DATA PROCESSING AGREEMENT FOR MIRAKL SERVICES

1. PURPOSE

1.1. This Data Processing Agreement (hereinafter the "DPA") completes the Order Form and Mirakl's General Terms of Use (hereinafter together, the "Agreement") signed between Mirakl and Customer, in order to reflect the Parties' agreement regarding the Personal Data processed for the performance of the Agreement as described in annex 1 "Details of the Processing", in accordance with the requirements of the Applicable Data Protection Law.

1.2. Within the scope of their contractual relationship, it is understood that the Parties act in their respective capacities:

(i) For the Personal Data of their respective business contacts processed in the context of their reciprocal commercial relationship: of independent data controllers for Mirakl and Customer;

(ii) For the Personal Data processed in the context of the administrative, technical and commercial management of the Cloud Services: of independent data controller for Mirakl;

(iii) For the Customer Personal Data processed in the context of the provision of the Cloud Services by Mirakl to Customer and Customer's use of the Cloud Services;

- ***of data controller for Customer*** since Customer determines the purposes and the means of the Processing of the Customer Personal Data as described in the annex 1 "Details of the Processing" of this DPA; and
- ***of data processor for Mirakl*** since Mirakl ensures, on behalf of Customer and under its documented instructions, the Processing of the Customer Personal Data as described in the annex 1 "Details of the Processing" of this DPA.

2. DEFINITIONS

2.1. The following terms, whether used in the singular or in the plural, shall have the meaning set forth below. The other capitalized terms in the DPA shall have the meanings set forth in the Agreement.

"Applicable Data Protection Law" means the regulation applicable to personal data provided under any provision of a legislative or regulatory, European or member state nature, including in particular the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR").

"Customer Personal Data" means the Personal Data which is contained in the Customer Data.

"Data Subject", "Personal Data", "Personal Data Breach", "Processing" and "Special category of Personal Data" have the meaning assigned to it in the Applicable Data Protection Law.

"Sub-processor" means any third parties that Mirakl group may engage in connection with the provision of the Cloud Services, in accordance with the DPA.

2.2. If and to the extent Mirakl is Processing Customer Personal Data on behalf and in accordance with the documented instructions of Customer within the scope of a United States privacy state legislation ("US State Law"), the Applicable Data Protection Law, where permitted and compatible with such US State Law, this DPA is to be read as referencing US State Law among the regulation applicable to personal data and specific references to GDPR are replaced with equivalent article or section of US State Law.

"Business Purpose" shall have the same meaning as in the US State Law;

"Commercial Purpose" shall have the same meaning as in the US State Law;

"Controller" includes "Business" as defined under the US State Law;

"Data Subject" includes "Consumer" as defined under the US State Law.

"Personal Data" includes "Personal Information" as defined under the US State Law.

"Personal Data Breach" includes "Breach of the Security of the System" as defined under the US State Law.

"Processor" includes "Service Provider" as defined under the US State Law.

The parties agree that, with regard to the processing of Personal Information under the US State Law, Controller is a Business and Processor is a Service Provider.

Controller discloses Customer Personal Data to Processor solely for: (i) valid Business Purposes; and (ii) to enable Processor to perform the services described in the Agreement and in Schedules of the DPA.

Processor shall not: (i) sell Personal Data; (ii) retain, use or disclose Personal Data for a Commercial Purpose other than providing the services specified in the Agreement and in Schedules of the DPA or as otherwise permitted by the US State Law; nor (iii) retain, use, or disclose Personal Data except as permitted under the Agreement and the present DPA between Controller and Processor.

2.3. If and to the extent Mirakl is Processing Customer Personal Data on behalf and in accordance with the documented instructions of Customer within the scope of the UK Data Protection Act 2018 ("UK Law") the Applicable Data Protection Law, where permitted and compatible with such UK Law, this DPA is to be read as referencing UK Law among the regulation applicable to Personal Data and specific references to GDPR are replaced with equivalent article or section of UK Law.

3. SCOPE OF THE DPA

3.1. The following provisions apply to the Customer Personal Data processed by Mirakl, acting as data processor, and its Sub-processors where applicable, for the provision of the Cloud Services. Customer shall not process, store or use in any way whatsoever Personal Data in nonproductive environments. Therefore, this DPA will not apply to such environments.

3.2. Customer acts as a single point of contact for Mirakl and shall obtain any relevant authorization, consent, and permission for the Processing of Personal Data in accordance with the Agreement and this DPA in particular. Any instruction given to Mirakl by Customer or any of its Authorized Users shall be deemed to have been given on Customer's behalf. Vice versa, any information given by Mirakl to Customer shall be deemed given to any Authorized User of the Cloud Services.

3.3. Customer shall not submit and/or provide any kind of Special category of Personal Data through the Cloud Services at all events.

4. COMPLIANCE

4.1. The Parties shall comply with the obligations set forth in the Applicable Data Protection Law. Customer agrees that Mirakl is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. Mirakl does not determine whether Customer Data includes information subject to any specific law or regulation.

4.2. Customer shall have sole responsibility for:

(i) the accuracy, quality, fairness and lawfulness of the Customer Personal Data and the means by which Customer obtained such Personal Data;

(ii) (a) assessing the appropriate legal grounds (pre-contractual measures, agreement, legitimate interest, vital interests, public interest, legal obligations) under the Applicable Data Protection Law for the Processing of the Customer Personal Data and obtain, where applicable, the Data Subjects' free, specific, informed unambiguous consent to the Processing in accordance with the Applicable Data Protection Law, (b) retain evidence of the Data Subject's consent to the Processing, (c) ensure Data Subjects can exercise their right to withdraw their consent at any time;

(iii) informing the Data Subjects about the Processing of the Customer Personal Data operated by Mirakl and its Sub-processors; and

(iv) obtaining any relevant authorization where required by the applicable law

5. DOCUMENTED INSTRUCTIONS

5.1. Mirakl shall only process the Customer Personal Data on behalf of Customer and upon its documented instructions (including the DPA and its annex 1, unless provided otherwise by an applicable law.

5.2. By entering into this DPA, Customer instructs Mirakl to process the Customer Personal Data:

(i) to provide the Cloud Services;

(ii) a further specified via Customer's use of any functionality of the Cloud Services;

(iii) as documented in the Agreement, including the Order Form and the Documentation; and

(iv) as further documented in any other written instructions given by Customer and acknowledged by Mirakl as constituting instructions for purposes of this DPA.

5.3. If Mirakl considers that a Customer's instruction does not comply with the Applicable Data Protection Law or the Agreement, Mirakl shall not be required to comply with such instruction and will notify Customer.

6. SUPPORT

6.1. Upon Customer's request, Mirakl shall provide the relevant and available information to enable Customer to ensure that Mirakl's obligations under this DPA are complied with.

6.2. Mirakl undertakes to make available to Customer the relevant information to enable Customer to demonstrate compliance with its obligations under the Applicable Data Protection Law, in particular by reasonably assisting Customer in ensuring compliance with obligations pursuant to Article 32 to 36 of the GDPR (security of Processing – notification to the supervisory authority and communication to the Data Subject in case of a Personal Data Breach – data protection impact assessment and prior consultation with the supervisory authority).

6.3. To the extent the applicable law requires Mirakl to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to Mirakl and keep it accurate and up to date. Mirakl may make any such information available to the supervisory authority if required by the Applicable Data Protection Law.

7. SUB-PROCESSORS

7.1. Customer authorizes Mirakl to engage Sub-processors in connection with the provision of the Cloud Services.

Mirakl is authorized to use the Sub-processors with whom it already works at the date of signature of this DPA.

7.2. Mirakl has entered or shall enter into written agreements with each Sub-processor containing similar Personal Data protection obligations to those in this DPA with respect to the protection of the Customer Personal Data to the extent applicable to the nature of the service provided by such Sub-processor.

7.3. Mirakl shall inform Customer of any new third-party Sub-processor that will process the Customer Personal Data engaged during the Term. In case Customer has legitimate reasons to reject a new Sub-processor for non-conformity with the Applicable Data Protection Law, the Customer may object to Mirakl's appointment of such new third-party Sub-processor by notifying its rejection to Mirakl in writing within thirty (30) days of Mirakl's notice regarding the appointment of such new Sub-processor. Mirakl will in such case make reasonable efforts to (i) make available to Customer a change in the Cloud Services if technically and/or commercially feasible, or (ii) recommend a change to Customer's configuration or use of the Cloud Services to avoid the Processing of the Customer Personal Data by the objected-to new Sub-processor. If the Parties are not able to find a mutually agreeable solution within thirty (30) days of Mirakl's notice to Customer of such new Sub-processor's appointment, then Customer shall cease to use the Cloud Service impacted by this appointment and will be entitled to terminate the Agreement by sending a written notice to Mirakl. Such termination shall take effect at the time determined by Customer which shall be no later than thirty (30) days of the date of Mirakl's notification. If Customer does not terminate within this thirty (30) days period, Customer shall be deemed to have approved the appointment of the new Sub-processor.

7.4. Upon Customer's request, Mirakl shall make available the current list of its Sub-processors involved in the provision of the Cloud Services.

8. DISCLOSURE AND CONFIDENTIALITY

8.1. Mirakl will not disclose or provide access to any Customer Personal Data except: (i) as required by the Customer; (ii) as described in this DPA; or (iii) as required by law.

8.2. Mirakl will not disclose or provide access to any Customer Personal Data to law enforcement or other third party unless required by law. If law enforcement contacts Mirakl with a demand for Customer Personal Data, Mirakl will attempt to redirect the law enforcement agency to request that data directly from Customer. To the extent permitted by applicable law, Mirakl will notify Customer and provide a copy of the demand, unless prohibited from doing so.

8.3. Mirakl shall ensure that the Processing of the Customer Personal Data is strictly limited to persons, including its employees, Affiliates' employees and its Sub-processors' employees, for whom access to said Personal Data is necessary to perform the Agreement. Such persons shall be bound by confidentiality obligations with respect to the Personal Data they may process.

9. SECURITY

9.1. Mirakl shall maintain the appropriate technical and organizational measures described in Annex 2 "Technical and Organizational Measures" of this DPA to ensure the security, confidentiality, and integrity of the Customer Personal Data, including protection against a Personal Data Breach.

9.2. Customer has reviewed the technical and organizational measures implemented by Mirakl and agrees that they provide a level of security appropriate to the risk with to the Processing of the Customer Personal Data. Customer is responsible for implementing and maintaining appropriate security measures for components that Customer provides or controls.

9.3. Mirakl is authorized to modify, at any time, the technical and organizational measures implemented without notice to Customer provided a similar or greater level of security is maintained.

10. PERSONAL DATA BREACHES

10.1. Mirakl shall notify Customer without undue delay after becoming aware of a Personal Data Breach, providing Customer with the information available at the time.

10.2. If relevant, Mirakl may thereafter send another notice to Customer, providing Customer with further information discovered by Mirakl with regards to the Personal Data Breach.

10.3. Mirakl shall take all necessary corrective actions to mitigate harmful effects and prevent recurrence of such Personal Data Breach, to the extent the actions are within Mirakl's reasonable control. These obligations shall not apply to Personal Data Breaches that are caused by Customer or the Data Subjects.

11. AUDITS

11.1. Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Mirakl shall make available to Customer or Customer's independent third-party auditor, which is not a competitor of Mirakl, any reports and/or audits regarding Mirakl's compliance with the obligations set forth in this DPA. Customer agrees that any information and audit rights granted by the applicable Data Protection Laws will be satisfied by these reports and/or audits.

11.2. If Mirakl fails to comply with section 11.1 and provided that Customer notifies Mirakl at least sixty (60) calendar days in advance, Customer may request an on-site audit of the security measures relevant to the protection of the Customer Personal Data. Before the beginning of any on-site audit, Customer and Mirakl shall mutually agree upon the scope, timing and duration of the audit. The Parties acknowledge and agree (i) on a maximum of one (1) audit per year, (ii) the audit shall be limited to a maximum of five (5) business days, and (iii) Customer shall bear all costs associated with the audit including reimbursing Mirakl for any time expended for any such on-site audit, including time spent by its personnel, except in the event the audit reveals a material breach of the security measures attributable to Mirakl.

12. CUSTOMER PERSONAL DATA DELETION

12.1. At the end of the Subscription Term, Customer hereby instructs Mirakl to delete the Personal Data remaining on servers hosting the Cloud Service within a reasonable time period (that cannot exceed six (6) months) and respecting the Protection Law unless applicable law requires retention for a longer period of time.

13. DATA SUBJECT REQUEST

13.1. Mirakl will assist the Customer, in a manner consistent with the functionality of the Cloud Services and Mirakl's role as a processor with the fulfillment of Data Subject requests to exercise their rights. When Mirakl receives a request End-Customer to exercise one or more of his or her rights in connection with Cloud Services for which Mirakl is a data processor, Mirakl will redirect the data subject to make its request directly to Customer.

13.2. It is understood that the responsibility to reply to Data Subject requests is Customer's exclusive responsibility, Mirakl will however make its reasonable efforts to enable Customer to handle such requests. Customer will be able to (i) handle anonymization requests in autonomy through a tool made available by Mirakl (as further described in the Documentation) and (ii) contact the Support Service regarding other requests it may receive from such Data Subjects.

14. DATA CENTER LOCATION AND INTERNATIONAL TRANSFER

14.1. The Customer Data will be primarily hosted in the data center used by Mirakl to Customer's region, unless specified otherwise in the Order Form.

14.2. Mirakl shall be entitled to process the Customer Personal Data outside the European Union in accordance with the Applicable Data Protection Law.

14.3. When required by the Applicable Data Protection Law, the Parties acknowledge and agree to rely on the system of the standard contractual clauses published by the European Commission. Furthermore, Customer shall conduct, with the reasonable assistance of Mirakl if and when required, an assessment of the impact and ability of the third country's legislation to ensure the effectiveness of the Data Subjects' rights.

14.4. If and when necessary, Customer is informed Mirakl relies on the standard contractual clauses on its customers' behalf with its Sub-processors.

15. PRIVACY AND SECURITY CONTACTS

15.1. Customer Privacy Contact: référencé dans le Bon de Commande

15.2. Customer Security Contact référencé dans le Bon de Commande

15.3. Mirakl Group DPO: privacy@mirakl.com

15.4. Mirakl CISO: security@mirakl.com

ANNEX 1: DETAILS OF THE PROCESSING

1. DETAILS OF THE PROCESSING

1.1. Nature and Purpose of the Processing. Mirakl shall process the Customer Personal Data as necessary, to provide the Cloud Services pursuant to the Agreement and as further instructed by Customer in its use of the Cloud Services. The purpose of the Processing of the Customer Personal Data by Mirakl is the provision of the Cloud Services to Customer.

1.2. Categories of Data Subjects.

1.2.1. Mirakl Core Platform: The Data Subjects concerned by the Processing of the Customer Personal Data are: (i) end users and (ii) Authorized Users.

1.2.2. Mirakl Payout Platform: The Data Subjects concerned by the Processing of the Customer Personal Data are Authorized Users.

1.2.3. Mirakl Ads Platform: The Data Subjects concerned by the Processing of the Customer Personal Data are Authorized Users. The parties hereby acknowledge that personal data of end users are processed by and stored in a pseudonymised or anonymised form that does not allow Mirakl to identify directly or indirectly the individuals.

1.3. Categories of Personal Data. Customer submits and/or provides the Customer Personal Data through the Cloud Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- For end users: name, surname, shipping address, billing address, email, telephone number, order history.
- For Authorized Users: title, name, surname, company name, email, address, certificate of incorporation or representative's identity card, bank account details, representative's information (title, name, surname, email, telephone, fax).

1.4. Categories of recipients. The recipients of the Customer Personal Data are: (i) employees of the Mirakl group, (ii) service providers (including Sub-processors) of the Mirakl group, (iii) where applicable, lawyers of the Mirakl group and all interested parties, and (iv) where applicable, administrative or judiciary authorities.

2. DURATION OF THE PROCESSING

2.1. The duration of the Processing of the Customer Personal Data is equal to the term of the Agreement, subject to Mirakl's obligation to delete the Customer Personal Data as detailed in the DPA. However, Customer is able and responsible to set up the Cloud Services to limit the maximum duration during which the Customer Personal Data shall be stored within the Cloud Services.

2.2. Mirakl reserves the right to store and archive all technical information, electronic exchange, Customer Personal Data as well as any Personal Data of any kind whatsoever for the purpose of satisfying any applicable legal requirements or for evidentiary purposes, pursuant to Mirakl's document retention policies, in accordance with applicable law.

ANNEX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

This Information Security Addendum or Technical and Organizational Measures, per the GDPR[1] ("Addendum"), outlines the security requirements that Mirakl will maintain as part of the Cloud Services ("Security Requirements") and is incorporated into the agreement between the Parties ("Agreement") by and between Mirakl and Customer. Capitalized terms used in this Addendum without a definition will have the meanings given to them in the Agreement.

1. Information security program

Mirakl will:

(i) implement and maintain a comprehensive written information security program;

(ii) update and review such program, as necessary, on a regular basis or upon a material change in the provision of the Cloud Services; and

(iii) ensure such program

- complies with applicable laws and applicable industry standards (including ISO 27001, ISO 27018, ISO 27701, ISO 22301, SOC 1 Type II, SOC 2 Type II),
- includes appropriate administrative, logical, technical, and physical safeguards that comply with this Addendum,
- detect and prevent against a Security Breach ("Security Breach" means a breach of the Cloud Services' security leading to the accidental or unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Mirakl, and
- is reasonably designed to achieve the following objectives:
    a. to ensure the security and the confidentiality, integrity, and availability of Customer Data;
    b. to protect against threats or hazards to the security and integrity of Customer Data; and
    c. to prevent unauthorized or accidental access, acquisition, destruction, loss, deletion, disclosure, alteration, or use of Customer Data.

The provisions of this Addendum will control in the event of a conflict between the Agreement (including any other attachments, exhibits or schedules thereto) and this Addendum.

2. Security, privacy & resilience by design

Mirakl will incorporate security, privacy & resilience into the design and operation of the Cloud Services, and will dynamically respond to changes in legal obligations, regulatory guidance, industry best practices, and known and foreseeable risks to the Customer Data.

3. Security policies

Mirakl will maintain information security policies covering at minimum the following key areas:

- Risk Management
- Asset Management
- Human Resources Security
- Access Control
- Physical and Environmental Security
- Operations Security

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- Cryptography
- Secure Development
- Vulnerability and Patch Management
- Security Monitoring
- Security Incident Management
- Third Party Vendor Management
- Business Resilience

4. People management

Background checks: Mirakl will conduct background checks on candidates for employment in accordance with local laws and regulations.

Security Awareness and Training: Mirakl will provide security & privacy awareness training to Mirakl employees at the time of hire and annually thereafter. Training will be regularly updated to include applicable information on security & privacy topics, including, responsibilities for protecting data and systems, and emerging threats and trends.

5. Identity & Access Management

Mirakl will permit only those Mirakl personnel and third parties who are authorized pursuant to the Agreement (collectively, "Mirakl Users") to access the Customer Data. Mirakl Users will use the Customer Data solely as permitted under the Agreement and this Addendum.

Mirakl will employ the Principle of Least Privilege when granting access to the Customer Data. This means that only Mirakl Users who have a need-to-know or access the Customer Data will be granted access, and only to the extent such access is required for their assigned job function.

Mirakl will follow industry standards to authenticate and authorize users.

Mirakl Users will not use shared or generic identification credentials to access Customer Data.

Mirakl will require Mirakl Users to use two-factor authentication to access systems where Customer Data resides.

Mirakl will maintain a centralized repository of all identification credentials used to access Mirakl's network where Customer Data resides.

Mirakl will revoke access from Mirakl Users who no longer require access to Customer Data.

Mirakl will periodically review and revoke access rights of Mirakl Users, as needed.

Authentication to Mirakl's network resources, platforms, devices, servers, workstations, applications and devices will not be allowed with default passwords.

Mirakl will ensure that external network connections to Mirakl's network are secure.

Mirakl will change default server passwords prior to placing the device or system into production.

Workstations that have been inactive for a period of time will be automatically locked.

6. Secure Data Handling

Mirakl will encrypt the Customer Data, during transmission and at rest, using industry standard algorithms.

Mirakl will apply and maintain full disk encryption at rest on all Mirakl's systems that access, transmit, or store Customer Data.

Symmetric encryption keys and asymmetric private keys will be encrypted in transit and storage, protected from unauthorized access, and secured. Cryptographic key management and rotation procedures will be documented. Access to encryption keys will be restricted to key custodians. Mirakl will follow industry standards to generate, store, and manage cryptographic keys used to encrypt Customer Data.

Mirakl will maintain secure data disposal procedures, including but not limited to using secure erase commands, degaussing, and "crypto shredding" as appropriate, and as in accordance with industry standards.

Customer Data will be logically separated from that of other Mirakl Customers.

7. Infrastructure & Network Security

Mirakl will install, configure, and maintain perimeter and network security controls to prevent unauthorized access to Customer Data.

Mirakl will perform continuous monitoring and logging, and relevant alerting for security events, including attempted and successful access, unauthorized changes on endpoints, network devices, and server systems that contain Customer Data, and other indicators of compromise. All logs will be protected from unauthorized access or modification.

Mirakl will implement and maintain security and hardening standards for network devices, based on industry best practices.

8. Change management

Mirakl will follow documented change management procedures in order to prevent any change that could lead to unauthorized disclosure, modification or destruction of data.

9. Application Security

Mirakl will follow secure software development life cycle secure coding practices, such as those developed by the Open Web Application Security Project (OWASP) Top 10 (found at www.owasp.org), to ensure harmful code is not delivered into production and best practices are followed. Coding practices will include:

(i) separate development, test, and production environments;

(ii) risk assessment during the conception phase;

(iii) code/peer reviews;

(iv) security scanning of all Mirakl software and/or applications storing, processing, or transmitting Customer Data; and

(v) use of only non-production, obfuscated, or de-identified data used in non-production environments (e.g., development or test).

10. Physical security

Physical security. Mirakl will use industry-standard measures in order to ensure physical security of its premises, notably:

(i) Physical access control mechanisms (distinguished access authorizations for Mirakl personnel and third parties; restricted keys and passes, identification of persons with authorized access, protections of exits, video surveillance) to ensure only authorized persons can obtain physical access to premises from which the Cloud Services are provided.

(ii) Establish protocols to protect against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster at Mirakl premises.

Equipment security. Mirakl will protect its systems and other equipment to reduce risks from environmental threats and hazards and opportunities for unauthorized access.

Additionally, for equipment stored in Mirakl's premises, Mirakl will:

(i) Protect equipment that is power-dependent from power failures, surges and other electrical anomalies.

(ii) Protect all power, telecommunication and network cabling from unauthorized access and damage.

(iii) Maintain its systems and other equipment to ensure their continued availability and integrity.

(iv) Implement exit procedures to control unauthorized removal of systems and other equipment.

11. Risk Management; Third Party/Mirakl Assurances

Mirakl regularly performs risk assessments, at least annually or when significant changes occur. These risk assessments cover information security and privacy matters.

Mirakl will maintain a third-party risk management program which includes:

(i) maintenance of information security agreements to ensure that Mirakl's third parties with access to Customer Data are bound to security requirements at least as restrictive as those set forth in this Addendum; and

(ii) monitoring and auditing third parties with access to Customer Data for compliance with the requirements set forth in this Addendum.

Risk management will include remediation by Mirakl of any identified findings commensurate with risk and evidence of completion.

Mirakl will maintain a risk assessment program, which defines roles and responsibilities for performing risk assessment and responding to results. Mirakl will perform regular risk assessments to verify the design of controls that protect business operations and information technology.

12. Vulnerability & Patch Management

Vulnerability scanning: Mirakl will perform routine vulnerability scans and will remediate them according to industry standards and associated security risks.

Penetration tests: Mirakl will, at least once a year, retain an independent third party to conduct a penetration test of Mirakl's infrastructure and systems in order to detect any material security weaknesses. In the event weaknesses are found, Mirakl will make the reasonable and available corrections, according to the associated security risks. Mirakl will, upon Customer's request and no more than once a year, provide Customer with the executive summary of such penetration test.

Patch management: Mirakl will apply security patches and system updates to Mirakl-managed software and applications, appliances, and operating systems according to industry standards and associated security risks.

13. Business Continuity & Disaster Recovery

Mirakl will maintain policies and procedures for responding to an emergency or a force majeure event that could damage Customer Data or production systems that contain Customer Data. Such procedures include:

- Data Backups: A policy for performing periodic backups of production file systems and databases to meet the Recovery Point Objective described below;
- Business Continuity Plan: A formal process to address the framework by which an unplanned event might be managed in order to minimize the loss of vital resources;
- Disaster Recovery plan: A formal disaster recovery plan for the production environment designed to minimize disruption to the Service which includes requirements for the disaster plan to be tested on a regular basis;
- RPO / RTO: Recovery Point Objective is no more than one (1) hour and Recovery Time Objective is no more than 24 hours.

14. Security Breach Notification

Mirakl will maintain and annually update a documented security breach action and response plan.

If Mirakl discovers or is notified of a security breach that results in unauthorized access, disclosure, or use of Customer Data ("Data Breach"), Mirakl will promptly at its expense:

(i) notify the impacted Customer(s) of the Data Breach without undue delay;

(ii) investigate the Data Breach;

(iii) mitigate the effects of the Data Breach; and

(iv) perform post-incident assessments and report on the results of such assessment(s) to the impacted Customer.

15. Reporting & Audit

At least annually, Mirakl will engage with an independent assessor to:

(i) conduct a compliance assessment and provide, upon request, a full attestation, review or report under:

   a. Service Organization Control (SOC 2 Type II) or

   b. other similar industry recognized independent compliance assessment.

(ii) conduct a certification assessment and provide, upon request, a valid certificate under:

   a. ISO/IEC 27001 or

   b. other similar industry recognized independent compliance assessment.

16. Contact

For any security-related question or request, the Customer will use Mirakl's Support Portal (get.mirakl.help) as a single point of contact.