



Privacy and Data Protection Policy

Table of Contents

Introduction	3
Defined Terms	4
Lawful Basis of Processing	5
Personal Data We Collect.....	6
Privacy Notices	7
How We Use Your Personal Data	7
How Long Your Data is Stored	8
Information We Share	8
Lawful Requests	9
Mergers and Acquisitions	9
Personal Data of Children.....	10
Safeguarding Your Personal Data.....	10
International Transfers	10
Individual Rights Regarding Data Processing.....	10
How to Submit a Request.....	12
Automated Decision Making.....	13
Supervisory Authorities	13
Website Privacy.....	13
Data Breaches	15
Updates to this Policy.....	15
Contact	15

Security Management Resources® Privacy and Data Protection Policy

Effective 1 January 2024

Security Management Resources® - the SMR Group of Companies - are committed to protecting the privacy of our clients, candidates and other visitors who use our website and contract with us for services.

This Privacy and Data Protection Policy (The Policy) informs you how Security Management Resources® (hereinafter “SMR”, “we”, “us” and “our”) prioritizes your privacy, processes and protects your personal data. The Policy concerns the SMR website and any other SMR products or services which collect personal data or which are linked to this Policy or on which this Policy is visible. SMR is the data controller for the processing of personal data under applicable law.

This Policy does not apply to third party websites to which the SMR website, products or services may link.

Introduction

SMR has recently updated our Privacy and Data Protection Policy to clarify how we protect your personal data in keeping with new standards introduced by the European data protection law known as the General Data Protection Regulation (GDPR).

We want you to know what personal data we collect in our interactions with you. We also want you to understand your rights in respect of your personal data. This Policy explains the purposes of collecting and use of your personal data and describes how you have adequate control over your own personal data.

All organizations that process personal data are required to comply with data protection legislation. This includes in particular the Data Protection Act 1998 (or its successor) and the EU General Data Protection Regulation (together the “Data Protection Laws”). The Data Protection Laws give individuals certain rights over their personal data and imposes certain obligations on the organizations that process their data.

Privacy and data protection standards and laws vary by country and are subject to change. We recommend that you read this Policy carefully and check back frequently to review any updates made as a result of evolving privacy and data protection laws.

At any point in time should you have any questions about this Policy, please contact privacy@smrgroup.com.

Defined Terms

- **“SMR”** means Security Management Resources® Inc., Security Management Resources® Limited, and Security Management Resources® Asia Limited.

Additionally, The General Data Protection Regulation (GDPR) effective 25 May 2018 in the UK has terminology that is helpful to keep in mind as you read through the SMR Policy.

- **“consent”** means any freely given, specific, informed and unambiguous indication of an individual’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **“data controller”** means an individual or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **“data processor”** means an individual or organization which processes personal data on behalf of the data controller.
- **“personal data” *** means any information relating to an individual who can be identified, such as by a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **“personal data breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **“process”, “processing” or “processed”** means any operation or set of operations performed on personal data, such as collection, recording, organization, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **“profiling”** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.
- **“sensitive personal data” *** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data

concerning health, an individual's sex life or sexual orientation and an individual's criminal convictions.

- **“Supervisory authority”** means an independent public authority which is responsible for monitoring the application of data protection.

* For the purposes of this Policy we use the term ‘personal data’ to include ‘sensitive personal data’ except where we specifically need to refer to sensitive personal data.

Lawful Basis of Processing

SMR will only process personal data where we have a legal basis for doing so. We may collect and process your data on one or more of several legal bases:

1. Your consent, whereby we have obtained your prior expressed consent (written, verbal or online) to the processing of your personal data. This legal basis is used only in relation to processing that is entirely voluntary. It is not used for processing that is necessary or obligatory in any way.
2. Any contract between you and us. The processing is a contractual necessity in connection with any contract between SMR and you.
3. Our legitimate interest. We have a legitimate interest in carrying out the processing to manage, operate or promote our business and that legitimate interest is not overridden by your legally protected interests, fundamental rights or freedoms.
4. Processing is necessary for compliance with a legal obligation that we are subject to.

We may also use your information during the course of internal audits to demonstrate our compliance with certain industry standards.

SMR will review the personal data we hold on a regular basis to ensure it is being lawfully processed and it is accurate and relevant. Prior to transferring personal data to any third party (i.e. past, current or prospective employers, suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party such as software solutions providers and back office support, we will establish that we have a legal reason for making the transfer.

You have a right to withdraw your consent to the processing of your personal data at any time by contacting privacy@smrgroup.com.

Personal Data We Collect

As a recruitment and consultancy business, SMR collects and processes both personal data and sensitive personal data. It is necessary for us to collect an adequate amount of relevant data in order to conduct our business. We are also required to do so to comply with other legislation, and to keep this data for different periods depending on the nature of the data.

We may collect personal data from you in a variety of ways. This may include directly from you, from your devices that interact with our services or from third party sources.

Information collected directly from you may include:

- Contact details: i.e. your name(s), email address(es), telephone number(s), postal address(es);
- Demographic information: i.e. gender, date of birth or age, ethnicity, language, title or degree.
- Information related to your access of our secure candidate portal to include username and password.
- Any consents or communications that you provide to us.
- Personal interests notified by you.
- Work-related information and qualifications provided by you that might normally be found on a resume or CV: i.e. employment history; current or past employer's names and contact details.
- Educational background and other qualifiers: i.e. degrees, certifications, achievements, competencies and skills, memberships in professional organizations.
- Other information collected on the basis of your prior expressed, voluntary consent, including public social media profiles.
- Compensation information.
- Position descriptions and other details related to client engagements such as organizational structure and reporting relationships to include names and titles.

Information collected when our website or products or services are used:

- Your user account identity if you log in to our secure candidate portal.
- Your browser, operating system, device model, IP-address and time of access.
- Other information collected based on your consent.

Information collected from third party service providers:

- Personal data from third parties that may include data resulting from the completion of assessment instruments, reference details and other information that would normally be collected during recruitment activities.

Please review Section, **“Website Privacy”** that further discusses privacy issues specifically relevant to website usage.

Privacy Notices

Where SMR collects personal data from an individual, we will give the individual a privacy notice at the time when we first obtain the personal data.

Where we collect personal data other than from an individual directly, we will give the individual a privacy notice within a reasonable period after obtaining the personal data, but at the latest within one month. If we intend to disclose the personal data to a third party, then the privacy notice will be issued when the personal data are first disclosed (if not issued sooner).

Where SMR intends to further process the personal data for a purpose other than that for which the data was initially collected, we will give the individual information on that other purpose and any relevant further information before we do the further processing.

How We Use Your Personal Data

The Data Protection Laws require that personal data is processed lawfully, fairly and in a transparent manner. SMR processes personal data in relation to our own staff, employment seekers (candidates) and individual client contacts. SMR is a data controller for the purposes of the Data Protection Laws.

We may hold personal data on individuals for the following purposes:

- To communicate with you.
- Administration and processing of candidates' personal data for the purposes of providing employment services, including processing using software solution providers and back office support.
- Administration and processing of clients' personal data for the purposes of introducing candidates, providing consultancy services and execution of any additional contractual obligations.
- Accounts and records.
- Advertising, marketing, public relations and customer services.
- Staff administration.

From time to time, we may conduct surveys or studies designed to measure your preferences, expectations and opinions on a particular issue or issues. The processing of personal data collected through such research is governed by this Policy. If you participate in any such survey or study, we will first have obtained any necessary consent, where required for such use, in accordance with the applicable law.

We use anonymized data for reporting purposes. Such data have been anonymized and cannot be used to identify you. Such anonymized data may contain:

- Aggregate visitor numbers of our website.
- Aggregate visitor numbers of our social media sites.
- Average visit duration.

Please review the Section of this Policy, **“Website Privacy”** for information specific to website privacy.

We may process your personal data for the purposes of detecting, investigating and preventing unlawful activities. We may provide your information to law enforcement authorities based on their request or based on a legal basis defined in any applicable law for prevention and investigation of unlawful activities. We may disclose your personal data to any party in response to an order from a court of competent jurisdiction.

How Long Your Data is Stored

SMR takes every reasonable step to ensure that your personal data are only processed for the minimum period necessary for the purposes set out in this Policy.

We will retain candidate data only as long as your online candidate profile account is valid, plus the applicable period for limitation of legal claims and any additional periods required or permitted under applicable law. If you have created a candidate profile, you may indicate you no longer wish to be considered for employment opportunities or request that your data be deleted as described in the section “Individual Rights Regarding Data Processing”.

You will be asked to update your data on a regular basis. It is important to regularly review your personal data for accuracy and ensure it is kept up-to-date.

We may retain your personal data for the duration of any period necessary to establish, exercise or defend any legal rights.

Information We Share

Except as described in this Policy, SMR does not sell, lease, rent or otherwise disclose your personal data to any third party.

SMR only discloses your data to approved third parties with whom we have trusted, binding relationships. We may disclose your personal data to:

- To SMR Clients: candidate personal data - for the purpose of placing candidates in their employ.
- To SMR Candidates: client data - for the purpose of evaluating the organization and any positions for possible employment.
- Third party candidate management system providers; for the purpose of maintaining accurate candidate profiles.
- Third party service providers of assessment testing instruments, to conduct candidate assessments.
- Third party service providers of background and reference checking services, to verify employment and conduct preliminary background screening.
- Past or current employers to obtain references.
- Intermediaries such as umbrella companies.
- Back office support.

Data that is shared, stored and/or processed by these authorized third parties is based on our prior instructions in binding contracts that are compliant with the requirements of applicable law and are conducted in accordance with this Policy. Prior to disclosing your data to any third party, we will have first obtained your necessary expressed consent, where required for such use, in accordance with the applicable law.

These authorized third parties are not permitted to use your personal data for any other purpose other than those described in this Policy. They are required to keep your personal data strictly confidential.

You, or another data controller at your request, have the right to request that SMR rectify any inaccurate or incomplete personal data concerning you even if it has been given to a third party. In this case, SMR will tell those third parties that we have received a request to rectify the personal data unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold; however, SMR will not be in a position to audit those third parties to ensure that the rectification has occurred.

Lawful Requests

We may be required by the binding requirements of applicable law, or for the purposes of responding to legal proceedings or other lawful requests to disclose your personal data to authorities or third parties. We may also disclose or otherwise process your personal data, in accordance with applicable law, to defend our legitimate interests (i.e. in civil or criminal legal proceedings).

Mergers and Acquisitions

Each of the SMR companies are privately held and managed by their owners. In the event of any change of ownership or reorganization of our businesses (i.e. mergers and acquisitions), we may disclose your personal data to potential or actual purchasers or their advisers, where appropriate. We will promptly notify you of any such action.

Personal Data of Children

SMR's business is not targeted to children. Therefore, we do not collect personal data of children and will not carry out any automated decision-making or profiling using the personal data of a child.

Safeguarding Your Personal Data

Privacy by design and by default is at the heart of safeguarding your personal data. We want you to know that appropriate safeguards are in place to adequately protect your privacy.

SMR has implemented technical and organizational security measures designed to ensure that data protection is integral to all processing activities and to protect your personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, unauthorized access and any other unlawful or unauthorized forms of processing in accordance with applicable law.

We maintain a variety of physical, electronic and procedural safeguards to protect your personal data including encryption and a secure candidate portal. Only SMR appointed personnel and authorized third party companies, as described in the section "Information We Share", are entitled to access or process your personal data.

International Transfers

Our services may be provided using resources and servers located in various countries, partly located outside of EU/EEA. Therefore, your personal data may be transferred across international borders outside the country in which you use our services. We will ensure that any such transfer is covered by appropriate contractual measures (i.e. using European Commissions Standard Contractual Clauses), that the transfer has an appropriate legal basis and that the data processing and confidentiality fulfills the requirements in relevant laws.

Our candidate management system is certified under the [Privacy Shield Framework](#) as relates to compliant data flows between the EU (and Switzerland) and the US.

Individual Rights Regarding Data Processing

SMR will endeavor to ensure that the personal data we possess are accurate. While we take reasonable steps to ensure that the personal data we process are limited to that reasonably required in connection with the purposes set out in this Policy, we encourage you to regularly update the information in your candidate profile if you

have set up one with us. Below are rights with regard to the processing of your personal data that you may be able to exercise, subject to applicable law.

A. Providing your Personal Data

You may choose not to provide your personal data to us. Should you elect not to provide your personal data, we may be unable to consider your candidacy for employment. Should you choose to provide your personal data, we will give you a privacy notice when we first obtain the data from you.

B. Subject Access Requests

You may have the right to request access to or obtain copies of your personal data.

C. Validation and Correction

If you have created a candidate profile you can log in and edit your personal data. If you do not have one, please contact us so we can act upon your request to quickly rectify, remove or complete your information.

D. Erasure

You may have the right to ask us to erase your personal data. SMR cannot keep a record of individuals whose data it has erased, so you may be contacted again by us if we come into possession of your personal data at a later date. If we have shared the data, we will take reasonable steps to inform other data controllers and data processors to erase your personal data, taking into account available technology and the cost of implementation. Upon receipt of your request, we will investigate your request before deciding what action to take.

E. Restriction of Processing

If you believe that your personal data is inaccurate, the processing of it is unlawful or we are not processing your data in accordance with the processing purpose, you may have the right to request we restrict processing it. If we have given the personal data to any third parties, we will tell those third parties that it has received a request to restrict the personal data unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold; however, SMR will not be in a position to audit those third parties to ensure that the rectification has occurred.

F. Data Portability

You may have the right to receive personal data that you have provided to us, in a structured, commonly used and machine-readable format in order to transmit those data to another data controller in circumstances where the processing is based on your consent or a contract; and, the processing is carried out by automated means.

G. Right to Object

You have the right to object, on legitimate grounds, to the processing of your personal data. If you object to your personal data being processed, we will cease processing unless we have compelling legitimate grounds to continue to process the personal data which override the individual's interests, rights and freedoms or for the establishment, exercise or defense of legal claims.

H. Unsubscribing

Subscription to any of SMR's products, services or marketing is entirely voluntary and requires a proactive action including expressed consent on the part of the individual. We include an unsubscribe link in all electronic messages we send you (i.e. job announcements, newsletters). You may withdraw your consent to receiving these at any time. Should you do so, we will update our database and will not send you further messages of this nature. We may continue to contact you to the extent necessary for the purposes of any other services you have requested.

I. Withdrawing Your Consent

You may withdraw your consent to the processing of your personal data at any time. If your consent is withdrawn, it does not prevent us from processing your personal data based on other legal bases such as storing your data as required by applicable law. Withdrawal of consent does not affect the lawfulness of any processing performed prior to the date on which we receive notice of such withdrawal.

How to Submit a Request

All requests regarding individual rights should be sent to privacy@smrgroup.com. You may also click on the [Contact Us](#) form on the SMR website. Additionally, you may contact us via postal mail at:

Security Management Resources®
41 West Lee Highway; Suite 59-108
Warrenton, VA 20186 USA

SMR shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision-making processes or profiling within one month of receipt of the request. We may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Where we consider that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature, we may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

Automated Decision Making

The nature of SMR's work does not lend itself to, nor do we engage in or employ any automated decision making. Should that change at a future date, SMR will not subject individuals to decisions based on automated processing that produce a legal effect or a similarly significant effect on the individual, except where the automated decision is necessary for the entering into or performance of a contract between the data controller and the individual, is authorized by law or the individual has given their explicit consent.

Supervisory Authorities

Should you believe that our processing of your personal data infringes on your legal rights, you may contact the appropriate supervisory authority for your location.

- In the US the supervisory authority is the [Federal Trade Commission](#) (FTC).
- In the UK the supervisory authority is the [Information Commissioner's Office](#) (ICO).
- A current list of websites for additional supervisory authorities can be found online [here](#).

Website Privacy

We want you to have a secure, seamless experience during your visit to the Security Management Resources® website. Please note that certain features on our website are offered by third parties and the third-party privacy policies apply.

The SMR website is owned and operated by SMR in the United States, but the information you provide will be accessible by SMR employees and third-party suppliers in other countries in accordance with this Policy. If you are visiting the SMR website from a country other than in the United States, your communications with us will necessarily result in the transfer of information across international borders. The level of legal protection for personal data is not the same in all countries, however we will take security measures described in this Policy in an effort to keep your information secure.

By using the SMR website, you understand that your personal data will be stored and processed in the United States and in any country to which we may transfer your information in the course of our business operations.

- **Cookies**

Cookies are small text files that are placed on your computer by websites that you visit. Cookies are widely used to make websites or services work, or to work more efficiently, as well as to provide reporting information. The SMR website utilizes cookies that allow you to navigate through the site smoothly. These cookies do not collect information that can identify you. Rather they are

anonymous and simply move the user through the site. There is no third-party advertising on the SMR site nor do we share any of your information. Therefore, no targeting or advertising cookies are present on the SMR website.

You can easily disable cookies in your browser. Doing so may result in a less than optimal experience on the SMR website, but it will not affect your ability to access the information on the website or log in to our secure candidate portal.

By using the SMR website you agree that we can place these types of cookies on your device.

You can find additional information about cookies by visiting [All About Cookies.org](#).

- **Links**

There are links to third party websites on the SMR website.

- **Social Media**

- Our website and services use options which enable you to share content on social media. Links to SMR's pages on social media outlets are available in several locations on the site. Should you choose to follow these links and leave the SMR website, each such third-party service provider may collect personal data regarding your visits and interaction with its services based on its own policies and rules concerning data privacy. Please review the privacy policy for each of these social media sites as SMR cannot be held liable for privacy policies or terms and conditions concerning data privacy of such third parties.

- **Sharing**

- ShareThis is available to facilitate your ability to share the "Insights" section of the SMR website via social media. Please review their [Privacy Notice](#) prior to utilizing their service.

- **Content**

- Content published on the SMR website often includes links to third party sites that contain additional information on a topic, event or article. Should you choose to follow these links and leave the SMR website, each such third-party service provider may collect personal data regarding your visits and interaction with its services based on its own policies and rules concerning data privacy.

- **Analytics**

SMR uses Google Analytics to analyze usage of our website. The information that Google Analytics collects is in an anonymous form. It helps to compile reports so that we can understand usage of our website and improve it. If you want further information about how Google Analytics function or do not want your data used by Google Analytics, please visit Google's "[Safeguarding your data](#)" or the [Google Analytics Opt-out Browser Add-on](#) page.

Data Breaches

Should SMR establish that a personal data breach has taken place, we will take steps to contain and recover the breach. Where a personal data breach is likely to result in a risk to the rights and freedoms of any individual in the UK, we will notify the ICO. Where the personal data breach happens outside the UK, we will alert the relevant supervisory authority for data breaches in the effected jurisdiction.

Should SMR identify a personal data breach resulting in a high risk to the rights and freedoms of any individual, we will notify all affected individuals without undue delay.

We will not be required to tell individuals about the personal data breach where:

- We have implemented appropriate technical and organizational protection measures to the personal data affected by the breach, in particular to make the personal data unintelligible to any person who is not authorized to access it, such as encryption.
- We have taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialize.
- It would involve disproportionate effort to tell all affected individuals. Instead, SMR will make a public communication or similar measure to tell all affected individuals.

Updates to this Policy

SMR reserves the right to change and modify this Policy from time to time. When we update this Policy, we will modify the “Effective Date” to indicate when such changes have come into effect.

If the changes are material and affect you in an adverse way, we will contact you via email and/or prominently post a notice advising the change at the beginning of this Policy.

Contact

Please contact SMR regarding any privacy or data protection issues at:

privacy@smrgroup.com

Security Management Resources®, Inc.
Attention: Privacy Officer
41 West Lee Highway; Suite 59-108
Warrenton, VA 20186 USA