

- 1
- 2
- 3
- 4
- 5

SOM DSA #: _____
Disclosing Agency id #: _____
Partner Agency id #: _____
Review cycle: _____
1st review date: _____

SOM DSA #: _____
 Disclosing Agency id #: _____
 Partner Agency id #: _____
 Review cycle: _____
 1st review date: _____
 2nd review date: _____

**DATA SHARING AGREEMENT
 BETWEEN
 MICHIGAN DEPARTMENT OF STATE
 AND
 ROCKTHEVOTE
 FOR
 AN APPLICATION PROCESSING INTERFACE (API) CONNECTION TO ONLINE VOTER REGISTRATION**

1. Introduction

This Data Sharing Agreement (DSA) is between the Michigan Department of State (MDOS) and RockTheVote (Partner Agency). MDOS and Partner Agency are collectively referred to as the parties.

The Partner Agency is the party that is collecting and sharing data with MDOS under this DSA. MDOS will be receiving and validating the data submitted by RockTheVote. The data will be received by the Online Voter Registration (OVR) system and validated against the Mainframe. Each eligible voter registration will be processed and recorded by the Michigan Department of State.

This DSA establishes the conditions under which MDOS agrees to receive privileged data from the Partner Agency (the data) and it provides for the protection of that data. It also identifies the responsibilities of each party and establishes terms governing the use, disclosure, and disposition of the data.

2. Purpose

The data will be used by the Partner Agency only as is expressly agreed upon by the parties under this DSA. Access to the data by any party or for any purpose not identified in this DSA is strictly forbidden. Data provided by MDOS remains the property of MDOS.

Partner Agency will send data collected from prospective voters on their website, via the Application Processing Interface (API), to the Michigan Online Voter Registration. The API will transmit all required information necessary to complete a voter registration transaction via the Online Voter Registration.

Review date: _____

9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44

**DATA SHARING AGREEMENT
BETWEEN
MICHIGAN DEPARTMENT OF STATE
AND
ROCKTHEVOTE
FOR
AN APPLICATION PROCESSING INTERFACE (API) CONNECTION TO ONLINE VOTER REGISTRATION**

1. Introduction

This Data Sharing Agreement (DSA) is between the Michigan Department of State (MDOS) and RockTheVote (Partner Agency). MDOS and Partner Agency are collectively referred to as the parties.

The Partner Agency is the party that is collecting and sharing data with MDOS under this DSA. MDOS will be receiving and validating the data submitted by RockTheVote. The data will be received by the Online Voter Registration (OVR) system and validated against the Mainframe. Each eligible voter registration will be processed and recorded by the Michigan Department of State.

This DSA establishes the conditions under which MDOS agrees to receive privileged data from the Partner Agency (the data) and it provides for the protection of that data. It also identifies the responsibilities of each party and establishes terms governing the use, disclosure, and disposition of the data.

2. Purpose

The data will be used by the Partner Agency only as is expressly agreed upon by the parties under this DSA. Access to the data by any party or for any purpose not identified in this DSA is strictly forbidden. Data provided by MDOS remains the property of MDOS.

Partner Agency will send data collected from prospective voters on their website, via the Application Processing Interface (API), to the Michigan Online Voter Registration. The API will transmit all required information necessary to complete a voter registration transaction via the Online Voter Registration.

45 **3. Data To Be Shared**

46

47 Partner Agency will provide MDOS with the data required to complete an online voter
48 registration. Partner agency will provide full name, Michigan Driver License/Personal
49 Identification number, birthdate, eye color, and last four digits of the social security number.
50 MDOS will provide the Partner Agency with basic (approval or rejection notification)
51 information related to the status of each submitted voter registration. The Data provided by
52 MDOS remains the sole and exclusive property of the MDOS.

53

54 **4. Method of Transfer**

55

56 The data will be shared by the following means:

57

58 File drop

59 Secure file transfer

60 Encrypted email attachment

61 Encrypted file on a removable storage device

62 File Transfer Service

63 Data warehouse

64 Paper (hard copy)

65 Fax

66 Online access

67 Other: (describe) RockTheVote will establish an Application Programming Interface (API) with
68 the State of Michigan's Online Voter Registration (OVR)

69

70 MDOS requires that all data should be encrypted at rest and in transit in compliance with DTMB
71 standards.

72

73 **5. Frequency of Transfer**

74

75 The data to be shared under this DSA will be transferred only at a frequency and for a
76 period of time as is necessary to meet the purpose stated in §2 above. The frequency is
77 expected to be on-going and the duration will be until one party agrees to discontinue
78 transfers.

79

80 **6. Availability of Data**

81

82 MDOS reserves the right to schedule the time and duration of the availability of
83 electronic access to the Online Voter Registration. MDOS does not guarantee continuous
84 availability during scheduled times, but will use reasonable efforts to make the Online Voter
85 Registration available as agreed under this DSA.

86

87

88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131

7. Legal Authority

MDOS. MDOS shall adhere to all federal and state laws and regulations pertaining to sharing the requested data, including but not limited to: the Identity Theft Protection Act, MCL § 445.61 *et. seq.*, the Social Security Number Privacy Act, MCL § 445.81 *et. seq.*, and Fair Credit Reporting Act, 15 U.S. Code § 1681 *et seq.*

Partner Agency. The Partner Agency acts under an established authority to collect the data. The Partner Agency **collects data from Michigan residents and provides the information through the API.** This API is established only to assist Michigan citizens with registering to vote. The Partner Agency shall adhere to the DPPA, Identity Theft Protection Act, Fair Credit Reporting Act, and the Social Security Number Privacy Act, as applicable.

8. Notices and Consents

To the extent required by law, regulations, or rules, MDOS and the partner agency covenant that appropriate notices, consents, and authorizations have been and will continue to be obtained from the individuals and entities the data concerns. Notices will include how data obtained from the individuals and entities the data concerns will be used and stored.

9. Data Classification

The MDOS has classified the data using [DTMB Technical Standard No. 1340.00.14, Information Technology Information Security.](#)

The data classification level for the data shared under this DSA is confidential.

The security categorization is moderate.

The minimum security controls and control enhancements derive from the [National Institute of Standards and Technology \(NIST\) SP 800-53, Recommended Security Controls for Federal Information Systems.](#) The minimum baseline security controls are the starting point for the security control selection process, and are the basis from which controls and control enhancements may be removed, added or customized to achieve the level of security protection required for the data or information system.

Additional security controls that are not addressed in the NIST SP 800-53 Security Controls may be required based on regulatory compliance or by contractual obligation. The MDOS considers all non-publicly available data to be considered a minimal classification of confidential with a potential moderate data impact level. The additional security controls associated with the data include: The API is built using a NIST approved process.

132 **10. MDOS' Responsibilities**

133

134 MDOS must:

135

- 136 a. Provide Partner Agency with access to the data consistent with law, regulations, rules,
137 and contractual obligations, and the terms and conditions of this DSA.
- 138
- 139 b. If necessary, work with Partner Agency and the Department of Technology,
140 Management, and Budget (DTMB) to facilitate the sharing of data under this DSA.
- 141
- 142 c. Perform access reviews to ensure that Partner Agency has established and uses
143 adequate administrative, technical, and physical safeguards to protect data from
144 unauthorized disclosure.
- 145
- 146 d. Perform annual reviews to ensure each person with access to MDOS' data: (1) needs
147 and uses the data in connection with their State work duties and (2) understands their
148 responsibility in protecting the data. MDOS may perform onsite inspections of Partner
149 Agency's premises to ensure compliance with this DSA.

150

151 **11. Partner Agency's Responsibilities**

152

153 Partner Agency must:

154

- 155 a. **Protect the data.** Partner Agency must establish and use appropriate administrative,
156 technical, and physical safeguards to protect the data from being accessed, used,
157 disclosed, or stored in a manner other than as provided in this DSA. Protocols must be
158 in writing and provided to the MDOS upon request.
- 159
- 160 i. **Administrative safeguards** include policies, procedures, training, and
161 other measures designed to carry out security requirements. For
162 example, appointing a security officer or implementing an incident
163 response plan.
- 164
- 165 ii. **Physical safeguards** include limitation of access to physical areas of
166 information systems. For example, implementing a clean-desk policy,
167 requiring locked file cabinets, or use of identification cards to access
168 certain areas.
- 169
- 170 iii. **Technical safeguards** include automated processes used to protect and
171 control access to data on information systems. Examples include
172 encryption, use of passwords, and data loss prevention tools.
- 173
- 174 b. **Create a security policy pertaining to the data.** A security policy is a written document
175 describing the system in terms of categories of data processed, users allowed access,

176 and access rules between the users and the data. It describes procedures to prevent
177 unauthorized access by clearing all protected data on storage objects before they are
178 allocated or reallocated out of or into each system. Further security protocols using
179 password protection and authentication must be provided where the computer system
180 contains information for more than one program, project, office, or agency so that
181 personnel do not have unauthorized or unlimited access. Partner Agency must provide
182 MDOS with a copy of the security policy upon request.

- 183
- 184 c. **Maintain a log of the data received from MDOS.** The log must contain the data
185 requested; purpose of request; date data received; name of
186 agency/division/unit/employee making the request; name of other employees who may
187 have access; date destroyed; and method of destruction. MDOS may require Partner
188 Agency to include categories of information in addition to those listed in this subsection.
189 The log must be retained by the Partner Agency for either term of agreement plus five
190 years, or according to agency retention schedule, whichever is longer. Partner Agency
191 must provide MDOS with a copy of the log upon request.
- 192
- 193 d. **Use the data only for the stated purpose.** Partner Agency will use the data provided
194 under this DSA solely for the purpose identified in §2 above.
- 195
- 196 e. **Limit access** to the data provided under this DSA to those specifically listed in **Schedule**
197 **B.**
- 198
- 199 f. **Limit access** to the data provided under this DSA to the agents, contractors, and
200 subcontractors who require access to the data to perform the intended activities on
201 behalf of Partner Agency, upon review and written permission by MDOS. Agents,
202 contractors, and subcontractors must agree in writing to the same or more stringent
203 terms and conditions of this DSA. The Partner Agency must provide a copy of the written
204 agreements referenced here upon the request of MDOS.
- 205
- 206 g. **Minimize data requests, usage, and disclosures.** Partner Agency will request, use, and
207 disclose only the minimum amount of data necessary to fulfill the purposes of this DSA.
- 208
- 209 h. **Not disclose the data except as expressly permitted in this DSA or as required by law.**
210 Except as otherwise provided in this DSA, Partner Agency will not disclose the data to
211 others.
- 212
- 213 i. **Exempt data from disclosure under FOIA when permitted.** Partner Agency will not
214 disclose the data in response to a request under the Freedom of Information Act (FOIA),
215 MCL 15.231, *et seq.* unless the law requires (and not merely permits) disclosure.
216 Partner Party must exempt the data from disclosure under FOIA when permitted by law.
217 If Partner Agency determines the law requires disclosure of the data under FOIA,
218 Partner Agency will notify MDOS prior to making any disclosures of data not intended
219 under this DSA. Exceptions to this subsection include:

- 220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
- i. data that was already in Partner Agency’s possession without an obligation of confidentiality;
 - ii. data that was developed independently by the Partner Agency;
 - iii. data that was obtained from a source other than MDOS without an obligation of confidentiality; or
 - iv. data that was or is publicly available when received, or thereafter became publicly available (other than through any unauthorized disclosure by the Partner Agency).
- j. **Comply with retention and disposal schedules.** Partner Agency’s must destroy the data, including copies of the data, upon completion of the purpose stated in §2, consistent with applicable law and State record retention and disposal schedules. Partner Agency must provide written certification of data destruction if requested by MDOS.

239
240

12. Training

241 By executing this DSA, Partner Agency certifies that the driver, and vehicle, and related
242 records obtained by Partner Agency will be used in compliance with the federal DPPA and
243 related Michigan driver privacy legislation. Partner Agency understands that the willful,
244 unauthorized use or improper re-disclosure of personal information or highly restricted
245 personal information obtained under this DSA could subject an individual to criminal penalties
246 imposed by law. DOS will provide, and Partner Agency will mandate, DPPA training to all
247 persons that will access DOS data. Failure to comply with this section is a material breach and
248 grounds for termination of this DSA.

249
250
251
252

13. Costs and Damages

253 Partner Agency agrees to reimburse MDOS for all documented costs incurred to
254 implement this DSA, including but not limited to, hardware, storage, and communication charges,
255 as well as DTMB staff costs. Partner Agency will be charged for necessary programming changes
256 at the applicable DTMB rates.

257 Partner Agency further agrees that they shall be responsible for all database
258 administration functions, including database backup, and that they shall pay all costs related to
259 operating and maintaining the data supplied by MDOS. Partner Agency further agrees that they
260 will not impose, or seek to impose, any audit requirement or audit cost upon MDOS as a result
261 of this DSA.
262

263 Each party will be responsible for its own costs, losses, and damages related to the
264 sharing of data under this DSA except as otherwise provided in §14 below. Neither party will be
265 liable to the other for any claim related to or arising under this DSA for consequential,
266 incidental, indirect, or special damages.

267

268 **14. Security Breach Notification**

269

270 Partner Agency must adhere to [DTMB Technical Procedure No. 1340.00.01.02, How to](#)
271 [Handle a Breach of Personal Identifiable/Sensitive Information Incidents](#). Partner Agency must
272 implement internal policies and procedures for reporting data security incidents and provide
273 MDOS a copy upon request. Partner Agency’s internal policies and procedures for data security
274 incidents must be as stringent as or more stringent than MDOS’s.

275

276 Notwithstanding any internal policy to the contrary, if Partner Agency discovers any
277 “suspected or actual” use or disclosure of MDOS’s data not provided for under this DSA, the
278 Partner Agency must report it to MDOS within one business day of the breach or suspected
279 breach being identified. The parties will cooperate with one another to investigate, mitigate,
280 and remedy unauthorized access, use, or disclosure of the data.

281

282 Partner Agency must identify through audits or other available means entities or
283 persons who improperly access, use, or disclose the data.

284

285 If any act, error, omission, negligence, misconduct, and/ or breach by Partner Agency or
286 its contractor compromises the security, confidentiality, or integrity of the data, Partner Agency
287 will take all reasonable actions required to comply with applicable law as a result of such
288 security incident and assumes full responsibility for any associated costs and duties, including
289 but not limited to notification of affected individuals and entities, and if requested by MDOS,
290 will provide credit and identity monitoring services for 24 months to affected individuals.

291

292 **15. Accuracy**

293

294 MDOS will use reasonable efforts to ensure the completeness, accuracy, and timeliness
295 of the data provided under this DSA. However, MDOS cannot guarantee data accuracy and will
296 therefore not be held responsible for any damage to Partner Agency resulting from the
297 disclosure or use of data that is inaccurate, incomplete, or outdated.

298

299 **16. Cooperation; Execution of Additional Agreements**

300

301 The parties will execute such documents as may be necessary to realize the intentions of
302 this DSA or comply with law. The parties will also require third parties to execute such
303 documents as may be necessary to realize the intentions of this DSA or comply with law, prior
304 to granting the third-party access to the data. Examples include business associate and non-
305 disclosure agreements.

306

307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323

17. Issue Resolution

The parties will work collectively to resolve system issues relative to Partner Agency’s access to the data. Additionally, upon the request of either party, the parties will convene as reasonably necessary for the purpose of resolving problems that may arise in the administration or enforcement of this DSA. The parties will exchange documentation as reasonably necessary to identify and explain issues and positions. Any portion of this DSA that may be subject to interpretation will be addressed at these meetings.

18. Notices

Notices and other written communications must be addressed to the individuals below or their successors. Parties may amend contact information by providing written notice of the change to the other party. Notices or other written communications required or related to this DSA must be in writing and delivered in person or by email.

<p>For MDOS:</p> <p>Melissa Smiley, Chief of Staff 430 W. Allegan Lansing, MI 48933 (517) 335-2436 SmileyM1@michigan.gov</p> <p>With copy to: Michael J. Brady, Chief Legal Director 430 W. Allegan Lansing, MI 48933 517-599-7343 bradym@michigan.gov</p>	<p>For Partner Agency:</p> <p>Carolyn DeWitt, Executive Director RockTheVote 1440 G Street NW Washington, DC 20005 202-719-9910</p>
---	--

324
325
326
327
328
329
330
331
332
333

19. Compliance Monitoring

On at least an annual basis, the parties will review the practices and procedures outlined in this DSA to ensure compliance with the terms of the DSA and the law. The parties will provide the results of such reviews to the other party upon written request. The parties will also ensure that they take appropriate measures to ensure that information about the DSA is kept up-to-date. The parties have designated the individuals listed below as responsible for this section.

Main Point of Contact for **MDOS: Jonathan Brater, Bureau of Elections Director**

334 Main Point of Contact for RockTheVote: Carolyn DeWitt, Executive Director

335

336 The parties also recognize that this DSA is subject to compliance audits, investigations,
337 and reviews as provided by law.

338

339

340 **20. Amendments**

341

342 This DSA may be amended by written agreement of the parties. If amendment to this
343 DSA is required to comply with federal or State laws, rules, or regulations, the parties will
344 promptly enter into negotiations to meet those legal requirements.

345

346 **21. Effective Date and Term**

347

348 This DSA is effective as of April 25, 2020 and will expire on April 1st, 2025, unless
349 terminated under §22. The DSA may be renewed by amending the DSA. Parties will meet no
350 less than 30 days prior to the end of this term to begin renewal process.

351

352 **22. Termination**

353

354 This DSA may be terminated for any reason by either party upon 30 days' prior written
355 notice to the other party.

356

357 **23. Survival**

358

359 The rights, obligations, and conditions set forth in §10, MDOS's Responsibilities; §11,
360 Partner Agency's Responsibilities; and any right, obligation, or condition that, by its express
361 terms or nature and context is intended to survive the termination or expiration of this DSA,
362 survives any such termination or expiration.

363

364 **24. Entire Agreement**

365

366 This DSA replaces and supersedes all prior agreements between the parties relating to
367 the subject matter of this DSA.

368

369 **25. Execution**

370

371 This DSA may be executed in counterparts, each of which is deemed to be an original,
372 and all of which taken together constitutes one and the same instrument. The signature of any
373 party transmitted by email is binding.

374

375 **26. Successors; Assignment**

376

377 This DSA insures to the benefit of and is binding upon the parties, their respective
378 successors-in-interest by way of reorganization, operation of law, or otherwise, and their
379 permitted assigns. Neither party may assign this DSA to any other party without the prior
380 approval of the other party.

381

382 **27. No Third-Party Beneficiaries**

383 This DSA does not confer any rights or remedies upon any person or entity other than
384 the parties and their respective successors-in-interest by way of reorganization, operation of
385 law, or otherwise, and their permitted assigns.

386

387

388

389 **28. Authority to Bind**

390

391 Each person signing this DSA represents that he or she is duly authorized to execute this
392 DSA on behalf of the responsible agency.

393

For MDOS:

Jonathan Brater
Director, Bureau of Elections

Date

For Partner Agency:

Carolyn DeWitt
Executive Director, RockTheVote

Date

394

395

396
397

Schedule A
Data To Be Shared and File Formats of the Data

Data to Be Shared	File Format
Full name (Middle Name, if applicable), Michigan Driver License/Personal Identification number, birthdate, eye color, and last four digits of the social security number.	This data will be transmitted from RockTheVote to the State of Michigan via a Application Processing Interface (API). The file format will be a JSON string.

398
399

400 Data Elements

401
402
403
404
405
406
407
408
409
410
411
412

413
414

415
416
417

418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436

Schedule B

State Employees with Data Access Privileges

This access is the same as the general public. The general public does not authenticate to the OVR application. However, during completion of the application the OVR application sends information submitted in the application to the Driver License (DL) Mainframe to validate if the person completing the application has a valid driver's license or Personal Identification Card (PID). The data elements used to validate if the person is a registered voter on the mainframe include the following: full name, driver's license or state id number, birthdate, eye color, and SSN4 (specified in MCL 168.509ii). This information will be used to notify the general public whether or not they have a valid driver's license or state id and if they are allowed to register to vote.

If a SOM Employee needs to view the data submitted by the general public, they would use their standard QVF user ID and password to access the information.

1 (One) - State Administrative Manager

7 (Seven) – Departmental Analysts

2 (Two) – Departmental Technicians

437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480

Schedule C
Security Procedures for Partner Agency

Rock the Vote is compliant with the NIST 800-53 and Virginia SEC 525 security standards, and the organization underwent an external audit from ImpactMakers in 2018 to certify compliance with both standards.

Rock the Vote maintains several NIST-based internal security policies and processes, including but not limited to:

- Software development lifecycle;
- Hosting contingency plan;
- Hosting quarterly review process;
- Disaster recovery plan (DRP) and business continuity plan (BCP);
- Info system security plan (SSP);
- Configuration management plan (CMP);
- Incident response plan (IRP);
- Business impact analysis (BIA).

Rock the Vote runs quarterly vulnerability scans using a third-party software (Qualys), runs monthly log file audits, receives and follows recommended GitHub security alerts for vulnerable dependencies, forces quarterly password resets for all system, and has automated password resets for inactive accounts, etc.

Rock the Vote’s Online Voter Registration Platform is a cloud-deployed Ruby application on an AWS environment, with infrastructure built using a certified AWS architect. Rock the Vote uses an external firewall service (Sucuri), DDoS mitigation and prevention, and IP-based restrictions to continually monitor, log, and deflect any attempts to penetrate the system.

481
482
483
484
485
486
487
488
489
490
491
492
493

Schedule D
Third-Party with Data Access Privileges

Rock the Vote volunteers never have access to or can see the State of Michigan’s API. Only Rock the Vote’s Data Privacy Officer (David Pruter) and other Rock the Vote employees, as designated solely on an as-needed basis by the Data Privacy Officer, will have access to API keys/tokens.

Only certain Rock the Vote employees with white-listed IPs can access non-sensitive user data from the Online Voter Registration Platform. No Rock the Vote employees, volunteers, or affiliates ever have access to PII such as SSNs or driver’s license/ID numbers.