GDPR Compliance, Data Protection and Information Security

Shrey Sports recognises the importance of protecting personal information and is committed to ensuring full compliance with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

We understand that the provision of sportswear and teamwear to universities involves the handling of personal information relating to students, university employees, sports club members, coaches and other authorised representatives. This may include names, contact details, delivery addresses, garment sizes, order histories and individual teamwear requirements.

We apply a risk-based approach to data protection, incorporating appropriate technical, organisational and physical security measures to protect personal information throughout its lifecycle.

1. Data Protection Governance and Accountability

Shrey operates a structured approach to data protection, with responsibility for ensuring that personal information is handled appropriately assigned within the business.

Our approach includes:

- Maintaining appropriate data protection policies and procedures covering the collection, processing, storage, sharing and disposal of personal information.
- Ensuring that employees who handle personal data understand their responsibilities under GDPR.
- Providing appropriate guidance and training to relevant employees on confidentiality, data security and the correct handling of personal information.
- Maintaining appropriate records of data processing activities and the purposes for which personal information is collected and used.
- Reviewing data protection procedures periodically and updating them where necessary to reflect legislative changes, operational requirements and emerging security risks.
- Applying the principles of data protection by design and default, ensuring that only the personal information necessary for a particular business activity is collected and processed.

2. Technical and Information Security Measures

We recognise the importance of protecting personal information against unauthorised access, accidental disclosure, alteration, loss or destruction.

Our security approach incorporates appropriate measures, including:

- Password-protected access to business systems and information.
- Access controls designed to ensure that employees can only access personal information necessary to fulfil their specific responsibilities.
- Secure storage of electronic information within authorised business systems.
- Appropriate protection of computers, mobile devices and other equipment used to access or process personal information.

- Regular software and security updates to help protect against vulnerabilities and cyber security threats.
- Appropriate data backup and recovery arrangements to support the availability and restoration of business information in the event of system failure or disruption.
- Secure disposal of electronic and physical records when they are no longer required.

Where appropriate to the nature and sensitivity of the information, encryption and additional authentication measures are applied to provide further protection.

3. Access Controls and Employee Confidentiality

Access to personal information is restricted to authorised personnel with a legitimate business requirement.

Employees are expected to maintain confidentiality when handling customer, university and individual data. Personal information must not be disclosed to unauthorised parties or used for purposes unrelated to the original business requirement.

Access permissions are reviewed where appropriate, particularly when employees change roles or leave the organisation.

4. Data Subject Rights

Shrey recognises and supports the rights of individuals under UK GDPR.

We have processes in place to respond appropriately to requests from individuals wishing to exercise their data protection rights, including:

- Right of access – individuals can request details of the personal information held about them and obtain a copy.
- Right to rectification – individuals can request that inaccurate or incomplete information is corrected.
- Right to erasure – individuals can request deletion of their personal information where the relevant legal conditions are met.
- Right to restriction – individuals can request that the processing of their personal information is restricted in certain circumstances.
- Right to data portability – individuals can request their personal information in a structured, commonly used and machine-readable format where applicable.
- Right to object – individuals can object to certain types of personal data processing.

Requests will be handled through an appropriate internal process, with the identity of the requester verified where necessary and responses provided within the statutory timescales.

5. Data Retention and Secure Disposal

Personal information is retained only for as long as necessary to fulfil the purpose for which it was collected, taking account of contractual, operational and legal obligations.

Where information is no longer required, it is securely deleted, destroyed or anonymised as appropriate.

We recognise that university-related information, including individual student orders and teamwear records, must not be retained indefinitely without a legitimate business or legal reason.

6. Data Sharing and Third-Party Suppliers

Where personal information needs to be shared with third parties to fulfil contractual requirements, such as delivery partners or other service providers, this is restricted to the information necessary to perform the relevant activity.

We recognise our responsibilities when engaging third-party organisations that process personal information on our behalf. Appropriate contractual arrangements and safeguards will be applied, including requirements relating to confidentiality, security, permitted processing and the protection of personal information.

Personal information will not be sold or disclosed to third parties for unrelated marketing purposes.

7. Personal Data Breaches and Incident Management

Shrey recognises the importance of identifying, reporting and responding promptly to any actual or suspected personal data breach.

Our incident management approach includes:

- Prompt internal reporting and escalation of suspected data breaches.
- Investigation to establish the nature, extent and potential impact of an incident.
- Taking immediate steps to contain the incident and prevent further unauthorised access or disclosure.
- Assessing the risks to affected individuals and identifying appropriate remedial action.
- Maintaining an appropriate record of incidents and the actions taken.
- Notifying the university without undue delay where an incident involves personal data processed on its behalf.
- Supporting the university with any investigation, regulatory reporting or communication with affected individuals where required.

Where Shrey acts as a data processor, we will support the university in meeting its statutory reporting obligations.

8. Contract-Specific Data Protection Arrangements

For the duration of the university contract, Shrey will work collaboratively with the university to ensure that all personal information processed as part of the sportswear provision is handled in accordance with agreed data protection requirements.

This will include:

- Agreeing the respective data protection responsibilities of Shrey and the university.
- Entering into an appropriate Data Processing Agreement where required.
- Ensuring that personal information is only processed for authorised contractual purposes.
- Applying appropriate access restrictions and security measures to university-related information.
- Supporting the university with requests from data subjects and any relevant compliance or audit requirements.
- Ensuring that personal information is securely returned, deleted or retained in accordance with agreed contractual and legal requirements at the end of the contract.

Conclusion

Shrey Sports is committed to maintaining appropriate technical, organisational and administrative safeguards to protect personal information and uphold the rights of data subjects.

We recognise that data protection is an ongoing responsibility rather than a one-off exercise. Our procedures will continue to be reviewed and developed throughout the contract to ensure that personal information entrusted to us by the university, its students and its staff is handled securely, responsibly and in full accordance with applicable data protection legislation.

Acton London, W3 6AY
+44 7488703678
matt.cooke@shreysports.co.uk
shreysports.co.uk
info@kohlisports.com