Metis
GLOBAL RECRUITMENT

# General Privacy Strategy

***General Overview***

On May 25, 2018, European Union's General Data Protection Regulation (GDPR) has entered into force, leading to a new regime applicable to all companies operating in the European Union or targeting EU citizens. Coming after years of discussion at the highest levels, GDPR represents a major change in the legal framework for the protection of personal data.

GDPR was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. It effectively gives individuals more control over how organizations use their data and introduces hefty penalties for organizations that fail to comply with the rules. It also ensures data protection law is almost identical across the EU, meaning that all EU citizens and companies benefit from the same legal treatment.

***Our company's commitment***

As a high-level legal recruitment company, we are aware that our activities are subject to a variety of industry standards and EU regulations. We continue to be committed to ensuring compliance with both such local and international rules and have been working on ensuring the highest standards of compliance of our products. Our team members are constantly working on ensuring that our processes and products do not pose any non-compliance risks with the data protection rules.

Moreover, we have been working on creating an effective privacy culture within the company, to ensure an effective training of all our employees and collaborators and high levels of awareness of potential risks in data handling.

Lastly, we have been working on adapting our materials and internal policies to reflect the Privacy by Design principle of GDPR and to guarantee our clients that we abide by the best standards in the industry as far as privacy is concerned.

***Why this policy exists***

This data protection policy ensures Metis Global Recruitment:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data

- Protects itself from the risks of a data breach

***Data Privacy Principles***

**Privacy by Design**

This principle states that any action a company undertakes that involves processing personal data must be done with data protection and privacy in mind at every step. This includes internal projects, marketing tools and activities, product development, IT systems, recruitment process. To comply with this principle, all our functions, including IT and HR, ensure that privacy is built in during the whole life cycle of a system or process they are using. As the basis for privacy compliance, this principle is directly tied into the following five.

**Purpose limitation**

Processing personal data is only permissible if and to the extent that it is compliant with the original purpose for which data was collected. The only exception to this requirement is where the new purpose is compatible with or directly connected to the original purpose. Indications for this will be any link with the original purpose, the context in which the personal data has been collected, the nature of the personal data, the possible consequences of the intended further processing for data subjects or the existence of appropriate safeguards. While we do evaluate potential exception on a case-by-case basis according to these rules, we are committed to minimizing the applicability of the exception as much as we can.

**Data minimization**

As data controllers, we have to ensure that only personal data which is necessary for each specific purpose is collected and processed. This regards the amount of personal data collected, the extent of the processing, the period of storage and accessibility. Under the GDPR, data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". This links back to the purpose limitation principle above. We are constantly seeking to make sure that we collect enough data to achieve the stated purpose, but not more than absolutely needed.

**Accuracy**

Personal data must be accurate and kept up to date. Inaccurate or outdated data should be deleted or amended. As data controllers, we are committed to taking "every reasonable step" to comply with this principle, including constant updating and verification procedures for the data we hold and process.

**Integrity and confidentiality**

Under the GDPR, personal data must be protected against unauthorized access using appropriate organizational and technical measures. This goes to the heart of protecting the privacy of individuals. As a data controller, we have to assess risks, implement appropriate security for the data concerned and, crucially, check on a regular basis that it is up to date and working effectively. The GDPR introduces strict breach reporting requirements which we are striving to satisfy.

**Accountability and transparency**

According to this GDPR principle, data controllers must be able to *demonstrate* compliance with the GDPR at all times. This means that it is not enough to comply, we also have to be able to prove it and document it. Therefore, we have introduced a range of processes to be able to demonstrate compliance, which vary depending on the complexity of the processing. The following measures taken reflect the concrete commitment we made towards protecting data privacy and our concern for incorporating all these core principles into our daily operations.

**List of measures taken by our company:**

1. **Dedicated Governance Structure**
- Existence of a permanent Data Protection Officer (DPO) function.
- Cooperation between all company functions, coordinated by the DPO, into securing privacy compliance.
- Inclusion of Privacy Compliance as a core value within the company.

2. **Personal Data Inventory and Policy**
- Mapping of data and data fluxes in the company, including the legal bases for processing.
- Monitoring and updating of data and data categories on a regular basis, to ensure that all data privacy principles are respected.

3. **Embedded Data Privacy into our operations**
- Introduction of a Corporate Privacy Strategy, built around "privacy by design".
- Integration of privacy into all our operations, including marketing, social media, online presence and branding, HR, tax and finance, which can be reflected into our documentation and policies.
- Creating services that take into account the Privacy by Design principle and using the same principle in testing and deploying them on the market.

4. **Training and Awareness Programs**
- Privacy Training Strategy, to ensure that all our employees, interns and collaborators who process personal data are appropriately trained, so that

they can quickly identify and respond to any potential risks which may appear in their handling of personal data.
- Creation of a culture of privacy in the firm, through regular trainings, awareness campaigns and exchange of information with all our employees, interns and collaborators.
- Constant training of the person holding the DPO role through individual study, trainings and conferences.

**5. Mitigation of Third Party Risks**
- Evaluate, monitor and maintain data privacy requirements for third parties (e.g., clients, vendors, processors, affiliates) at the highest standards possible, according to our principles.
- Conduct due diligence on third party data sources, whenever selecting them as partners or continuously, for existing collaborations.

**6. Introduction of GDPR rights enforcement mechanisms**
- Close collaboration between all business units with the DPO for incorporation of privacy principles, as well as for implementation and evaluation.
- Preparation of materials to document practices and policies used by each function, to allow easy tracking of data movements.
- Introduction of tools and procedures to accurately and rapidly respond to data subject requests, as required by the regulation.

## General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their line manager if they are unsure about any aspect of data protection.