Data Security & Privacy Statement

Cyber Security Overview (*August 1st, 2021*)

VISIBILITY SOFTWARE CYBER SECURITY OVERVIEW

Introduction

Maintaining protection of the data entrusted to our care is of the utmost importance to Visibility Software. This Procedure applies to all data maintained in the hosted ("cloud") environment with Visibility Software.

This document should be read in conjunction with Visibility Software's Privacy Policy and Visibility Data Breach Policy.

Infrastructure

- Cloud environment established on Amazon AWS
- Main data center for Amazon AWS is on the east coast
- Rolling 14 days of backups are stored in a data center on the west coast
- Email platform leverages Amazon SES with domain authentication
- Domain monitoring to track accessibility and uptime

Access

- Access is restricted to key personnel
- Multi-factor authentication to access servers
- Additional authentication to access data

Defense

- Secure Sockets Layer (SSL) enforced for system access and email delivery
- Multiple firewalls
- Intrusion detectors
- Antivirus technology
- 24-hour NOC monitoring with rapid response teams

VISIBILITY SOFTWARE DATA BREACH PROCEDURE

Introduction

Visibility Software LLC ("Visibility Software") is committed to protecting your data through our compliance with this data breach procedure ("Procedure"). Maintaining protection of the data entrusted to our care is of the utmost importance to Visibility Software.

This Procedure applies to all data maintained in the hosted environment with Visibility Software.

This Procedure may change from time to time, so please check the Procedure periodically for the most current version. If you have any questions about the meaning or interpretation of this Policy, the English-language version of this Policy is the official text.

Visibility Software is committed to managing personal information in accordance with the Visibility Software Privacy Policy.

This document sets out the processes to be followed by Visibility Software staff in the event that Visibility Software experiences a data breach or suspects that a data breach has occurred. A data breach involves the loss of, unauthorized access to, or unauthorized disclosure of, personal information.

This document should be read in conjunction with Visibility Software's Privacy Policy.

Process

Initial Alert

Where a privacy data breach is suspected or known to have occurred, any member of Visibility Software staff who becomes aware of this must, within 24 hours, alert the CEO and COO of Visibility Software.

The Information that should be provided (if known) at this point includes:

- When the breach occurred (time and date)
- Description of the breach (type of personal information involved)
- Cause of the breach (if known) otherwise how it was discovered
- Which system(s) if any are affected?
- Which organizations/servers are involved?
- Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach)

Assess and Determine the Potential Impact

Once notified of the information above, the COO must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity.

Criteria for determining whether a privacy data breach has occurred

- Is personal information involved?
- Is the personal information of a sensitive nature?
- Has there been unauthorized access to personal information, or unauthorized disclosure of personal information, or loss of personal information in circumstances where access to the information is likely to occur?

For the purposes of this assessment the following terms are defined in the Privacy Policy: personal information, sensitive information, unauthorized access, unauthorized disclosure and loss.

Criteria for determining severity

• The type and extent of personal information involved
• Whether multiple individuals have been affected
• Whether the information is protected by any security measures (password protection or encryption)
• The person or kinds of people who now have access
• Whether there is (or could there be) a real risk of serious harm to the affected individuals

Data Breach Managed

• Ensure that immediate corrective action is taken, if this has not already occurred (corrective action may include: retrieval or recovery of the personal information, ceasing unauthorized access, shutting down or isolating the affected system); and
• Create a summary report. The report must contain the following:
• Description of breach or suspected breach
• Action taken
• Outcome of action
• Processes that have been implemented to prevent a repeat of the situation.

Response

There is no single method of responding to a data breach and each incident must be dealt with on a case by case basis by assessing the circumstances and associated risks to inform the appropriate course of action.

The following steps may be undertaken (as appropriate):
• Immediately contain the breach (if this has not already occurred).
• Corrective action may include: retrieval or recovery of the personal information, ceasing unauthorized access, shutting down or isolating the affected system.
• Evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach
• Call upon the expertise of, or consult with, relevant staff in the particular circumstances.
• Engage an independent cyber security or forensic expert as appropriate.
• Assess whether serious harm is likely
• Make a recommendation whether this breach constitutes notification to Customers.

The “Response Team” must undertake its assessment within 48 hours of being convened.

Notification

Having regard to the Response team’s recommendation, COO will determine whether there are reasonable grounds to notify customer of the occurrence (or suspected occurrence) of data breach.
If there are reasonable grounds, the COO must prepare a prescribed statement and provide a copy to Customer as soon as practicable (and no later than 48 hours after becoming aware of the breach or suspected breach).Visibility Software will NOT notify each individual in the Cyber Recruiter system (aka Applicants) and it is the responsibility of the Customer to communicate the data breach to the applicants affected.

VISIBILITY SOFTWARE PRIVACY POLICY

Introduction

Visibility Software LLC (“Visibility Software”) respects your privacy and is committed to protecting it through our compliance with this privacy policy (“Policy”). Maintaining protection of the data entrusted to our care is of the utmost importance to Visibility Software.

This Policy describes the types of data you may collect from your applicants/employees when accessing the site hosted by Visibility Software. It also describes our policies and practices for collecting, using, protecting, and disclosing that data.

Please note that supplementary rules apply in relation to individuals whose data is collected if they are located in the European Union or European Economic Area. (Please see appendix A: EU Privacy Notice.)

This Policy applies to personal data collected on a Careers/Applicant Self-Service site hosted with Visibility Software.

This Policy may change from time to time, so please check the Policy periodically for the most current version. If you have any questions about the meaning or interpretation of this Policy, the English-language version of this Policy is the official text.

Data Collected and How It Is Collected

The Careers page of Cyber Recruiter can collect several types of personal data about an applicant. What actually is collected is determined by the setup an organization hosting a system with Visibility Software determines. Visibility Software does not dictate which pieces of information are collected. The organization hosting Cyber Recruiter with Visibility Software should review all legal requirements before asking for specific information from an applicant. Information collected could include:

• Data by which an applicant may be personally identified, including name, postal address, email address, or telephone number
• Data by which an applicant's experience may be identified, including school history, work history, and professional references
• Data by which an applicant's background may be verified, including social security number and birthdate

Data could be collected from:

• Applicants applying for jobs
• Employees already employed by an organization

This data is collected:

• Directly from the applicant/employee when applying to a job or updating the profile.

Data Provided

We collect data provided when an applicant interacts with a Website in our environment. That data includes:

• Personal data provided when submitting an application.
• Records and copies of correspondence (including email and other electronic messages)

Features that are developed in the future may result in the collection of additional new personal data.

Although we limit access to certain pages and set certain privacy settings for data based on the account profile used to sign in, no security measures are perfect or impenetrable. Additionally, we cannot control the actions of others with whom authorized users may choose to share their access.

How Personal Data Is Used

Data collected, including any personal data, is used:

• To evaluate an applicant's suitability for a job
• To contact an applicant about a job
• To comply with any legal obligations
• To notify an applicant about potential new jobs
• To remind an applicant of an outstanding action item during the hiring process
• For any other purpose where the applicant's consent is obtained

Disclosure of Personal Data

You may disclose personal data collected as described in this Policy:

• To contractors, service providers, and other third parties used to support your business and who are bound by contractual obligations to keep personal data confidential and use it only for the purposes for which you disclose it to them
• To fulfill the purpose for which the applicant provided it
• For any other purpose disclosed by you when the applicant provided the data
• With the applicant's consent

You may also disclose an applicant's personal data:

• To comply with any court order, law, or legal process, including to respond to any government or regulatory request.
• If you believe disclosure is necessary or appropriate to protect the rights, property, or safety of the applicant. This includes exchanging personal data with other companies and organizations for the purposes of fraud protection and credit risk reduction.

Visibility Software Privacy Personal Data

Visibility Software will not sell, trade, or share an applicant's personal data, including their name, phone number, email, or physical address, nor will it send mailings on behalf of other unrelated organizations. This policy applies to all data collected by organizations using a site hosted by Visibility Software, both online and offline, as well as any electronic, written, or oral communication.

Accessing and Correcting Personal Data

Applicants may access and correct data using the following methods:

• When applying to a job
• By signing into the Self-Service portal.
• By emailing the organization to request access to, correct, or delete any personal data provided to the organization.

You may choose not to accommodate a request to change or delete data if you believe the change or deletion would violate any law or legal requirement or cause the data to be incorrect.

If an applicant requests to delete content, copies of the content may remain viewable in cached and archived pages or might have been copied or stored by other users. Proper access and use of data provided, is governed by your Terms of Use, although for EU/EEA-based individuals this does not prejudice the applicant's mandatory rights under EU Protection Law (see Appendix A: EU Privacy Notice).

Return, Transfer, or Disposal of Information

All Confidential Information and/or Personal Data must be returned, transferred, or Disposed of in accordance with applicable laws and regulations, the agreement between the Client and Visibility, and Visibility's policies and procedures that control the Disposal of Confidential Information

and/or Personal Data. Visibility will take reasonable measures to ensure that such Disposal is performed in a secure manner and includes temporary files created as a result of the Processing of Personal Data.

When Disposing of Client Data, Personnel shall take reasonable measures to protect against unauthorized access to or use of the information in connection with its Disposal. Examples of such reasonable measures include, but are not limited to, any of the following:

a. Burning, pulverizing, or shredding of papers or records containing Information so that the Information cannot be practicably read or reconstructed;

b. Destroying or erasing electronic media containing Information so that the Information cannot practicably be read or reconstructed, consistent with reasonable standards

Visibility will provide further details about its internal Document Retention policy to its Clients upon written request.

Children Under the Age of 16

The careers site is not intended for children under 16 years of age. Do not knowingly collect personal data from children under 16 without parental consent. No one under age 16 may provide any personal data to or on your Careers site. If you expect applicants under the age of 16, seek legal counsel regarding how to set up your Careers site to be compliant. If you learn you have collected or received personal data from a child under 16 without verification of parental consent, delete that personal data.

Data Security

Visibility Software has implemented technical and operational measures designed to secure personal data from accidental loss and from unauthorized

access, use, alteration, and disclosure. When developing new or enhancing existing systems and processes, Visibility Software implements appropriate data protection throughout its data processing operations. All personal data provided is stored on password-protected databases on our secure servers behind firewalls and we use Secure Sockets Layer (SSL) to ensure that the transmission of sensitive data is encrypted and appropriately safeguarded. We train our employees on the importance of data security and focus specifically on practices for protecting against unauthorized disclosure of personal data. We have a documented incident response plan for promptly acting upon events that violate Visibility Software's security or privacy policies, should they occur, and this plan is reviewed and updated on an ongoing basis.

The safety and security of personal data also depends on you. Where we have given you (or where you have chosen) a password for access, you are responsible for keeping this password confidential. User passwords registered are encrypted to ensure protection against unauthorized access to personal data. We ask you not to share your password with anyone.

Unfortunately, the transmission of personal data via the internet is not completely secure. Although we do our best to protect personal data, we cannot guarantee the security of personal data transmitted over any public network. Any transmission of personal data is at your own risk. Without prejudice to any mandatory legal obligations to which we may be subject, we are not responsible for circumvention of any privacy settings or security measures contained on our Website.

Changes to Our Privacy Policy

Visibility Software may change, add, modify, or remove portions of this Policy at any time, which shall become effective immediately upon posting on this page. The date the Policy was last revised is identified at the bottom of the

policy. It is your responsibility to review this Policy for any changes. By continuing to use our hosted environment, use our services, or participate in our programs, you agree to any changes in the Policy.

Contact Information

If you have any questions about Visibility Software's privacy protection practices, please contact us at productsupport@visibilitysoftware.com

Appendix A: EU Privacy Notice

If an applicant is a resident of the European Union (EU) or European Economic Area (EEA) whose personal data is collected, the following additional information applies to the applicant.

Introduction

If the applicant is an EU or EEA resident and you knowingly collect personal data, you will do so in accordance with applicable laws that regulate data protection and privacy.

This includes, without limitation, the EU General Data Protection Regulation (2016/679) ("GDPR") and EU member state national laws that implement or regulate the collection, processing and privacy of personal data (together, "EU Data Protection Law").

This EU privacy notice ("EU Privacy Notice"), which should be read in conjunction with Visibility Software's Privacy Policy, provides further information as required under EU Data Protection Law on how Visibility Software handles or processes the personal data collected and with whom it may be shared.

This Privacy Notice also provides information on the applicant's legal rights under EU Data Protection Law and how the applicant can exercise them.

How Personal Data is Collected

All personal information collected, regardless of the location of the applicant, is transferred to the United States because the servers in the Visibility Software environment are all located in the United States. Because of the global nature of your organization, your organization may hold and process personal data that is collected around the world, including within the EU/EEA.

U.S. data privacy laws are currently not considered to meet the same legal standards of protection for personal data as those set out under EU Data Protection Law. However, in order to safeguard personal data received from the EU/EEA, all personal data provided is stored on password-protected databases on our secure servers behind firewalls and we use Secure Sockets Layer (SSL) to ensure the transmission of sensitive data is encrypted and appropriately safeguarded. This is to make sure that the personal data that you receive and process (so far as it relates to residents of the EU/EEA) is properly safeguarded in accordance with similar legal standards of privacy an applicant would enjoy under EU Data Protection Law.

Job Notification

If you provide job notification communications to individuals in the EU/EEA regarding potential job openings that may be of interest, this will be done in accordance with EU Data Protection Law, and in particular where you contact individuals for job notification purposes by SMS, email, fax, social media, and/or any other electronic communication channels, this will only be with the individual's consent.

Individuals are also free to object or withdraw consent to receive job notifications from you at any time, by contacting your organization directly, or removing the monitor on jobs with your organization.

Lawful Grounds on Which You Collect and Process Personal Data

You process applicant personal data for the above purposes, relying on one or more of the following lawful grounds under EU Data Protection Law:

• When an applicant has freely provided specific, informed, and unambiguous consent for your organization to process personal data for particular purposes

• Where you need to process and use the applicant personal data in connection with your legitimate interests and need to be able to effectively manage and operate your global organization in a consistent manner across all territories. You will always seek to pursue these legitimate interests in a way that does not unduly infringe on the applicant's legal rights and freedoms, particularly the applicant's right to privacy; and/or

• Where you need to comply with a legal obligation or for the purpose of your being able to establish, exercise, or defend legal claims

Please also note that some of the personal data received and that you process may include what is known as "sensitive" or "special category" personal data about the applicant, for example, personal data regarding the applicant's ethnic origin or veterans' statuses. If you process such sensitive or special category data, you will do it only in situations where:

• The applicant has provided you with their explicit consent to use it
• You have a legal obligation to process such data in accordance with EU Data Protection Law
• It is needed to protect the applicant's vital interests (or those of someone

else), such as in a medical emergency
• The applicant has clearly chosen to publicize such information; or
• It is needed in connection with a legal claim that you have or to which you may be subject

Disclosing Personal Data to Third Parties
You may disclose the applicant's personal data to certain third-party organizations that are processing data solely in accordance with your instructions ("Data Processors"), such as companies and/or organizations that support your business and operations (for example, providers of web or database hosting, IT support, screening agencies you use to conduct fraud checks, or mail management service providers), as well as professionals you use such as lawyers, insurers, auditors, or accountants. You use only those Data Processors that can guarantee to you that adequate safeguards are put in place by them to protect the personal data they process on your behalf.
In certain circumstances, for example, if you travel on business, we may also disclose the applicant's personal data to third parties called "Data Controllers." Such third parties may include travel agencies, airlines, car rental agencies, and hotels. Due to the nature of the business of the Data Controllers, they will make their own determinations as to how they process personal data. As Data Controllers, they are required to follow the EU Data Protection Law and are required to protect personal data with adequate safeguards and provide the applicant with notice if their processing goes beyond the instructions provided. The types of external third-party Data Controllers listed above may handle personal data in accordance with their own chosen procedures, and the applicant should check the relevant privacy policies of these companies or organizations to understand how they may use personal data.
Other than as described above, you will treat the applicant personal data as private and will not routinely disclose it to third parties without the applicant knowing about it. The exceptions are in relation to legal proceedings or where

you are legally required to do so and cannot tell the applicant (such as a criminal investigation). You should always aim to ensure that the applicant personal data is used only by third parties with whom you deal for lawful purposes and who observe the principles of EU Data Protection Law.

How Long Will You Retain Personal Data

Cyber Recruiter has the ability to retain personal data indefinitely. Your organization should determine a retention polity for personal data identifying an applicant for as long as necessary in the circumstances — for instance, as long you are considering an applicant for a job or find the applicant data useful for future job searches, for a reasonable period to send job notifications, or as may be needed to enforce or defend contract claims or as is required by applicable law.

Visibility Software has adopted a Records Management Policy. When a contract is ended, databases storing jobs and personal applicant data is removed completely from the Visibility Software environment no longer than 30 days after the end of the contract.

Personal Data Rights

In accordance with the applicant's legal rights under EU Data Protection Law, the applicant has a "subject access request" right, under which the applicant can request information about the personal data that you hold about the applicant, for what you use that personal data and to whom it may be disclosed, as well as certain other information.

Usually you will have one month to respond to a subject access request. However, you should reserve the right to verify the applicant's identity, and you may, in case of complex requests, require a further two months to respond. You may also charge for administrative time in dealing with any manifestly unreasonable or excessive requests. You may also require further information to locate the specific data the applicant seeks, and certain legal exemptions under EU Data Protection Law may apply when you respond to the applicant's subject access request.

Under EU Data Protection Law, EU/EEA residents also have the following rights, which the applicant may exercise by making a request to you in writing:

- That you correct personal data that you hold about an applicant that is inaccurate or incomplete
- That you erase the applicant's personal data without undue delay if you no longer need to hold or process it
- To object to any automated processing (if applicable) that you carry out in relation to the applicant's personal data
- To object to your use of the applicant's personal data for job notifications
- To object to and/or to restrict the use of the applicant's personal data for a purpose other than those set out above unless you have a compelling legitimate reason; or
- That you transfer personal data to another party where the personal data has been collected with the applicant's consent or is being used to perform services under a contract with the applicant and is being processed by automated means

So you can fully comply, please note that these requests may also be forwarded to third-party data processors that are involved in the processing of the applicant's personal data on your behalf.

If the applicant would like to exercise any of the rights set out above, please have them contact you directly.