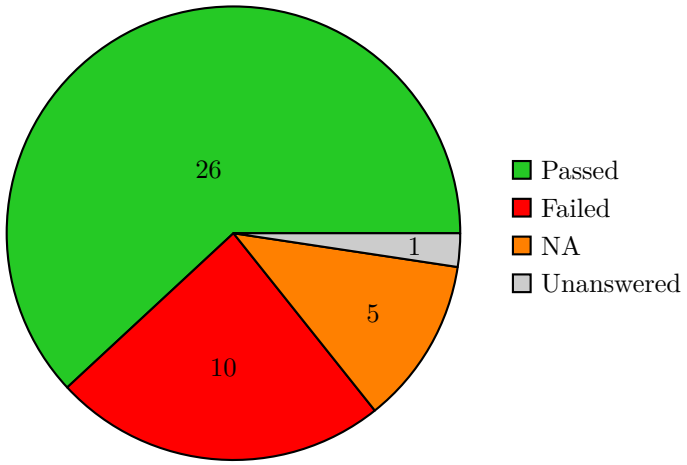
databrackets cybersecurity · audit · compliance

# 1 Executive Summary

72

**Assessment Score**

DISCLAIMER - Information provided by the customer for this assessment was not independently verified by our consulting team; the customer has provided details about their operation to the best of their knowledge. These reports and recommendations are for evaluation purposes only and not intended to be construed as legal advice. The customer is advised to consult with attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on the company and/or its personnel.




# 2 Results Overview

| Module | Incl in Assessment | # Areas Covered | Pass % | Failure % | Not Applicable |
|---|---|---|---|---|---|
| Scoping Exercise | Yes | 7 | 100% | 0% | 5 |
| Notice and Privacy Policy | Yes | 8 | 88% | 12% | 0 |
| Data Collection and Processing | Yes | 4 | 75% | 25% | 0 |
| Transfer of Personal Data | Yes | 2 | 100% | 0% | 0 |
| Data Subjects Rights | Yes | 5 | 60% | 40% | 0 |
| DPO and Governance | Yes | 3 | 67% | 33% | 0 |
| Sub-Processors | Yes | 2 | 50% | 50% | 0 |
| Storage and Archiving | Yes | 2 | 50% | 50% | 0 |
| Technical Controls | Yes | 2 | 0% | 100% | 0 |
| Breach Notification | Yes | 2 | 100% | 0% | 0 |
| Training | Yes | 1 | 100% | 0% | 0 |
| Artifacts | Yes | 4 | 75% | 25% | 0 |

databrackets cybersecurity · audit · compliance

## 3 Action Plan Summary

| Module | Question | Action Plan | Priority | Due Date | Status |
|---|---|---|---|---|---|
| Artifacts | Artifact 4 - Please provide a copy of the current .. | Review and update the existing contracts with proc.. | Medium | 2020-11-08 | In Progress |
| Data Collection and Processing | Do you maintain records of your processing activit.. | Data processors must m.. | Medium | 2020-09-01 | In Progress |
| Notice and Privacy Policy | Does the Privacy Notice describe the types of pers.. | Ensure that privacy no.. | Medium | 2020-11-08 | In Progress |
| Data Subjects Rights | Do you provide data subjects with options to manag.. | Organizations must have mechanism in place where d.. | Medium | 2020-11-08 | In Progress |
| Data Subjects Rights | Do you have process in place to safely erase all p.. | Document the mechanism/process in place for data d.. | Medium | 2020-11-08 | In Progress |
| DPO and Governance | If your business operates outside the EU, do you h.. | Companies that do not have an establishment within.. | Medium | 2020-11-08 | In Progress |
| Sub-Processors | Are there written agreements in place between sub-.. | Review and update the existing contracts with proc.. | Medium | 2020-11-08 | In Progress |
| Storage and Archiving | Does your organization store and archive personal .. | Review and update the existing process of storing .. | Medium | 2020-11-08 | In Progress |
| Technical Controls | Does your organization follow appropriate physical.. | Identify the existing technical controls in place .. | Medium | 2020-11-08 | In Progress |
| Technical Controls | Do you know who has access to personal information.. | Identify the individuals inside or outside the org.. | Medium | 2020-11-08 | In Progress |

{databrackets cybersecurity · audit · compliance}

# 4 Identified Risks with Action Plan

These are risks that have been identified, evaluated, and have an Action Plan. We have identified 0 high, 10 medium, and 0 low action items. Of all items in the action plan, 10 are pending and 0 are complete.

## 4.1 Artifact 4 - Please provide a copy of the current processor/sub processor agreement describing proper handling of the personal data.

**Module:** Artifacts

**Response:** Agreements not yet in place.

**Comments:** Formal agreements are yet to be in place.

**Action Plan:** Review and update the existing contracts with processors/sub-processors to include
- the nature and purpose of the processing
- the type of personal data and categories of data subjects
- duration of the processing
- and the obligations and rights of the controller.
(Reference - https://docular.net/documents/template/5515/data-processing-agreement-processor-sub-processor)

**Status:** In Progress

**Priority:** Medium

**Target Date for Completion:** 2020-11-08

## 4.2 Do you maintain records of your processing activities of data?

**Module:** Data Collection and Processing

List all the services and business related purposes that uses personal data of the data subjects:

**Response:** No

**Comments:** No, we don't have records of processing activities of personal data.

**Action Plan:** Data processors must maintain documents (such as data flows) that describes data processing. Sample template provided can be used to create one.

**Status:** In Progress

**Priority:** Medium

**Target Date for Completion:** 2020-09-01

databrackets
cybersecurity · audit · compliance

### 4.3 Does the Privacy Notice describe the types of personal information, including sensitive information, collected from individuals?

**Module:** Notice and Privacy Policy

**Response:** No

**Comments:** No, it doesn't describe the types of personal information, including sensitive information, collected from individuals

**Action Plan:** Ensure that privacy notice clearly describes the type of privacy data being collected, purpose and how it is processed. Attached privacy policy template can be used to create one.

**Status:** In Progress

**Priority:** Medium

**Target Date for Completion:** 2020-11-08

### 4.4 Do you provide data subjects with options to manage, review, and update their information?

**Module:** Data Subjects Rights

**Response:** No

**Comments:** No. We don't have a procedure in place for data subjects to request to manage, review or update their information.

**Action Plan:** Organizations must have mechanism in place where data subject can request to manage, review or update all their personal data and controller must oblige within reasonable time (generally 30 days). This information should also be published in privacy notice.

**Status:** In Progress

**Priority:** Medium

**Target Date for Completion:** 2020-11-08

### 4.5 Do you have process in place to safely erase all personal information on request?

**Module:** Data Subjects Rights

**Response:** No, we don't have procedures in place

**Comments:** No, We don't have adequate process in place to ensure complete data erasure.

**Action Plan:** Document the mechanism/process in place for data destruction.

**How is personal information destroyed?**

**Who authorizes destruction?**

**Who carries out destruction?**

**Status:** In Progress

**Priority:** Medium

**Target Date for Completion:** 2020-11-08

{databrackets cybersecurity · audit · compliance}

### 4.6 If your business operates outside the EU, do you have a representative in the EU?

**Module:** DPO and Governance

| Full Name of the representative within EU | Location of the representative within EU |
|---|---|

**Response:** Representative is not appointed.

**Comments:** No, we don't have a representative within EU.

**Action Plan:** Companies that do not have an establishment within EU yet processes EU citizens' personal data is required to have a representative within EU. A representative should be in identified at the earliest.

**Status:** In Progress

**Priority:** Medium

**Target Date for Completion:** 2020-11-08

### 4.7 Are there written agreements in place between sub-processor(s) and the processor that outline how personal data should be processed ?

**Module:** Sub-Processors

**Response:** No

**Comments:** No, we don't have a contract at present.

**Action Plan:** Review and update the existing contracts with processors/sub-processors to include
1. Duration of processing
2. Nature and purpose of the processing
3. The type of personal data
4. Categories of data subjects
5. Obligations and rights of the controller

**Status:** In Progress

**Priority:** Medium

**Target Date for Completion:** 2020-11-08

### 4.8 Does your organization store and archive personal information securely?

**Module:** Storage and Archiving

**Response:** Storage and Archiving Security controls are not in place.

**Comments:** No, The personal data is not stored and archived securely.

**Action Plan:** Review and update the existing process of storing personal data
- ensure that data is always stored on the media that has proper access control
- have a process to archive data
- backups are properly secured

**Status:** In Progress

**Priority:** Medium

**Target Date for Completion:** 2020-11-08

{databrackets cybersecurity · audit · compliance}

### 4.9 Does your organization follow appropriate physical and technical procedure to secure personal data?

**Module:** Technical Controls

**Response:** No

**Comments:** No, We don't have proper security procedure in place..

**Action Plan:** Identify the existing technical controls in place to ensure security of the personal data.
a) Physical Controls - e.g. Locked access to the physical devices (such as tapes) storing data.
b) Administrative Controls - e.g. Data controller must approve access to the privacy data and approval requests must be documented.
c) Technical Controls - e.g. Data encrypted on storage using AES encryption, keys managed in a secret vault.

**Status:** In Progress

**Priority:** Medium

**Target Date for Completion:** 2020-11-08

### 4.10 Do you know who has access to personal information inside/outside the organization?

**Module:** Technical Controls

**Response:** No

**Comments:** No, We don't have records of individuals who accesses personal data.

**Action Plan:** Identify the individuals inside or outside the organization having access to the privacy data. And procedure in place to authorize the access.

**Status:** In Progress

**Priority:** Medium

**Target Date for Completion:** 2020-11-08

---

## 5 Managed or Not Present Risks

Problems that have been managed or are not present in your organization.

{databrackets cybersecurity · audit · compliance}

## 5.1 Scoping Exercise

### 5.1.1 Does your organization process and/or handle any personal data of EU data subjects as part of providing goods and services?

**Uploaded File(s):** Evidence_1_9xXtfiZ.docx

**Describe your organization's primary business purpose:**

**Response:** Not Applicable

**Comments:** This is not applicable to us.

### 5.1.2 Does your organization have business presence in EU?

| Country | Address |
|---|---|
| Germany | 150, VAdamalai street |

**Response:** Not Applicable

**Comments:** This is not applicable to us since we do not have a presence in EU or process data of EU data subjects.

### 5.1.3 Where is your data geographically stored and processed?

| Name of the countries or locations where data is processed/stored: |
|---|

**Response:** Yes

**Comments:** List the locations where data is geographically stored and processed.

### 5.1.4 Do you have a designated Data Protection Officer (DPO)?

**Enter your DPO Name if any:**

**DPO's Phone Number(if applicable)**

**DPO's Email id(If applicable)**

**Response:** DPO Appointed

**Comments:** Yes, we have a designated Data Privacy Officer (DPO. Please specify the DPO name.

### 5.1.5 Does the information handled contain any of these types of sensitive personal data?

**Response:** No

**Comments:** No, we do not handle any special type of personal data like health records, sexual orientation or criminal records

{databrackets cybersecurity · audit · compliance}

#### 5.1.6 Are you a direct processor of the privacy information or do you process information on behalf of other businesses?

**Response:** Yes, direct processor.

**Comments:** Yes. our business processes the data directly

#### 5.1.7 List all the business processes that uses data collected from the data subjects?

List all the business process that involves data subjects information

**Response:** Yes, business processes listed

**Comments:** List all the business process that involves data collected from data subjects.

### 5.2 Notice and Privacy Policy

#### 5.2.1 Are data subjects provided with a privacy notice prior to data collection?

**Response:** Privacy Notice Provided

**Comments:** Yes, data subjects are provided with a privacy notice and consent collected at the time of data collection.
<Upload a copy of your privacy notice and consent>

#### 5.2.2 Do you have a process in place to record user consent before handling privacy information?

**Response:** Process is in Place.

**Comments:** Yes, we have a process in place to get and record user consent before capturing privacy information. (If applicable - Additional consent is obtained for sensitive privacy information processing).

#### 5.2.3 Is the Privacy Notice written in plain language so that it is easily understood by individuals?

**Response:** It is in plain language.

**Comments:** Yes, it is in plain text.
(Attach a copy of your privacy notice)

{databrackets cybersecurity · audit · compliance}

#### 5.2.4 Does the Privacy Notice describe the circumstances under which personal information is disclosed or shared with third parties, including service providers, and the purpose for those disclosures?

**Response:** Yes

**Comments:** Yes, Privacy Notice describes the circumstances under which personal information is disclosed or shared with third parties, including service providers, and the purpose of those disclosures.

#### 5.2.5 Are individuals informed that their personal information will be transferred to a third country or international organization and whether there is a legitimate transfer mechanism in place?

**Response:** Yes

**Comments:** Yes, they are informed that their personal information will be transferred to a third country or international organization and the legitimacy of such transfer.

#### 5.2.6 Does the Privacy Notice include the identity of and contact information for the controller or Data Protection Officer (DPO)?

**Response:** Yes

**Comments:** Yes, Privacy Notice includes the identity of and contact information for the controller or the controller's representative, as well as the contact details of the data protection officer

#### 5.2.7 In case the processing activities changes after the initial consent, is there a procedure in place to collect data subjects consent within 30 days ?

**Response:** Yes

**Comments:** Yes, we provide information prior to collecting/processing privacy data.

### 5.3 Data Collection and Processing

#### 5.3.1 Do you maintain a list of data - personal, sensitive, financial or health information that you collect from data subjects?

**List all Personal Data collected:**

**List all the Sensitive Data collected:**

**List all the Financial Data collected**

**List all the health information collected:**

**List all the sources you use to collect data ( user registration, purchases ,contact form, newsletter signups, third party sources etc):**

**Response:** Yes we maintain list of these data

**Comments:** Data processors should know what personal data is being processed, to ensure undocumented personal data is not collected and processed. In case of any data breaches, this information is required for investigations and breach notification.
<Please list all the personal data collected, the source they are collected >

{databrackets} cybersecurity · audit · compliance

#### 5.3.2 Do you ensure that the data protection controls are periodically reviewed?

**Response:** Yes

**Comments:** Yes, we ensure that privacy impacts are analyzed for each modification to the system.
Upload any reference file.

### 5.4 Transfer of Personal Data

#### 5.4.1 Does your organization store, process and/or transfer privacy data outside of EU countries?

**List all the countries within EU, where privacy data is transferred:**

**List all the countries outside of EU, where privacy data is transferred:**

**Response:** Only EU-based countries

**Comments:** We store,process and/or transfer privacy data only within EU countries.
List all the countries where privacy data is stored, processed or transferred.

#### 5.4.2 Do you have security controls in place while transferring data?

**List all key security controls you have in place:**

**Response:** Yes

**Comments:** Yes, we use secure data transfer mechanisms.<List all key security controls you have in place>

### 5.5 Data Subjects Rights

#### 5.5.1 Do you provide data subjects with options to export, remove & delete their information?

**Response:** Yes

**Comments:** The data subject can receive his/her personal data either in plain English and/or in a structured and machine-readable format.

#### 5.5.2 Do you provide data subjects with your organization's criteria on the period of storing their information?

**Response:** Yes,retention period shared

**Comments:** Yes, our retention period is " --Set no. of days or until consent is revoked or until local requires --" and we clearly state that in our privacy notice.

{databrackets cybersecurity · audit · compliance}

#### 5.5.3 Do you use data subjects data for profiling and/or automated decision-making process?

**Response:** Yes, with consent

**Comments:** Yes, we do. We get consent from the user during the registration process to perform such activity.

### 5.6 DPO and Governance

#### 5.6.1 Describe the current reporting structure for DPO?

**Response:** Reporting structure in place

**Comments:** Our DPO reports to top management and is involved properly and in a timely manner, in all issues which relate to the protection of personal data.

#### 5.6.2 Does the DPO perform his duties independently yet collaboratively with the top management?

**Response:** Yes

**Comments:** Yes, Our DPO fulfills all his/her responsibilities independently and keeping GDPR's data protection provision as focus.

### 5.7 Sub-Processors

#### 5.7.1 Are any of your data processing activities carried out by third parties?

| List all sub processor(s) ( if applicable) | Location(s) of the sub-processors( if applicable) |
|---|---|

**Response:** No third parties are engaged.

**Comments:** No, we don't have any third party contractors processing personal data.

### 5.8 Storage and Archiving

#### 5.8.1 Are you storing information within third party premises?

**Response:** No

**Comments:** No, we don't store data with third party.

{databrackets cybersecurity • audit • compliance}

## 5.9 Breach Notification

### 5.9.1 Do you have procedures in place to address a personal data breach within 72 hours to a supervising authority?

**Response:** Yes

**Comments:** Our organization has documented processes and procedures in place to meet the breach notification requirements. Attached below a copy of the breach notification process.

### 5.9.2 Do you have policies and procedures in place for reporting breaches to the data subjects?

**Response:** Yes

**Comments:** Our organization has documented process and procedures in place to meet the breach notification requirements to inform data subjects when a breach happens. <Attach a copy of the breach notification process>

## 5.10 Training

### 5.10.1 Do the employees in your organization receive training on data protection and other relevant law?

**Name of the person-in-charge of training:**

**Response:** Yes

**Comments:** Our organization has privacy training in place that is required to be taken by all employees yearly.
< attach any related training log>

## 5.11 Artifacts

### 5.11.1 Artifact 1- Please provide data inventory for personal data collected/processed by your business.

**Response:** Data inventory in place.

**Comments:** We do maintain data inventory and a copy of which is uploaded.

{databrackets cybersecurity · audit · compliance}

#### 5.11.2 Artifact 2 - Please provide data flow diagrams that shows collection, storage, processing, distribution and destruction of the personal data.

**Response:** Data Flow Diagram in place.

**Comments:** Updated data flow diagram is uploaded.

#### 5.11.3 Artifact 3 - Please provide a copy of your privacy notice/policy for review.

**Response:** Privacy policy in place.

**Comments:** The latest privacy policy is uploaded

---

# 6 Unidentified Risks

Risks that have not been identified yet due to question not being answered.

## 6.1 Data Collection and Processing

#### 6.1.1 Do you have policies and procedures in place if you collect information from children younger than 16 years of age?

---

*DISCLAIMER - Information provided by databrackets for this assessment was not independently verified by Databrackets; databrackets has provided details about their operation to the best of their knowledge. These reports and recommendations are for evaluation purposes only and not intended to be construed as legal advice. databrackets is advised to consult with attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on the company and/or its personnel.*