AMO Consultancy

Tailor-made applications to do exactly what you want, exactly how you imagined it.

GDPR Compliance Statement

Last updated 04/06/2024

1 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 standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

2 Our commitment

AMO Consultancy 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.

AMO Consultancy 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.

3 Our Operations with GDPR

AMO Consultancy adhere to a uniform standard of data protection and security throughout our organisation in accordance with GDPR policies as detailed in the different aspects below.

3.1 Continuous Information Audit

Carrying out a company-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. This is captured in the departmental Sensitive Data Transactions Log.

3.2 Data Policies & Procedures

3.2.1 Data Protection

We have revised our data protection policy to comply with GDPR standards. Accountability and governance measures are in place to ensure we understand, disseminate, and evidence our obligations and responsibilities.

3.2.2 Data Retention & Erasure

Our retention policy and schedule are under review to align with the principles of 'data minimisation' and 'storage limitation'. We have procedures for compliant and ethical storage, archiving, and destruction of personal information. We also understand when data subject rights, such as erasure, apply, including exemptions, response times, and notification duties.

3.2.3 Data Breaches

Our breach procedures are designed to quickly identify, assess, investigate, and report personal data breaches in line with ICO guidance.

3.2.4 International Data Transfers & Third-Party Disclosures

AMO Consultancy does not transfer personal data outside the EU. For UK-based and EU-based operations, we have strong procedures to secure, encrypt, and maintain data integrity. We conduct strict due diligence on all personal data recipients to ensure they have appropriate safeguards, enforceable data subject rights, and effective legal remedies.

3.2.5 Data Subject Access Request (SAR)

Employees can access their personal data, including personnel files, sickness records, disciplinary records, training records, appraisal notes, relevant emails, and other related documents. We comply with the revised 30-day timeframe for SAR responses and understand when we can extend the response time. We also consider the implications when requests involve information about others.

3.2.6 Data Protection Impact Assessments (DPIA)

For high-risk processing, large-scale processing, or special category/criminal conviction data, we have updated our documentation to record each assessment, rate the risks, and implement measures to mitigate those risks.

3.3 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. See below for a summary of processing activities:

3.3.1 Data Collection

Collecting personal data on behalf of your clients from various sources such as online forms, customer databases, or third-party providers.

3.3.2 Data Storage

Storing personal data in physical or digital formats, ensuring appropriate security measures are in place to protect the data.

3.3.3 Data Analysis

Analysing personal data to generate insights, reports, or for purposes specified by the data controller.

3.3.4 Data Transmission

Transmitting personal data between different systems or locations, ensuring secure transfer methods are used.

3.3.5 Data Hosting

Hosting data on servers or in the cloud, maintaining infrastructure that allows for data access, storage, and management.

3.3.6 Data Retrieval

Retrieving personal data as requested by the data controller, ensuring it can be accessed promptly and securely.

3.3.7 Data Backup

Creating and maintaining backups of personal data to prevent data loss and ensure data recovery in case of system failures or breaches.

3.3.8 Data Deletion/Erasure

Deleting or erasing personal data upon request or when it is no longer needed, ensuring compliance with data retention policies and regulatory requirements.

3.3.9 Access Control Management

Managing access to personal data, ensuring that only authorized personnel have access in accordance with data controller instructions.

3.3.10 Data Encryption

Encrypting personal data both in transit and at rest to protect it from unauthorized access and breaches.

3.3.11 Incident Response and Reporting

Monitoring for data breaches or security incidents and reporting them to the data controller and relevant authorities as required by GDPR.

3.3.12 Data Subject Request Handling

Assisting the data controller in handling data subject requests such as access, rectification, and deletion requests.

3.3.13 Compliance Monitoring

Monitoring processing activities to ensure they are in compliance with GDPR and ISO 27701 requirements and conducting regular audits.

3.3.14 Contract Management

Managing contracts with data controllers to ensure that data processing agreements reflect GDPR and ISO 27701 requirements.

3.4 Privacy Notice/Policy

We are updating our Privacy Notice(s) to comply with GDPR, ensuring individuals are informed about why we need their personal data, how it is used, their rights, disclosure details, and safeguarding measures.

3.5 Obtaining Consent

Our consent mechanisms have been revised to ensure individuals understand what data they provide, its use, and how they can consent. We have established processes for recording consent, including time and date stamps, and easy methods for withdrawing consent at any time.

3.6 Direct Marketing

AMO Consultancy does not engage in direct marketing. If we do in the future, we will include clear opt-in mechanisms, opt-out methods, and unsubscribe features on all marketing materials.

3.7 Data Protection Impact Assessments (DPIA)

For high-risk processing, large-scale processing, or special category/criminal conviction data, we have updated our documentation to record each assessment, rate the risks, and implement measures to mitigate those risks.

3.8 Third-Party PII Updates

We notify third parties of any modifications, withdrawals, or objections related to shared personal information within seven days and have implemented policies and procedures to manage these updates.

3.9 Processor Agreements

When using third parties to process personal data (e.g., payroll, recruitment, hosting), we ensure all parties comply with GDPR and align with AMO Consultancy's commitment. This includes regular reviews of their services, processing necessity, technical and organizational measures, and GDPR compliance.

3.10 Special Categories Data

We only process special category data when necessary and have identified the appropriate legal basis under Article 9(2) or the Data Protection Bill Schedule 1 condition. Consent for processing this data is explicit, verified by a signature, and includes clear instructions for modifying or withdrawing consent.

4 Comprehensive Data Protection and Breach Response Policy

AMO Consultancy takes the privacy and security of individuals and their personal information very seriously and takes 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.

We recognize the importance of identifying personal data breaches, understanding that they encompass more than just the loss or theft of data. To address any breaches that may occur, we have developed a comprehensive response plan and assigned a dedicated team to manage such incidents. Our staff are trained to escalate security incidents to the appropriate team to determine if a breach has occurred and to assess the potential risks to individuals.

In the event of a breach posing a high risk to the rights and freedoms of individuals, we are committed to informing those affected directly and without undue delay, aiming to do so within 24 hours of the breach being noticed. We understand our obligation to inform affected individuals promptly and know the relevant supervisory authority for our processing activities.

We have established a process to notify the Information Commissioner's Office (ICO) of a breach within 72 hours of becoming aware of it, even if all details are not yet available. We are knowledgeable about the information required to be provided to the ICO and to individuals affected by a breach, including offering advice to help them protect themselves from its consequences.

Additionally, we document all breaches, regardless of whether they need to be reported, ensuring comprehensive records of all incidents.

5 GDPR Roles and Employees

At AMO Consultancy, Bertrand Piquet, the Managing Director, has been appointed as the ISPMS Manager, encompassing the roles of Information Security Officer (ISO), Data Protection Officer (DPO), and Information Security Champion. Along with Amanda Moumen and other senior management, Bertrand Piquet is a member of the ISPMS Committee, which is tasked with developing and implementing our roadmap for GDPR compliance. This committee is responsible for promoting GDPR awareness, assessing our readiness, identifying gaps, and implementing necessary policies, procedures, and measures.

We recognize the importance of continuous employee awareness and understanding for maintaining GDPR compliance. To this end, we have engaged our employees in our preparation plans and implemented a comprehensive training program. This program, which is provided during induction and as part of our annual training, ensures that all employees are well-informed and equipped to adhere to GDPR requirements.