MyGoldCloud GDPR Compliance

Frequently Asked Questions

- Assessment
- Data Protection Policies
- Training and awareness
- Controls implemented to reduce and monitor risk
- Monitoring Compliance
- Reporting
- Annual Review Process

ASSESSMENT

1. **What does the MyGoldCloud service provide?**

   MyGoldCloud delivers cloud-based CRM and business applications to organisations based in the UK & EU. MyGoldCloud extends beyond sales, marketing and customer support to include bespoke data management tools from within our secure cloud.

   MyGoldCloud joins up the entire organisation around data and processes, promoting teamwork and collaboration. It provides a single 360° view of customers and the information is accessible anytime, anywhere.

2. **What personal data is held within a typical MyGoldCloud customer environment?**

   Subject to Section 8 of our Data Processing Agreement we will process personal data, the extent of which is determined and controlled by your (the Customer) at your sole discretion and which may include, but is not limited to, personal data relating to the following categories of data subjects:

   - Prospects, customers, business partners and vendors of Customer (who are natural persons)
   - Employees or contact persons of Customer's prospects, customers, business partners and vendors
   - Employees, agents, advisors, freelancers of Customer (who are natural persons)
   - Customer's Users authorised by Customer to use the Services

You may submit Personal Data to the MyGoldCloud Services the extent of which is determined and controlled by you, the Customer, at your sole discretion, and which may include, but is not limited to the following categories of personal data,

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- ID data
- Professional life data
- Personal life data
- Connection data
- Localisation data

3. What steps have we taken to identify the data processing activities of our organisation?

We have undertaken a data inventory and data mapping to determine the following:

- the types of personal data that are processed;
- the categories of data subjects whose personal data are processed;
- why the personal data is processed (in order to determine the lawful basis of processing);
- how the personal data is processed;
- where the personal data is processed or stored geographically;
- third parties to whom personal data is sent to or shared with;
- how long the personal data is retained for; and
- identified the safeguards in place to protect the personal data.

As a result of the above undertaking we have reviewed and updated our records of processing activities, data protection procedures, documentation and privacy notices.

4. Do we have a designated Data Protection Officer?

MyGoldCloud does not currently meet the mandatory criteria for appointing a DPO under the GDPR. In accordance with the GDPR we have carried out an assessment taking into account the relevant factors as to whether we should appoint a DPO on a voluntary basis.

We have concluded that at this time MyGoldCloud processing activities does not warrant the voluntary appointment of a DPO, but fully recognise that these will

change over time and therefore subject to continuous reassessment.

To contact the team that carries out the data protection functions and ensures compliance of the organisation with data protection regulations contact privacy@locationextreme.com

DATA PROTECTION POLICIES

5. **Does MyGoldCloud have updated Service Terms in place to reflect its processing obligations under GDPR?**

   We have updated our Terms of Service to reflect the new legal requirements. These are available here.

   Rather than a single Terms of Service covering all solutions, we now have a Master Services Agreement, which includes three different services terms:

   - MyGoldCloud
   - MyGoldMail
   - Consulting Services (including training)

   You will find the details of the service specific terms in the Data Processing Addendum The DPA does not materially change the terms and conditions but it does ensure that MyGoldCloud meets its obligations under GDPR.

6. **What data protection policies do we have in place?**

   We have the following policies in place to support our data protection compliance program:

   - Data protection policy
   - Privacy Notice
   - Information security policy
   - Cookie Policy
   - Sub-processors and Sub-contractors
   - Fair usage policy

   These policies can be accessed here.

7. **Where is data physically stored?**

   The MyGoldCloud service data is stored within a secure Microsoft Azure environment in the UK (secondary datacentres within the EC and specific

geographies may be assigned upon customer request). See our Information security policy for more information.

8. **Who do we share data with, on what basis and where is it geographically located?**
   All MyGoldCloud sub-processors are located within the UK, data is only shared with third parties with the full knowledge and consent of you, the customer, in fulfilment of your service agreement.

9. **How do we protect the data from unauthorised access or modification?**
   The way we do this is set out in the Data Processing Addendum of the Master Service Agreement which can be reviewed here.

10. **Do we test software using personal data?**
    No, we don't use personal data to test software, but we do enable customers to store personal data in production, using their own data, prior to a go-live or a new release.

11. **How does indemnity work in relation to data breaches?**

    This is covered within clause 10 of the Data Processing Agreement.

12. **How do we demonstrate compliance with the GDPR?**
    Our data protection compliance programme is at the heart of our approach to data protection. At the core of the compliance program is our implementation of robust policies which are available for review here.

13. **Do we have an Information Security Policy?**

    Yes we do. This policy is accessible here.

14. **Please provide a link to your Privacy Policy**

    Our privacy policy is available here.

15. **Do our employment contracts require employees to comply with our data protection policies?**
    Our employment contracts recognise that employees will have access to personal and sensitive personal customer data and they agree to comply with our Data Protection Policy at all times.

16. **How do we deal with Information Security incidents?**

We have security incident management process described within our policies here.

TRAINING AND AWARENESS

17. What training do we undertake as part of our data compliance program?

All staff receive information security awareness training on joining the company, refresher training annually and role-specific information security training. We maintain records of all such training. We also vet all new employees using a third-party organisation.

18. Have any staff undertaken GDPR specific training?

Key members of staff have undertaken certified GDPR training at Foundation and Practitioner level. We give additional training in relation to the policies associated with protecting personal data, as well as non-compliance with the information security management system, breach and incident management. Employees are reminded that their contractual Confidentiality obligations remain in force post leaving the company.

19. What training is done by MyGoldCloud sub-processors?

MyGoldCloud requires its sub-processors to satisfy equivalent obligations which include providing regular training in security and data protection to personnel whom they grant access to personal data.

CONTROLS IMPLEMENTED TO REDUCE AND MONITOR RISK

20. What information does MyGoldCloud process?

We only process information under the strict instruction of the customer which are set out in a written contract as required under the GDPR.

21. How do we assist the controller in demonstrating compliance with the GDPR?

There is a requirement for us to assist the controller in demonstrating compliance (e.g. assisting in responding to subject access requests and permitting audits by the controller or its third-party auditors).

22. How would MyGoldCloud as a processor deal with a Subject Access Request?

If the Data Subject clearly identifies the data controller in their request, we would promptly refer it to the data controller upon receipt of the request.

If the Data Subject does clearly identify the data controller then we are limited to checking our own database and the search would be restricted e.g. employees of the

data controller, third parties or parties to the Service Contract you have with us and therefore be MyGoldCloud data subjects.

23. Would MyGoldCloud provide us with the information to meet the Subject Access Request timeframes under the GDPR?

There are tools in MyGoldCloud that enable our customers to manage these requests themselves. We do not undertake fulfilment of Subject Access Requests on your behalf.

24. How would the rights of the data subject be administered in the MyGoldCloud environment? Such as Right to be Forgotten, Right to Access, Right to Data Portability, Right to Rectification etc

There are tools in MyGoldCloud for the customer to manage these requests. We do not undertake fulfilment of 'Right to be Forgotten' on your behalf.

25. What controls are in place to manage data encryption and access?

Encryption at Rest refers to the cryptographic encoding (encryption) of data when it is persisted. The Encryption at Rest designs in MyGoldCloud use symmetric encryption to encrypt and decrypt large amounts of data quickly according to a simple conceptual model:

- A symmetric encryption key is used to encrypt data as it is persisted
- The same encryption key is used to decrypt that data as it is readied for use in memory
- Data may be partitioned, and different keys may be used for each partition
- Keys are stored in a secure location with access control policies limiting access to certain identities and logging key usage. Data encryption keys are encrypted with asymmetric encryption to further limit access.

In addition, your customer MyGoldCloud file stores utilise Azure Storage Service Encryption for Data at Rest helping you protect your data to meet your organizational security and compliance commitments. With this feature, MyGoldCloud File Storage automatically encrypts your data before persisting it to MyGoldCloud Azure Storage, and decrypts the data before retrieval. The handling of encryption, encryption at rest, decryption, and key management in Storage Service Encryption is transparent to users. All data written to MyGoldCloud Azure Storage is encrypted through 256-bit AES encryption, one of the strongest block ciphers available.

Storage Service Encryption is enabled for all new and existing MyGoldCloud File storage accounts and cannot be disabled. Because your data is secured by default, you don't need to modify your code or applications to take advantage of Storage Service Encryption.

Storage Service Encryption does not affect MyGoldCloud File Storage performance

26. How does access control work?

Multiple levels of authorisation exist to permit access to data. With no public facing IPs we are able to ensure that MyGoldCloud data cannot be accessed outside of our secure cloud.

27. How is the data protected from disclosure to unauthorised parties during transmission?

All data transfer happens over encrypted links (HTTPS) utilising strong cryptographic algorithms.

28. How does MyGoldCloud manage backups?

Backups are available via our full point-in-time recovery model for 30 days. Backups are encrypted-at-rest and secured behind multiple layers of access controls held within Microsoft Azure data warehouses with full redundancy.

29. How does MyGoldCloud implement firewalls (between the public internet and the hosting server(s) and network)?

In addition to perimeter firewalls we have multiple safeguards within the service via monitored security controls embedded within our Microsoft Azure-based platform. MyGoldCloud services utilise the Microsoft Secure Development Lifecycle which incorporates privacy-by- design and privacy-by-default methodologies. Azure and related tools ensure you comply with GDPR data protection requirements enabling you to secure & encrypt personal data at rest and in transit, detect and respond to data breaches, and facilitate regular testing of security measures.

30. How does MyGoldCloud guards against network intrusion?

MyGoldCloud utilises Azure Security Center (ASC) which helps prevent and detect threats with tools that monitor traffic, collect logs, and analyse these data sources. Security Health Monitoring in ASC helps identify potential vulnerabilities. MyGoldCloud has a detailed Security Incident Response Management and notification process specific to its Azure environment.

31. Does MyGoldCloud use host-based network intrusion systems?

Yes, our UK based Microsoft Azure datacentre utilities Azure Monitor & Azure Security Centre to detect and response to any suspicious access attempts to your

system such as a login attempt from one of your users from a geographical location or IP address that they have not previously used. Our application-based firewall learns user behaviour so that if a user based in Wolverhampton attempts to log in from the Far East our breach detection systems will be triggered.

32. **Does MyGoldCloud provide a managed AV (anti-virus, anti-malware etc) solution for all customer systems?**
    Yes, all servers are secured by anti-malware and anti-virus solutions provided by our hosting sub-processor, Microsoft.

33. **How does MyGoldCloud carry out penetration testing against the servers, applications, and perimeter hardware?**
    MyGoldCloud is hosted within a Microsoft Azure environment in the UK which undergoes regular live site penetration testing against the managed infrastructure, services and application, more details available here.

34. **Does MyGoldCloud permit penetration testing against the servers, applications, and perimeter hardware.**
    MyGoldCloud partners with Microsoft Azure: Azure's Enterprise Cloud Red Teaming strategy and Assume Breach philosophy adopts a model that generates a number of combined attack scenarios such as Denial of Service, Malware Outbreak, Remote Code Execution, Customer data compromise, Inside attacker and Service Compromise.

38. **What access controls are in place at the datacentre?**
    MyGoldCloud is hosted within a Microsoft Azure environment in the UK: Azure is deployed in Microsoft regional datacentres. These datacentres are protected by layers of defence-in-depth security that include perimeter fencing, video cameras, security personnel, secure entrances, and real-time communication networks. This multi- layered security model is in use throughout every area of the facility, including each physical server unit.

39. **What technical certifications does the hosting company hold?**
    MyGoldCloud is hosted within a secure Microsoft Azure environment: consequently, the MyGoldCloud Azure Environment holds more certifications than any other cloud provider, it meets a broad set of international and industry-specific compliance standards, such as General Data Protection Regulation (GDPR), ISO 27001, HIPAA,

FedRAMP, SOC 1 and SOC 2, as well as country-specific standards, including Australia IRAP, UK G-Cloud and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify Azure's adherence to the strict security controls these standards mandate

40. **How does patch management work?**

    Windows updates are automatically applied to our VMs within the MyGoldCloud environment via Azure Automation.

41. **How long do you retain each item of our data for and the justification for the retention period?**

    The retention period is the responsibility of the customer based on the type of data that is held within your MyGoldCloud solution. If you terminate your agreement with MyGoldCloud we automatically delete your database(s) after 30 days.

42. **When do you notify us if you become aware of a data protection breach by your company or a sub-contractor?**

    We conform with the standards as laid out within the GDPR that requires us to notify you 'without undue delay'.

MONITORING COMPLIANCE

43. **What checks are undertaken on sub-processors?**

    We ask all suppliers to complete an information security questionnaire in accordance with our supplier management policy.

44. **How do we monitor compliance with GDPR?**

    We continually monitor conformance with existing legislation. Additionally, we receive continual updates on evolving data protection law and guidance from the UK Regulator – the Information Commissioners Office.

REPORTING

45. **How do we report on activities and compliance issues discovered?**

    A report is compiled by the privacy team in relation to any data privacy and information security issues such as breaches, complaints, guidance from regulators, and it is circulated to middle, senior & the board of directors for action.

ANNUAL REVIEW PROCESS

46. What do we review on an annual basis?

On an annual basis we review issues of compliance over the preceding 12months, as well as any changes in the law and regulations and the impact on processing, also any changes in data processing activities within the organisation such as the introduction of biometric data and mobile apps are reviewed as required upon deveopment or during our annual review.