GDPR Statement/ Policy

Introduction

The *EU General Data Protection Regulation ("GDPR")* will be in force across the European Union from 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 standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control of their personal information.

Our Commitment

Krusha Patel Coaching 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 continue to engage with our legal team to fulfil these demands.

Krusha Patel Coaching is 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.

How We are Preparing for the GDPR

Krusha Patel Coaching already have a consistent level of data protection and security in place; however, it is our aim to be fully compliant with the GDPR and maintain this position. *Our preparation includes:* –

- *Information Audit*– carrying out a business-wide information audit 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***–** updating data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including: –
    - *Data Protection*– our main policy and procedure documents for data protection is being revised by our legal advisors in order to meet the

standards and requirements of the GDPR. Accountability and governance measures are being put 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*– we are updating our retention policy and schedule to ensure that we meet the *'data administration'* and *'storage limitation'* principles and that personal information is stored, archived and destroyed compliantly and ethically. We will have dedicated erasure procedures in place to meet the new *'Right to Erasure'* obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
  - *Data Breaches*– our breach procedures will 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 will be robust and will be disseminated to all colleagues and consultants, making them aware of the reporting lines and steps to follow.
  - *Third-Party Disclosures*– we are carrying out strict 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)*– we are revising our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures will detail how to verify the data subject, what steps to take for processing an access request and what exemptions apply.

- *Legal Basis for Processing*– we are reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.
- *Privacy Notices* – we are revising our existing Privacy Notices and introducing new notices to comply with the GDPR. We will ensure 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*– we are reviewing our consent requirements and mechanisms for 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 clear and readily accessible way to withdraw consent at any time.
- *Direct Marketing*– we are revising the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions for

non-Corporate organisations; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.

- *Data Protection Impact Assessments (DPIA)*– where we process personal information that is considered high risk, involves large scale processing or includes special category information, we are developing stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. Documentation processes will be implemented 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*– where we use any third-party to process personal information on our behalf (*g. psychometric assessments etc.*), we are drafting 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***–** if we obtain and process any special category information, we will do so in complete compliance with the Article 9 requirements and will have high-level encryptions and protections on all such data. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we intend to provide information via our website of an individual's right to access any personal information that Krusha Patel Coaching processes about them and to request information about: –

- 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 your personal data for
- If we did not collect the data directly, information about the source
- The right to have incomplete or inaccurate data 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
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

Information Security, Technical and Organisational Measures

Krusha Patel Coaching takes the privacy and security of individuals and their personal information very seriously and we intend to 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 and have several layers of security measures to ensure this.

GDPR Roles and Employees

Krusha Patel has been appointed as our Data Privacy Manager and any related queries can be directed to her in the first instance at **info.krusha@mail.com**

Krusha Patel Coaching understands that colleague awareness and understanding is vital to the continued compliance of the GDPR. To this end we will introduce comprehensive guidance notes and make GDPR training available to all employees, associates and consultants, and it will also form part of our induction and development programmes.