Pureprofile

GDPR

COMPLIANCE DOCUMENT

Last updated May 2018

Introduction

The General Data Protection Regulation (***GDPR***) is a regulation under European Union (***EU***) law relating to data protection and privacy for all individuals within the EU. It was adopted on 14 April 2016 and will come into effect on 25 May 2018, replacing the 1995 Data Protection Directive.

The GDPR standardises data protection laws across the EU member states, and requires businesses to take measures to protect the personal information and privacy of individuals. The GDPR also regulates the transfer of personal information outside the EU.

The Pureprofile Group conducts business which includes services that involve handling personal information and is therefore affected by the GDPR.

This document sets out measures that Pureprofile is taking to protect personal information and ensure compliance with the GDPR. These measures apply to all brands within the Pureprofile Group, including Pureprofile, Sparcmedia, AdSparc and Cohort Digital.

Privacy by Design

The concept of privacy by design incorporates the principles of data protection at the outset of designing systems. Pureprofile adopts this approach in all current and future innovations to its systems and products.

Data Privacy Officer

Pureprofile has appointed a Data Privacy Officer (***DPO***) to monitor its compliance with the GDPR and serve as the contact point with relevant authorities. The DPO's role is to provide the knowledge, expertise, day-to-day commitment and independence to properly advise the company of its duties, and conduct compliance activities in relation to the GDPR.

Organisation-wide Compliance

The company has also established a working group, drawing on stakeholders from across the business, to take responsibility for the day-to-day management of the company's GDPR compliance programme.

Pureprofile will hold regular training programmes for personnel at all levels, including directors, heads of departments and key company service providers.

Consent

The GDPR's approach to privacy and consent means individuals understand what information they are providing and the purposes for which that information will be used.

Pureprofile has reviewed existing procedures in relation to obtaining an individual's consent as a legal basis for processing personal data. For example, we ensure that any consent obtained indicates affirmative agreement from the individual (opt in) rather than mere acquiescence (for example, failing to untick a pre-ticked box).

Furthermore, Pureprofile has implemented processes to ensure that an individual can easily withdraw their consent at any time.

Right to Access

Pureprofile has processes in place which will allow an individual to request what information the company has on them. Individuals shall have a further right to ask the company whether it is processing personal information in relation to them, for what purpose and where.

Right to be Forgotten

In line with the GDPR, Pureprofile has adopted the position that if an individual withdraws their consent from processing their personal information (for example by closing their Pureprofile account), or where the information is no longer relevant to the purposes for which it was collected, Pureprofile will delete the data and ensure that it is no longer available for further dissemination. As far as practicable, Pureprofile will halt processing of data by third parties.

Database Security

Pureprofile's cloud infrastructure provider is Amazon Web Services. AWS provides several security capabilities and services to increase privacy and control network access. These include: network firewalls and web application firewalls (WAFs), encryption in transit with TLS across all services and DDoS mitigation options. Databases are encrypted using the industry standard AES-256 encryption algorithm to encrypt data on the server (data at rest). These databases are not directly accessible by the public internet, but only from Pureprofile's applications that reside within the same virtual private cloud (VPC).

Data Breach Response and Notification

Pureprofile has adopted a data breach response plan, which deals with the identification of data breaches (or suspected data breaches) relating to personal information. The plan outlines processes for containing the breach; evaluating the risks associated with the breach; notification of the breach; and taking measures to prevent future breach.

Ongoing Review

Pureprofile recognises that compliance with the GDPR, and processes to facilitate protection of an individual's personal information and privacy, is an ongoing process. From time to time, the company will review and update its processes in light of new laws and business activities, and changes to data flows and the introduction of new processing activities.

Pureprofile

Thank you

www.pureprofile.com

Contact: business.pureprofile.com/contact