AcoBloom International

AcoBloom International & the General Data Protection Regulation (**GDPR**)

General Data Protection Regulation

Introduction

The General data protection regulation (GDPR) got operationalised on May 25th, 2018. The regulation deals with data protection and privacy of Individual data subjects.

The regulation puts the onus of data protection and privacy on the data controller who has to ensure that data processor follows GDPR guidelines to remain compliant towards GDPR, enabling protection of personal data of Individuals (Data Subjects) residing in European Union (EU) and United Kingdom, irrespective of the fact wherever such data is processed.

United Kingdom based on the principals of GDPR, is enacting its new legislation of data protection bill. The UK's third generation of data protection law has entered its Parliament. The Data Protection Bill was published on 14 September 2017 and aims to

modernise data protection laws to ensure they are effective in the years to come.

India also, in a recent judgment of the Hon'ble Supreme Court declared the right to privacy as a fundamental right and has provided much-needed push for introducing a robust and comprehensive data protection legislation in India.

Key Responsibilities

AcoBloom International's clients generally are data controllers or data processors, while AcoBloom acts as a data processor or data sub processor.

The data controller determines the legal means and purpose of processing of personal data of the data subject, while data processor processes the personal data on behalf of data controller or where we are data sub-processor, we process data on behalf of data processor.

Although, as per GDPR regulations Data controllers are primarily responsible for GDPR compliance, but we as data processor or data sub-processor consider ourselves as equally responsible for implementing organizational and security policies enabling privacy by design and default, demonstrating that data processing at our end are in compliance with GDPR.

Actions taken by AcoBloom International towards GDPR compliance

How we have prepared ourselves for GDPR?

- We have researched and familiarized ourselves with GDPR, which includes legal interpretation and our board of directors' firm resolution to be GDPR compliant
- At the time of transition of any process from our client, we have put in a process of identification of personal data of data subject with data controller or data Processor. The identified personal data is documented in Data Protection Impact documentation (DPID). Our Data Protection Impact documentation enables our clients i.e. Data Controller / Data Processor to be GDPR compliant.

- Our Director is a certified information system auditor and a gold member of Information Systems Audit and Control Association (ISACA), which is world's premier body of international information technology professionals focusing on IT governance. Under his leadership, we have accordingly implemented best practices in the area of IT governance and data security.
- We have not experienced a single incident of data breach and we are very confident that we shall never experience such incident, but in order for Data controllers to comply with GDPR, we have formulated a data breach response plan, and would be activated in case of any eventuality.

- We have reviewed our current policies, internal controls and standard operating procedures to make sure they are in Sync with framework of GDPR
- We have ensured all our software vendors and communication technology vendors are aware of GDPR
- We are closely monitoring any change in GDPR regulatory environment and specific country wise guidance as and when made available and would accordingly carry out any changes in compliance strategy if required.

AcoBloom International overall GDPR Compliance Methodology

1. **We have formulated a data protection and privacy governance frame work which revolves around:**
   - Maintaining Data Governance
   - Best practices around acquiring, identifying and classifying personal data
   - Managing personal data risk
   - Managing personal data security
   - Managing incident and breaches
   - Create and Maintain GDPR awareness
   - Maintaining Internal controls

GDPR COMPLIANCE METHODOLOGY

1. Structured Data Governance
2. Data Protection Impact Documentation(DPID)
3. Personal Data Inventory in DPID
4. Processing Register in form of SOP
5. Sharing of SOP with Clients
6. Contractual processing agreement
7. GDPR Compliant Technology
   a. Data Storage
   b. Processing & Reporting Softwares
8. Regular Trainings of Employees
9. Data Return & Deletion
10. Data Breach Notification
11. Right To Audit
12. Other Data Security Measures

2. **Data Protection impact documentation**

Before beginning with any processing or sub processing assignments, we carry out a data protection impact documentation (DPID), which includes identification of data "universe" related to our process; the steps in our DPID include identification of data subjects, category of data, purpose of processing , egal basis, Data flows identification and quantification of absolute risk, measures of mitigation of risk and assessment of residual risk and proportionality.

3. **Personal Data register or Inventory**

DPID, contains personal data registry or inventory. Personal data used in processing is also documented as a part of our contract, further it is periodically updated, monitored and acts as a GDPR compliance record for data controller/ data processor. We encourage masking of personal data not required for processing.

4. **Processing register**

After creation of Personal data registry a document in form of standard operating procedure (SOP)for various processing activities is formulated and documented as a part of our contract. SOP is periodically updated, monitored

and acts as a GDPR compliance record for data controller/ data processor.

5. Contractual

Our Agreements entered into with clients fully reflect our commitments towards privacy and confidentiality of clients data as data controller or data processors, enabling compliance with GDPR, further we specifically formulate a standard operating procedure (SOP) ensuring processing of data is in agreement with the client. The SOP becomes part of our main global services agreement...We also enter into a separate GDPR framework agreement for Data processing or Data sub-processing. Since the processing is done in a jurisdiction which is not in Europe and is in India, we can provide adequate safe guards in our contracts to maintain a mechanism that facilitates compliance with GDPR by our European and UK clients.

6. Technology and GDPR

i. Data storage Technology and GDPR

We store the raw (unprocessed data) and Final reports (Processed data) in following forms

a. Client Data Server

We encourage the use of client's own data server, which is remotely accessed through high speed Internet using a Secured VPNIPSEC tunnel by our processors sitting on a secured client in India, in this methodology the data is not transferred to our local machines and the unprocessed data and final reports as per the agreed SOP is processed using secured remote desktop application, with no copy paste rights. The deliverables are stored in the data server provided by client after processing.

b. *Secured Data Server in UK*

In case client himself does not have a secured server, to serve such clients we are in a contract with a third party data center vendor having its data center in United Kingdom and providing a private cloud which is fully compliant with GDPR. We and the client work on licensing methodology, which is remotely accessed through high speed Internet over a secured VPN (IPSEC) tunnel by our processors sitting in India, in this methodology the data is not transferred to our local machines and the unprocessed data and final reports as per the agreed SOP is processed using a secured remote desktop protocol technology (RDP) and deliverables are stored in the GDPR compliant private cloud in United Kingdom. The credentials of data center in UK providing GDPR compliant private cloud can be shared on request.

The storage of raw and processed data in above mentioned data server in UK is based on a Secure Platforms ensuring all data is encrypted in transit and at rest and, where appropriate, is securely backed up or replicated. The data stored is backed up in real time basis in a GDPR compliant environment.

ii. Processing and reporting software

In the field of accountancy we are required to use numerous processing and reporting software, as a data processor or data sub-processor, we ensure that the software used by us are secured and GDPR compliant. Some of the software which we use and have publicly reported their GDPR compliance are:

- **XERO**
- **Quick Books**
- **IRIS**

- **SAGE**

iii. Communication technology and GDPR

We use secured, Skype for business to ensure secured and authorized oral communication with the client. For emails we use GDPR compliant G-Suite based on authorized external and internal communication. The access to G-Suite is allowed only on the basis of two factor authentication i.e. two step verification process.

7. Staff training and compliance

Our Board of director's, fully support and understand the measures taken by our company to be GDPR enabled ensuring our clients i.e. Data controllers or where ever data processors to be GDPR compliant.

Our resources are highly aware of GDPR and regularly trained in various data security measures and GDPR requirements ensuring compliance. In fact all our

employees are required to sign a confidentiality agreement mandatorily.

8. Data return and Deletion

We have a very robust policy of Data return and deletion. We have incorporated standard clauses in our data processing agreements regarding Data return and deletion. Data controllers or where data processors are our client have full access to their raw and processed data 24X7, and have full right to delete, stop the processing or extract the data from secured private cloud/

clients own data server to remain compliant in terms of Data Subject rights of access, rectification, restrict the processing of, or delete any data that they have put into secured private cloud or data server.

The clients also have choice of sending a complete deletion instruction; we will delete the relevant client data within a maximum period of 90 days.

9. Data Breach notification

We provide contractual commitments through our data processing agreements around incident notification. In case of any incident, we will promptly inform our clients of incidents involving any data breach in line with the data incident regulations of GDPR. We have put in a process where our staff has been trained to report any data breach, enabling us further to intimate the data controller or wherever data processor is our client with specified timelines.

10. Right to Audit

As required by GDPR and as a best practice, we shall give our clients i.e. data controllers or wherever data processor is our client, contractual right to audit in context with our compliance with GDPR

11. Other data Security measures

We continue to have various data security measures including access controls, physical controls, network security, firewalls and vulnerability management etc, for details of our robust data security measures please visit data security page of our website www.acobloom.com/data-security-gdpr

Physical Security:

- Biometric entry to the premises is restricted through finger punch in.
- The office building is secured with manned security guards.
- Procedure in place to distinguish onsite personnel and visitor, by assigning ID badges.
- Video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas.
- Physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.
- Fire security and alarm system consisting of smoke and heat detectors, sensors. Fire-fighting equipment is also installed.
- The facility is also manned with security staff.
- Surprise audits are carried out to ensure security policies are followed. Non-Compliance with the same leads to disciplinary action.
- Physical access for onsite personnel to the sensitive areas is controlled. Access is authorizedbased on individual job function; access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc. are returned or disabled.

Network Security:

- A firewall is placed for a perimeter security of the network that restricts all traffic, inbound and outbound, from a "non-trusted" networks and hosts, and specifically deny all traffic except for protocols required for the environment.
- Direct public access between the internet and any system component is prohibited using security controls.
- VPN (IPsec) tunnel is commissioned for any site to site connectivity with client or any external data source.
- A vulnerability management program is in place for the whole organisation.
- Every employee has its unique username and password (complex password) to access his/her workstation.
- Electronic Devices such as mobile phones, PDA etc. are not allowed on the production floor, the USB ports and other media drives are disabled.
- Continuous monitoring of the web traffic and disciplinary actions are taken for any violations.
- Access to the local drives of our server is restricted based on the process the employee is assigned to.

- An effective backup and restore mechanism is in place to prevent data loss (In case clients use our cloud server).
- An automatic update of patches and anti-virus is in place.
- Multi-factor access to emails

Confidentiality:

- After having gone through the rigorous interview process, our candidates are screened thoroughly and get their backgrounds check (BGV) done through our tied up third parties vendor.
- Since employee base is the only authorized pool of people who have utmost responsibility to keep your data secure, all our candidates sign a confidentiality agreement with us besides explaining to them verbally the importance of confidentiality and data security.
- Restricted access to internet websites through content filter and the same is allowed only if it is a process requirement.

Our Commitment

We are more than 100% committed to GDPR compliance, as we believe, and law also mandates that the right to privacy is a fundamental right of a data subject. Our commitment towards GDPR compliance is across all our services to our European and UK clients, also we are equally committed in helping our clients i.e. Data Controllers to be GDPR compliant through our compliant organizational and data privacy policies including our contractual commitment with clients towards data privacy and protection.

Key terms in GDPR

-What is personal data and data subject?

Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

-What is processing?

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

-Who is data controller?

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

-Who is Data Processor?

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.