MANDIANT
YOUR CYBERSECURITY ADVANTAGE

Mandiant Candidate Data Processing Acknowledgement

I acknowledge that I have reviewed the following information about Mandiant's data processing practices*.

As a candidate of Mandiant, you are aware that Mandiant takes your fundamental right to privacy and the respect for, and compliance with, global data protection laws, including the EU General Data Protection Regulation (GDPR), very seriously. We strive to only collect, process, access, share, store, and/or transfer personal data that is absolutely required to manage the recruitment process and potential employment relationship and provide you with opportunities that benefit you. The personal data we collect about you is only used for the purposes for which it was provided. We do not take liberties with your personal data.

As a globally compliant organization, Mandiant endeavors to be open and transparent about the use of your data, how long it is maintained, where it is stored and who has access to it. Mandiant and its service providers are based in the United States. If a candidate is located outside of the United States, the candidate personal data may be transferred to the United States. We ensure we are abiding by our obligations to meet the requirements under applicable data protection laws. One of these obligations is processing under "legitimate interest." The purpose of this notification is to inform you of the GDPR approved legitimate interests under which we process your personal data.

Your personal data is processed by Mandiant, and in some cases our approved third-party service providers, for a number of different reasons, including:

- recruitment
- execution of the interview and assessment process
- equality in the workplace
- protection of Mandiant property
- a candidate's exercise of their privacy rights
- determination of the employment relationship
- transition from a candidate relationship to an employment relationship

Below is a summary of the circumstances under which Mandiant may process your personal data for legitimate purposes without the need to obtain your explicit, freely given consent.

Candidate Data Processing

Mandiant processes candidate data for legitimate and common business purposes to establish and manage the recruitment process and potential employment relationship, including establishing compensation and benefits, roles and responsibilities, background checks, badging, adherence to policies and procedures, emergency services, and training and development.

Mandiant Corporate Operations and Due Diligence

Mandiant uses personal data to operate the day-to-day running of our recruitment processes and develop our strategic growth plans. This includes management of relationships, sharing Mandiant intelligence with internal stakeholders, implementing safety procedures, and planning and allocating resources and budgeting.

Crime Detection and Prevention

Mandiant needs to process certain personal data to comply with industry standards, regulators' requirements and other requirements related to fraud prevention, anti-money laundering, and safety and security.

MANDIANT
YOUR CYBERSECURITY ADVANTAGE

Compliance with Foreign Law, Law Enforcement, Court and Regulatory Bodies' Requirements

Mandiant is subject to a multitude of laws and regulations, including reporting obligations to regulators, law enforcement and judicial agencies, and industry regulatory bodies. As a global company, Mandiant is subject to many competing laws that sometimes appear to be in direct conflict with data privacy laws in other parts of the world. Mandiant needs to use legitimate interest processing in many instances to process and share candidate personal data provided we put in place mitigations and safeguards to protect your rights.

For more detailed information related to the processing of your personal data please review our detailed Candidate Legitimate Interest Notification (see below). If you have any additional questions or concerns regarding Mandiant's processing of your personal data please contact Privacy@FireEye.com.

Mandiant will hold your personal data as long as is necessary to determine if it will offer employment to the candidate and for a period of time required to satisfy legal or regulatory obligations.

You have a number of rights under relevant data privacy laws. Depending on where you are based, those rights may include the right to (i) request access or copies of your personal data Mandiant processes, (ii) rectify incorrect personal data, (iii) delete your personal data, (iv) restrict the processing of your personal data, (v) determine the portability of your personal data, (vi) lodge complaints with competent authorities in your country, and/or (vii) request a list with the names and addresses of any potential recipients of your personal data. To exercise one or more of these rights, please contact Privacy@FireEye.com.

Mandiant Notification of Legitimate Interest for Candidate Data Processing

As a candidate of Mandiant, you should be aware that Mandiant takes your fundamental right to privacy and the respect for, and compliance with, global data protection laws, including the EU General Data Protection Regulation (GDPR), very seriously. We strive to only collect, process, access, share, store, and/or transfer personal data that is absolutely required to manage the recruitment process and provide you with opportunities that benefit you. The personal data we collect about you is only used for the purposes for which it was provided and for which you are aware and have had the opportunity to question. As a globally compliant organization, Mandiant endeavors to be open and transparent about the use of your data, how long it is maintained, where it is stored and who has access to it. We also ensure we are abiding by our obligations to meet the requirements under applicable data protection laws. One of these obligations is processing under "legitimate interest." The purpose of this notification is to inform you of the legitimate interests under which we process your personal data. However, before getting into the details of legitimate interests, we want to provide you with a little background on lawful processing under the GDPR.

Under the GDPR, personal data must be processed lawfully, fairly, and in a transparent manner. Processing is considered lawful when it is necessary for the legitimate business or legal interests of Mandiant provided we do not violate the fundamental rights and freedoms of our candidates and alternative workforce. Processing is also lawful when it is required to manage a contract such as an employment contract, and where it is required to comply with a legal obligation. Even under these processing rights, Mandiant must abide by the purpose limitations and data minimization principles defined in the GDPR to ensure we are only collecting, accessing and processing the minimal amount of personal data we need to manage the employment relationship.

MANDIANT
YOUR CYBERSECURITY ADVANTAGE

Your personal data is processed by Mandiant, and in some cases our approved third-party service providers, for a number of different reasons, including:

- recruitment
- execution of the interview and assessment process
- equality in the workplace
- protection of Mandiant property
- a candidate's exercise of their privacy rights
- determination of the employment relationship
- transition from a candidate relationship to an employment relationship

For processing of your personal data to be lawful under the GDPR, Mandiant needs to identify and document our lawful basis for the processing. In situations where Mandiant's legitimate interest for processing your data may not be acceptable under the GDPR, we will use another legal basis for processing, such as explicit, freely given consent. In situations where we must obtain consent, you will have the opportunity to decide whether or not you wish to have your personal data processed for a specific purpose not necessarily required to manage the recruitment process (e.g. surveys, maintaining your resume/CV indefinitely).

Below is a summary of the circumstances under which Mandiant will process your personal data for legitimate purposes without the need to obtain your explicit, freely given consent.

Employment Data Processing

Mandiant processes candidate data for legitimate and common business purposes such as:

- Establishing the recruitment and interview process, including potential roles and associated competencies and experience.
- Salary and compensation considerations
- Background checks and security vetting in recruitment and Human Resources (HR) functions
- Compliance with internal policies, accountability and governance requirements
- Government reporting requirements
- Candidate retention programs
- Travel and expense administration associated with interviews
- Intra-corporations hiring for external or internal candidates

Mandiant Corporate Operations and Due Diligence

Mandiant uses personal data to operate the day-to-day running of our business and develop our strategic growth plans. This includes management of relationships, sharing Mandiant intelligence with internal stakeholders, implementing safety procedures, and planning and allocating resources and budget for the following activities:

- Internal candidate analysis for planning and development
- Reporting and management information for budgeting purposes
- Sharing information internally for planning and staffing allocation
- Monitoring physical access to offices, visitors and CCTV operations in reception and any other restricted areas
- Processing personal data for the purpose of anonymizing/de-identifying/re-identifying it for the purposes of using the anonymized data for other purposes (product improvement, analytics, etc.)

MANDIANT
YOUR CYBERSECURITY ADVANTAGE

Crime Detection and Prevention

Mandiant needs to process certain personal data to comply with industry standards, regulators' requirements and other requirements related to fraud prevention and anti-money laundering, including:

- Crime detection and prevention
- Anti-money laundering watch-lists
- Credit checks and risk assessments
- Embargoed countries
- Terrorist financing detection and prevention
- Anti-fraud purposes - using information gathered from various sources, such as public directories and publicly available online personal or professional profiles, to check identities when purchases are deemed as potentially fraudulent
- Defending claims (e.g. sharing CCTV images for insurance purposes)

Compliance with Foreign Law, Law Enforcement, Court and Regulatory Bodies' Requirements

Mandiant is subject to a multitude of laws and regulations often with reporting obligations to regulators, law enforcement and judicial agencies, and industry regulatory bodies, such as health or financial regulators. As a global company, Mandiant is often subject to many competing laws that sometimes appear to be in direct conflict with data privacy laws in other parts of the world. Mandiant needs to use legitimate interest processing in many instances to process and share candidate personal data provided we put in place mitigations and safeguards to protect your rights. Examples of these instances are:

- Operation of Business Conduct and Ethics Line and Reporting under the Sarbanes-Oxley Act (SOX)
- Economic sanctions and export control list screening under economic sanctions and export control laws
- Data loss prevention software and tools for compliance with data protection laws and client contractual requirements
- Compliance with requests for disclosures to law enforcement, courts and regulatory bodies, both foreign and domestic

If you have any additional questions or concerns regarding Mandiant's processing of your personal data please contact Privacy@FireEye.com.

**Mandiant is responsible for administering Talent Acquisition lifecycle activities for FireEye Security Holdings, LLC during the Transition Services Agreement period, following the divestiture of the FireEye Products business to Symphony Technology Group. Click here to view the Candidate Data Processing Acknowledgement for FireEye Security.*