criticalmix

GDPR Compliance

WHAT IS THE GDPR?

The EU General Data Protection Regulation ('GDPR') is effective across the European Union on 25th May 2018. The broader use of technology, new definitions of what represents personal data, and a vast increase in cross-border processing have required a new Regulation to standardise data protection laws and processing across the EU. The GDPR was designed to give individuals stronger, more consistent rights to access and control their personal information.

OUR COMMITMENT

Critical Mix is committed to ensuring the security and protection of the personal information that we collect and process, and to provide a compliant and consistent approach to data protection. We are dedicated to safeguarding the personal information under our remit and to 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.

CRITICAL MIX COMPLIANCE

Critical Mix already has a consistent level of data protection and security across our organisation and we have taken the following steps to be fully compliant with the GDPR.

INFORMATION AUDIT

A company-wide information audit was conducted to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.

POLICIES & PROCEDURES

Data protection policies and procedures have been implemented to meet the requirements and standards of the GDPR and any relevant data protection laws, including:

Data Protection – Our main policy and procedure document for data protection meets the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities, with a dedicated focus on privacy by design and the rights of individuals.

Data Retention & Erasure – The Critical Mix retention policy and schedule ensures that we meet the 'data minimisation' and 'storage limitation' principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new 'Right to Erasure' obligation and are aware of when this and other data subject rights apply, along with any exemptions, response timeframes and notification responsibilities.

Data Breaches – Our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.

International Data Transfers & Third-Party Disclosures – Where Critical Mix stores or transfers personal information outside the EU, we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. Our procedures include a continual review of the countries with sufficient adequacy decisions, and standard data protection clauses or approved codes of conduct for those countries without standards. We carry out due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.

Subject Access Request (SAR) –SAR procedures are in place to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.

CRITICAL MIX COMPLIANCE

PRIVACY NOTICE/POLICY

Our Privacy Notices comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.

OBTAINING CONSENT

Consent mechanisms have been implemented among our survey members by obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records, and a way to withdraw consent at any time that is easy to see and access.

DIRECT MARKETING

Wording and processes for direct marketing will include clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and unsubscribe features on all subsequent marketing materials will be provided.

DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

Where we process personal information that is considered high risk, involves large-scale processing or includes special category/criminal conviction data, we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

PROCESSOR AGREEMENTS

In situations where we use any third party to process personal information on our behalf (e.g. Payroll, Recruitment, Hosting), Critical Mix has entered into compliant Processor Agreements and due diligence procedures for ensuring that they (as well as we) meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.

SPECIAL CATEGORIES DATA

When we obtain and process any special category information, we will do so in compliance with the Article 9 requirements and will have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit with the right to modify or remove consent being clearly signposted.

SURVEY MEMBER RIGHTS

In addition to the policies and procedures mentioned above, we provide easy access to information via our website of an individual's right to access any personal information that we collect and process about them, including...

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store their personal data for
- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

INFORMATION SECURITY AND TECHNICAL & ORGANISATIONAL MEASURES

Critical Mix takes the privacy and security of individuals and their personal information very seriously, and we 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 unauthorised access, alteration, disclosure or destruction.

GDPR ROLES & EMPLOYEES

Critical Mix has designated Jonathan A. Flatow as our Data Protection Officer, and we have appointed a data privacy team to develop and implement our roadmap for complying with the GDPR. The team is responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.

If you have any questions about our preparation for the GDPR, please contact Jonathan A. Flatow, 53 Riverside Avenue, Westport, CT 203-521-7833 or privacy@criticalmix.com

Effective Date: May 23, 2018

criticalmix

criticalmix.com

CALL 0808-189-2040

YOU CAN REACH US ANYTIME – WHENEVER YOU NEED US.