

GDPR Compliance Statement

Introduction

The **EU General Data Protection Regulation (“GDPR”)** came into force across the European Union on 25th May 2018 and brings with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

The 21st Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardize data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

Our Commitment

MarchingOrder (“we”, “us”, or “our”) is committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the UK’s Data Protection Bill.

We are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

Legal Basis for Processing Personal Data

The lawful base for MarchingOrder to process data resides in article 6(1)(f): “processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”

To demonstrate our legal basis for processing personal data, we employ the 3-part test as outlined in the Rigas case (<https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1515682033041&uri=CELEX:62016CJ0013>):

Balancing test – is the legitimate interest overridden by the individual’s interests, rights or freedoms?

- **Purpose Test** – is there a legitimate interest behind the processing?

- MarchingOrder receives data in two ways: directly from an institution, or directly from the data subject with the express permission of an educational institution.
- MarchingOrder collects this data to perform contractual obligations with those institutions e.g. displaying a graduate's name on-screen at a ceremony, collecting ticket orders for an institutional event like graduation, etc.
- **Necessity Test** – is the processing necessary for that purpose?
 - Without processing this data, MarchingOrder would not be able to perform core business functions
 - Without processing this data, MarchingOrder would not be able fulfill contractual obligations with client educational institutions
- **Balancing Test** – is the legitimate interest overridden by the individual's interests, rights or freedoms?
 - While we are contracted with educational institutions, our legitimate interest is also aligned with the legitimate interest of the data subject. The data subjects use MarchingOrder to confirm the name that shows on screen at a graduation ceremony, order and send tickets to their guests, provide notes for phonetic pronunciation, etc.
 - All information collected is used in a way that may be “reasonably expected” by the data user. How MarchingOrder uses that information is also stated as “for graduation ceremony purposes only.” MarchingOrder does not engage in marketing activities or the sale of personal information. Following a graduation ceremony, that information is not processed for any purpose.
 - Information collected does not qualify as “Special Category Data”
 - Data subjects may contact the school or MarchingOrder to be fully erased from the MarchingOrder website.
 - Our retention policy and schedule to ensure that we meet the ‘*data minimization*’ and ‘*storage limitation*’ principles and that personal information is stored, archived and destroyed compliantly and ethically.

Information Security & Technical and Organizational Measures

MarchingOrder takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorized access, alteration, disclosure or destruction and have several layers of security measures, including: -

- Our cloud hosts have a MAD system that protects the server, in addition to IP filtering, firewalls, port closing, and logging
- Our cloud server runs vulnerability scans, penetration tests, and anti-malware software
- All site users must be authenticated by password or SSO; additionally, all users are added to our site directly by our clients (educational institutions)
- We use SSL/HTTPS for connections to the site



MarchingOrder
303 West Joaquin Ave, Suite 230
San Leandro, CA 94577
+001 888-988-0346
info@marchingorder.com
www.marchingorder.com

- We use an HMAC SHA-256 hashing algorithm with a SSK to ensure connections are coming from trusted sources
- The server is backed up regularly to an image if needed; these backups are periodically purged
- Our office is not accessible to unauthorized personnel
- Data is locally encrypted with TDE via SQL Server
- Our contract workers are bound by confidentiality agreements which include FERPA compliant language
- We are FERPA and GDPR compliant, and our staff is well-versed in the importance of both

Questions

If you have any questions about our preparation for the GDPR, please contact Tyler Mullins.