sovren

GDPR Compliance Analysis, Article by Article

Conducted by Robert Ruff, Security Officer

May 14, 2018

Legend

Information only
Applies to Data Controllers only
Not applicable to controllers or processors
Applicable to both controllers and processors
Directly applicable to processors
Sovren comments

Under the GDPR, Sovren is a Data Processor, and our customers are Data Controllers.

Sovren's Data Protection Officer & Security Officer
Robert H. Ruff
robert.ruff@sovren.com

Sovren's Compliance Officer
Amanda Lamb
amanda.lamb@sovren.com

1107 FM 1431 STE 205
Marble Falls, Texas 78654 USA
+1 713.562.7112

" I certify that Sovren's SaaS Service is in full compliance with all requirements of the GDPR, both by design, by policy, by practice, and in actual reality."

--Robert Ruff, Security Officer and Data Protection Officer

© 2018 Copyright Sovren Group, Inc. All rights reserved. | sovren.com

Service Statement

Parsing and Geocoding

Sovren's SaaS system does not store documents sent to it for parsing and/or geocoding, nor does it store the results from such processing. All processing takes place in memory. Neither documents nor results are ever written to disk or any other persistent storage. Typically processing time is less than one half second, after which the memory is reclaimed.

AI Matching

Sovren's SaaS system does store documents sent to it for indexing into AI Matching, but before storing and indexing, the Service expunges all PII (as per Exhibit A attached hereto), thereby ensuring that no PII is stored and no PII is searchable. Typically processing time is less than one second, after which the memory is reclaimed.

Chapter 1 – General provisions

Article 1 – Subject-matter and objectives
Article 2 – Material scope
Article 3 – Territorial scope
Article 4 – Definitions

Chapter 2 – Principles

Article 5 – Principles relating to processing of personal data
Article 6 – Lawfulness of processing
Article 7 – Conditions for consent
Article 8 – Conditions applicable to child's consent in relation to information society services
Article 9 – Processing of special categories of personal data

Our software only processes data contained in the resume or CV, and does not use any other data source or processing (except geocoding). Thus, although resumes/CVs may contain data that is referred to in paragraph 1, paragraph 2e exempts us from this Article.

© 2018 Copyright Sovren Group, Inc. All rights reserved.

Article 10 – Processing of personal data relating to criminal convictions and offences
Article 11 – Processing which does not require identification

Chapter 3 – Rights of the data subject

Section 1 – Transparency and modalities

Article 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject

Section 2 – Information and access to personal data

Article 13 – Information to be provided where personal data are collected from the data subject

Sovren's AI Matching provides exact and human understandable explanations of how it calculated every match score. This allows the data controller to exactly meet all the requirements of 13.2.f., for every transaction, every time.

Article 14 – Information to be provided where personal data have not been obtained from the data subject

Article 15 – Right of access by the data subject

Since Sovren stores no data sent to its SaaS parsing Services, and retains no PII ever, the data controller never need contact Sovren to accomplish its duties under this Article, as only the data controller, not Sovren, has any such data.

Section 3 – Rectification and erasure

Article 16 – Right to rectification

Since Sovren stores no data sent to its SaaS parsing Services, and retains no PII ever, the data controller never need contact Sovren to accomplish its duties under this Article, as only the data controller, not Sovren, has any such data.

Article 17 – Right to erasure ('right to be forgotten')

See comments for Article 16.

Article 18 – Right to restriction of processing

See comments for Article 16.

Article 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing

See comments for Article 16.

© 2018 Copyright Sovren Group, Inc. All rights reserved.

Article 20 – Right to data portability

Sovren's resume parsing service provides output in HROpenStandards.org's Resume 2.5 format, exactly, in XML or JSON, and is thus documented and portable, helping data controllers meet the obligations of 20.1

Section 4 – Right to object and automated individual decision-making

Article 21 – Right to object

Article 22 – Automated individual decision-making, including profiling

See comment for Article 13.

Section 5 – Restrictions

Article 23 – Restrictions

Chapter 4 – Controller and processor

Section 1 – General obligations

Article 24 – Responsibility of the controller

Article 25 – Data protection by design and by default

Article 26 – Joint controllers

Article 27 – Representatives of controllers or processors not established in the Union

Article 28 – Processor

See Sovren Enterprise Security Policy and Sovren PII Policy. Sovren does not use other processors EXCEPT optionally a controller can elect to have Sovren geocode a resume using Google or Bing. This is an optional step under the control and direction at all times of the data controller.

Article 29 – Processing under the authority of the controller or processor Sovren provides no batch processing directly. Each transaction is initiated and directed solely by the data controller, and processed by Sovren only as instructed.

Article 30 – Records of processing activities

Article 30.5 exempts Sovren from this article. All records are fully maintainable/ reportable by the data controller.

Article 31 – Cooperation with the supervisory authority

See Sovren Enterprise Security Policy, Security of Processing, #4

© 2018 Copyright Sovren Group, Inc. All rights reserved.

Section 2 – Security of personal data

Article 32 – Security of processing

See Sovren Enterprise Security Policy, Security of Processing, #1, #2, #3

Article 33 – Notification of a personal data breach to the supervisory authority

See Sovren Enterprise Security Policy, Security of Processing, #5

Article 34 – Communication of a personal data breach to the data subject

See Sovren Enterprise Security Policy, Security of Processing, #5

Section 3 – Data protection impact assessment and prior consultation

Article 35 – Data protection impact assessment

Article 36 – Prior consultation

Section 4 – Data protection officer

Article 37 – Designation of the data protection officer

Sovren is exempt from needing this position but elected to appoint one anyway.

Article 38 – Position of the data protection officer

Article 39 – Tasks of the data protection officer

Section 5 – Codes of conduct and certification

Article 40 – Codes of conduct

Article 41 – Monitoring of approved codes of conduct

Article 42 – Certification

Article 43 – Certification bodies

Chapter 5 – Transfers of personal data to third countries or international organizations

Article 44 – General principle for transfers

Article 45 – Transfers on the basis of an adequacy decision

Article 46 – Transfers subject to appropriate safeguards

Article 47 – Binding corporate rules

Article 48 – Transfers or disclosures not authorised by Union law

© 2018 Copyright Sovren Group, Inc. All rights reserved. | sovren.com

Chapter 6 – Independent supervisory authorities

Section 1 – Independent status

Section 2 – Competence, tasks and powers

Chapter 7 – Cooperation and consistency

Section 1 – Cooperation

Section 2 – Consistency

© 2018 Copyright Sovren Group, Inc. All rights reserved. | sovren.com

Section 3 – European data protection board

Article 68 – European Data Protection Board
Article 69 – Independence
Article 70 – Tasks of the Board
Article 71 – Reports
Article 72 – Procedure
Article 73 – Chair
Article 74 – Tasks of the Chair
Article 75 – Secretariat
Article 76 – Confidentiality

Chapter 8 – Remedies, liability and penalties

Article 77 – Right to lodge a complaint with a supervisory authority
Article 78 – Right to an effective judicial remedy against a supervisory authority
Article 79 – Right to an effective judicial remedy against a controller or processor
Article 80 – Representation of data subjects
Article 81 – Suspension of proceedings
Article 82 – Right to compensation and liability
Article 83 – General conditions for imposing administrative fines
Article 84 – Penalties

Chapter 9 – Provisions relating to specific processing situations

Article 85 – Processing and freedom of expression and information
Article 86 – Processing and public access to official documents
Article 87 – Processing of the national identification number
Article 88 – Processing in the context of employment
Article 89 – Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

© 2018 Copyright Sovren Group, Inc. All rights reserved. | sovren.com

Chapter 10 – Delegated acts and implementing acts

Chapter 11 – Final provisions

© 2018 Copyright Sovren Group, Inc. All rights reserved. | sovren.com

EXHIBIT A

Sovren PII Policy

Sovren's software processes two types of recruiting documents: Job Advertisements, and Candidate Advertisements (also known as resumes or CVs). Both types of documents are intended by their authors to be public and to be distributed widely in order to accomplish their goals. Neither type of document, therefore, reasonably contains ANY data that is expected by the creator to be treated as confidential or private or secret in any way, to any extent, in any forum, in any locale, at any time.

Therefore, Sovren deems that its core processing activities relate to documents which, although they may have PII, are intended to contain such PII, and that the publication or distribution of such PII bears no risk of damage to the originator.

Nevertheless, in order to simplify its security practices, and to provide security far beyond what is expected, Sovren has implemented the following practices:

Data sent to public SaaS endpoints

DATA TYPE: JOB ADVERTISEMENTS

Job Advertisements do not contain PII because they relate to organizations, not individuals. Sovren will revise its TOS to prohibit customers and prospects from sending Job Advertisements to Sovren if such advertisements contain an individual's PII. Sovren will not store any Job Advertisements that are sent for parsing or geocoding, unless they are explicitly sent to an endpoint that includes storage by the Sovren AI Matching Engine.

DATA TYPE: RESUMES OR CVS (CANDIDATE ADVERTISEMENTS)

Sovren will not store any resumes that are sent to it for parsing or geocoding, unless they are explicitly sent to an endpoint that includes storage by the Sovren AI Matching Engine.

© 2018 Copyright Sovren Group, Inc. All rights reserved.

When the RESULTS of parsing resumes are to be stored into the Sovren AI Matching Engine, Sovren will expunge the following information before storage:

1. All References, in entirety.
2. All phone numbers of any kind, found anywhere in the document.
3. All URLs and IP addresses found of any kind, found, anywhere in the document.
4. All email addresses of any kind, found anywhere in the document.
5. All twitter handles of any kind, found anywhere in the document.
6. All Street Addresses of the candidate, found anywhere in the document.
7. All candidate full names, found anywhere in the document.
8. All Candidate Contact Info EXCEPT municipality, region(s), country and postal code.
9. All other Personal Data that we parse for, including
    - Ancestor (FathersName and MothersMaidenName)
    - Availability
    - Birthplace
    - DateOfBirth
    - DrivingLicense
    - FamilyComposition
    - Gender
    - Hukou (HukouCity and HukouArea) (China)
    - Location (CurrentLocation and PreferredLocation)
    - MaritalStatus
    - MessagingAddresses
    - MotherTongue
    - NationalIdentityNumber
    - Nationality
    - Passport
    - Politics (China)
    - Salary (CurrentSalary and RequiredSalary)
    - Visa

    unless they are both inconsequential and cannot be safely removed.

© 2018 Copyright Sovren Group, Inc. All rights reserved. | sovren.com

Internal data

DATA TYPE: CRM DATA

CRM data includes contact info for individuals related to a customer or prospect of Sovren. The CRM database is encrypted at rest. No CRM data will be stored outside of the CRM database.

DATA TYPE: JOB ADVERTISEMENTS OR RESUMES/CVS SENT TO SOVREN TO USE IN ITS QA/DEV PROCESSES

Documents sent to Sovren by its customers and prospects for use in its internal QA/Dev processes may be stored locally on a developer's hard drive in a folder marked "Resumes" or "Jobs" (whichever may be appropriate) for no more than 48 hours. These folders must be encrypted using Windows EFS. At the end of 48 hours, those files MUST be added to the "Resumes" or "Jobs" folder in Sourcegear Vault, and deleted from the local machine (including deleted from the Recycle bin).

Resumes or Jobs received by email must be promptly saved to secure folders as described above, and the emails deleted.

Download access to the "Resumes" and "Jobs" folders in Sourcegear Vault shall be restricted to the Chief QA Officer. Only the Chief QA Officer may have downloads from the Sourcegear Vault Resumes or Jobs archives on his local machine, and then only while conducting active QA sessions and only when those files are downloaded and stored only to EFS-encrypted folders. ALL QA REPORTS must be stored only in EFSencrypted folders.

Either the Security Officer or the Chief QA Officer may grant individual developers access to download some or all of the Sourcegear Vault Resumes or Jobs archives to other machines, using the form shown as Appendix A hereto. Signed copies of that form are to be provided to the Security Officer, who is to store the form into the correct security archive, and also to set a calendar item to audit compliance with the form's dictates.

© 2018 Copyright Sovren Group, Inc. All rights reserved. | sovren.com

Application data

SOVREN APPLY:

The Sovren Apply will store resumes sent to it in an encrypted database. This data will include PII, but such PII is necessary to the purpose of the application (finding the right people to hire, and contacting them), and is encrypted at rest and subject to inapplication authentication schemes.

QWIK RECRUIT:

QwiK Recruit will store all of its data in an encrypted database. This data will include PII, but such PII is necessary to the purpose of the application (finding the right people to hire, and contacting them), and is encrypted at rest and subject to in-application authentication schemes.

Summary

These practices will render stored parsed results unable to be used to identify persons. As a result of storing no PII, we will have the safest of all possible security profiles for stored SaaS Service data data: an empty safe.

© 2018 Copyright Sovren Group, Inc. All rights reserved. | sovren.com