



GDPR Compliance Policy

1. Introduction

Admicity (hereinafter referred to as "the Company") is committed to protecting and respecting the privacy of individuals whose personal data we collect and process. This policy outlines our approach to compliance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). It ensures that the Company handles personal data in a lawful, transparent, and secure manner.

Please also refer to the Admicity Data Security and Compliance Policy for Student Information Integration

2. Scope

This GDPR Compliance Policy applies to all employees, contractors, and third-party service providers involved in the collection, processing, and storage of personal data at Admicity. It covers all personal data processing activities within the Company's operations, including customer data, employee data, and any other personal information we may process.

3. Definitions

- **Personal Data:** Any information relating to an identified or identifiable natural person (data subject).
 - **Processing:** Any operation or set of operations performed on personal data, whether or not by automated means, such as collection, storage, use, transfer, or deletion.
 - **Data Subject:** An individual whose personal data is being processed by Admicity.
 - **Data Controller:** Admicity, as it determines the purpose and means of processing personal data.
 - **Data Processor:** Any third-party processing personal data on behalf of Admicity.
-

4. Principles of GDPR Compliance

Admicity is committed to the following principles as outlined in the GDPR:

- **Lawfulness, Fairness, and Transparency:** We process personal data lawfully, fairly, and in a transparent manner.
- **Purpose Limitation:** We collect data only for specified, explicit, and legitimate purposes and do not process it in a manner incompatible with those purposes.
- **Data Minimization:** Personal data we collect is adequate, relevant, and limited to what is necessary for processing purposes.
- **Accuracy:** We take reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date.
- **Storage Limitation:** Personal data is retained only for as long as necessary to fulfil the purposes for which it was collected.
- **Integrity and Confidentiality:** We ensure appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

5. Lawful Bases for Processing

Admicity processes personal data only when a lawful basis for doing so exists, such as:

- **Consent:** The data subject has given clear consent for processing their personal data for specific purposes.
- **Contractual Necessity:** Processing is necessary for the performance of a contract to which the data subject is a party.
- **Legal Obligation:** Processing is necessary for compliance with a legal obligation to which Admicity is subject.
- **Legitimate Interests:** Processing is necessary for the legitimate interests pursued by Admicity, provided that such interests are not overridden by the data subject's rights and interests.

6. Rights of Data Subjects

Data subjects have the following rights under GDPR, and Admicity will ensure that these rights are respected:

- **Right to Access:** Individuals have the right to access their personal data and obtain information on how it is processed.
- **Right to Rectification:** Individuals can request that inaccurate or incomplete data be corrected.
- **Right to Erasure ("Right to be Forgotten"):** Data subjects can request the deletion of personal data when it is no longer necessary for the purposes for which it was collected.
- **Right to Restrict Processing:** Individuals can request a restriction on the processing of their personal data.
- **Right to Data Portability:** Individuals can request that their personal data be provided in a structured, commonly used, and machine-readable format.
- **Right to Object:** Individuals have the right to object to the processing of their personal data on grounds relating to their particular situation.
- **Right to Withdraw Consent:** Where consent is the basis for processing, individuals have the right to withdraw it at any time.

7. Data Breach Notification

In the event of a personal data breach, Admicity will notify the relevant supervisory authority within 72 hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. If the breach poses a high risk, affected individuals will also be informed without undue delay.

8. Data Protection by Design and Default

Admicity adopts a privacy-first approach in all systems and processes, ensuring that data protection is embedded into the design of our technology and operational practices. This includes applying appropriate technical and organizational measures to ensure that only necessary personal data is processed for each specific purpose.

9. Third-Party Data Processors

Admicity only engages third-party data processors that can demonstrate their own compliance with GDPR. Data processing agreements are in place with all third-party processors to ensure they act in accordance with our instructions and the provisions of GDPR.

10. Data Retention

Admicity retains personal data only for as long as it is necessary to fulfil the purposes for which it was collected, or as required by law. Once data is no longer needed, it will be securely deleted or anonymized in accordance with our data retention policy.

11. Data Transfers

Where Admicity transfers personal data outside the European Economic Area (EEA), we ensure that such transfers are in compliance with GDPR and are made to countries or organizations that provide an adequate level of data protection. This includes implementing safeguards such as Standard Contractual Clauses (SCCs) or ensuring that the recipient organization is certified under recognized frameworks like the EU-U.S. Data Privacy Framework.

12. Data Protection Officer (DPO)

Admicity has appointed a Data Protection Officer (DPO) to oversee GDPR compliance. The DPO is responsible for:

- Monitoring the Company's data protection strategy and its implementation.
- Conducting audits and providing advice on data protection impact assessments.
- Serving as the contact point for individuals and supervisory authorities.

For any GDPR-related inquiries or requests, data subjects may contact our DPO at:

- **Email:** steve@admicity.co.uk

13. Training and Awareness

Admicity ensures that all employees, contractors, and third parties handling personal data are fully trained on GDPR compliance. Regular training sessions and awareness programs are conducted to ensure ongoing compliance with data protection obligations.

14. Policy Updates

This GDPR Compliance Policy is reviewed and updated annually, or as required, to reflect changes in our data processing practices or updates in data protection regulations. Any significant changes will be communicated to data subjects and stakeholders as necessary.

15. Compliance Monitoring and Audits

Admicity regularly conducts internal and external audits to ensure that data protection measures are in place and GDPR compliance is maintained. Any non-compliance issues will be addressed promptly to mitigate risks and ensure adherence to the law.

16. Contact Information

For any questions or concerns regarding this policy or our GDPR compliance, please contact:

- **Email:** steve@admicity.co.uk
- **Address:** The Tower, Ray Mead Road, Maidenhead, England SL6 8NJ

17. Conclusion

Admicity is fully committed to complying with GDPR and ensuring the protection of personal data. We recognize the importance of data privacy and security and strive to maintain the highest standards in safeguarding the personal information entrusted to us.

By adopting this GDPR Compliance Policy, Admicity ensures that we process personal data in a manner that is transparent, secure, and respectful of the rights of individuals.

This policy is effective as of 1st March 2024.