This Data Processing Agreement (hereinafter, the "DPA") is incorporated into and subject to the terms of the agreement between Mirakl and Customer (the "Agreement") governing Customer's access to and use of the Mirakl Cloud Services. All capitalized terms not defined herein shall have the meaning ascribed to them in the General Terms of Use or, if applicable, in an Order Form.

1. PURPOSE AND SCOPE

1.1) Purpose. The purpose of this DPA is to reflect the Parties' agreement regarding the Personal Data processed in the context 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) Scope. 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; and

(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 Annex 1 "Details of the Processing" of this DPA; and
- of data processor for Mirakl since Mirakl performs, on behalf of Customer and upon its documented instructions, the Processing of the Customer Personal Data as described in Annex 1 "Details of the Processing" of this DPA.

2. DEFINITIONS

2.1) General Definitions.

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	has the meaning assigned to it in the Applicable Data Protection Law.
Personal Data	has the meaning assigned to it in the Applicable Data Protection Law.
Personal Data Breach	has the meaning assigned to it in the Applicable Data Protection Law.
Processing	has the meaning assigned to it in the Applicable Data Protection Law.
Special Category of Personal Data	has the meaning assigned to it in the Applicable Data Protection Law.
Sub-processor	means any third parties that the Mirakl group may engage in connection with the provision of the Cloud Services, in accordance with this DPA.

2.2) US State Law. 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"), this DPA is to be read as referencing the US State Law among the

regulations applicable to the Customer Personal Data and specific references to GDPR are replaced with the equivalent article or section of the US State Law.

Business Purpose	has the meaning assigned to it in the US State Law.
Commercial Purpose	has the meaning assigned to it in the US State Law.
Controller	includes “Business” as defined in the US State Law.
Data Subject	includes “Consumer” as defined in the US State Law.
Personal Data	includes “Personal Information” as defined in the US State Law.
Personal Data Breach	includes “Breach of the Security of the System” as defined in the US State Law.
Processor	includes “Service Provider” as defined in the US State Law.

The Parties agree that, regarding 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 provide the Cloud Services.

Processor shall not: (i) sell Personal Data; (ii) retain, use, or disclose Personal Data for a Commercial Purpose other than providing the Cloud Services or as otherwise permitted by the US State Law; nor (iii) retain, use, or disclose Personal Data except as permitted under the Agreement and this DPA.

2.3) UK Law. 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"), this DPA is to be read as referencing the UK Law among the regulation applicable to the Customer Personal Data and specific references to GDPR are replaced with the equivalent article or section of the UK Law.

3. COVERED PERSONAL DATA

3.1) Customer Personal Data. The following provisions apply to the Processing of the Customer Personal Data 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 Responsibilities. 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. Any instruction given to Mirakl by any of Customer’s Authorized Users shall be deemed to have been given on Customer’s behalf. Vice versa, any information given by Mirakl to any Authorized User shall be deemed given to Customer.

3.3) Special Category of Personal Data. Customer shall not submit and/or provide any kind of Special Category of Personal Data through the Cloud Services.

4. COMPLIANCE

4.1) Compliance with the Applicable Data Protection Law. The Parties shall comply with the obligations set forth in the Applicable Data Protection Law. Customer agrees that Mirakl is not required to comply with any laws or regulations applicable to Customer or Customer’s industry that are not applicable to the Cloud Services. Mirakl does not determine whether Customer Data includes information subject to any specific law or regulation.

4.2) Customer Compliance. 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, and unambiguous consent to the Processing in accordance with the Applicable Data Protection Law; (b) retaining evidence of the Data Subject's consent to the Processing; and (c) ensuring 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 Application Data Protection Law.

5. DOCUMENTED INSTRUCTIONS

5.1) Limitation of Purposes. Mirakl shall only process the Customer Personal Data on behalf of Customer and upon its documented instructions (including this DPA and its Annex 1, unless provided otherwise by the Applicable Data Protection Law).

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

(i) to provide the Cloud Services;

(ii) as 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 the purpose of this DPA.

5.3) Unlawful Instructions. If Mirakl reasonably 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 to resolve the matter.

6. SUPPORT

6.1) Provision of Information. 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) Assistance. Mirakl undertakes to make available to Customer the relevant and available 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 its obligations pursuant to Article 32 to 36 of the GDPR.

6.3) Records. To the extent the Applicable Data Protection Law requires Mirakl to collect and maintain records of certain information relating to Customer, Customer will, if requested, provide Mirakl with such information 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) Use of Sub-processors. Customer grants a general authorization to 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) Sub-processors Obligations. Mirakl has entered or shall enter into a written agreement 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) New Sub-processors. Mirakl shall inform Customer of a new Sub-processor appointed during the Term of the Agreement to carry out the Processing of the Customer Personal Data. Should Customer have legitimate reasons to reject such appointment for non-compliance by the Sub-processor with the Applicable Data Protection Law, Customer may object to it upon written notice to Mirakl within thirty (30) days of Mirakl's notice of the new Sub-processor's appointment. 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 practicable, 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 its subscription to such Cloud Service upon 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 such 30-day period, Customer shall be deemed to have approved the appointment of the new Sub-processor.

7.4) List of Sub-processors. 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) Limitation of Disclosure. Mirakl will not disclose or provide access to the Customer Personal Data to any third parties except (i) as requested by Customer; (ii) as described in this DPA; or (iii) as required by the Applicable Data Protection Law.

8.2) Compelled Disclosure. If a law enforcement agency contacts Mirakl with a demand to access the Customer Personal Data, Mirakl will attempt to redirect the law enforcement agency to request that access directly from Customer. To the extent permitted by the Applicable Data Protection Law, Mirakl will notify Customer and provide a copy of the demand, unless prohibited from doing so.

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

9. SECURITY

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

9.2) Customer Responsibilities. Customer has reviewed the technical and organizational measures implemented by Mirakl and confirms that they provide a level of security appropriate to the risks associated with the Processing of the Customer Personal Data.

9.3) Security Updates. Mirakl is authorized to modify, at any time, Mirakl's technical and organizational measures without notice to Customer, provided a similar or greater level of security is maintained.

10. PERSONAL DATA BREACHES

10.1) Personal Data Breach Notification. 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) Further Notice. If relevant, Mirakl may thereafter send another notice to Customer, providing Customer with further information discovered by Mirakl during the investigation.

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

11. AUDITS

11.1) Mirakl Audits. 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 Law will be satisfied by the provision of these reports and/or audits.

11.2) Customer Audits. 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 applicable to the protection of the Customer Personal Data. Before the beginning of any on-site audit, Customer and Mirakl shall mutually agree on 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 by Mirakl of this DPA.

12. CUSTOMER PERSONAL DATA DELETION

Upon termination or expiration of the Agreement, Customer hereby instructs Mirakl to return and/or delete the Customer Personal Data in accordance with Section "Effect of termination" of the General Terms of Use for Mirakl Cloud Services.

In any case, Customer hereby instructs Mirakl to delete the Customer Personal Data ninety (90) days after termination or expiration of the Agreement.

13. DATA SUBJECT REQUESTS

It is understood that it is Customer's sole and exclusive responsibility, as data controller, to reply to Data Subjects' requests to exercise their rights.

Notwithstanding the foregoing, Mirakl will make commercially reasonable efforts to enable Customer to reply to 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 Mirakl's support service regarding other requests it may receive from such Data Subjects.

If Mirakl receives any such request from a Data Subject, Mirakl will redirect the Data Subject to make its request directly to Customer.

14. DATA CENTER LOCATION AND INTERNATIONAL TRANSFERS

14.1) Data Center Location. The Customer Data will be primarily hosted in the data center used by Mirakl in Customer's region, unless requested otherwise by Customer.

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

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

If and when necessary, Customer is informed that Mirakl relies on the standard contractual clauses of the European Commission on Customers' behalf with its Sub-processors.

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.

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

(ii) Mirakl Payout Platform: the Data Subjects concerned by the Processing of the Customer Personal Data are Authorized Users.

(iii) 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 is processed by and stored in a pseudonymized or anonymized form that does not allow Mirakl to identify directly or indirectly the Data Subjects.

(iv) Mirakl Target2Sell: the Data Subjects concerned by the Processing of the Customer Personal Data are (i) Authorized Users and, if applicable; (ii) web users.

1.3) Categories of Personal Data. Customer submits Customer Personal Data to the Cloud Services, the extent of which is determined and controlled by Customer, 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).

2. DURATION OF THE PROCESSING

Subject to Section 12 of this DPA, the duration of the Processing of the Customer Personal Data is the Term of the Agreement. However, Customer is able and responsible to set up the Cloud Services to further limit the maximum duration during which the Customer Personal Data is stored within the Cloud Services.

ANNEX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

These technical and organizational measures outline the security requirements that Mirakl will maintain as part of the Cloud Services and is incorporated into the DPA. Capitalized terms used in this Annex without a definition will have the meaning assigned 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 22301, SOC 1 Type II, SOC 2 Type II);
- includes appropriate administrative, logical, technical, and physical safeguards that comply with this Annex;
- detects and prevents 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 or otherwise controlled by Mirakl); and
- is reasonably designed to achieve the following objectives:
    a. ensure the security and the confidentiality, integrity, and availability of Customer Data;
    b. protect against threats or hazards to the security and integrity of the Customer Data; and
    c. prevent unauthorized or accidental access, acquisition, destruction, loss, deletion, disclosure, alteration, or use of the Customer Data.

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

2. SECURITY, PRIVACY, AND RESILIENCE BY DESIGN

Mirakl will incorporate security, privacy, and 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
- Cryptography
- Secure Development
- Vulnerability and Patch Management

- Security Monitoring
- Security Incident Management
- Third Party Vendor Management
- Business Resilience

4. PEOPLE MANAGEMENT

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

4.2) 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 and privacy topics, including responsibilities for protecting data and systems, and emerging threats and trends.

5. IDENTITY AND ACCESS MANAGEMENT

Mirakl will permit only those members of the 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 Annex.

Mirakl will employ the Principle of Least Privilege when granting access to the Customer Data. "Principle of Least Privilege" 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 Mirakl Users.

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

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

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

Mirakl will revoke access from Mirakl Users who no longer need access to the 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 the 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 the 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 in accordance with industry standards.

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

7. INFRASTRUCTURE AND NETWORK SECURITY

Mirakl will install, configure, and maintain perimeter and network security controls to prevent unauthorized access to the 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 the 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 to prevent any change that could lead to unauthorized disclosure, modification, or destruction of the Customer Data.

9. APPLICATION SECURITY

Mirakl will follow secure software development life cycle 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 the Customer Data; and

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

10. PHYSICAL SECURITY

10.1) Physical Security. Mirakl will use industry-standard measures 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's premises.

10.2) 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; and

(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 third parties with access to the Customer Data are bound by security obligations at least as strict as those set forth in this Annex; and

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

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 threats. Mirakl will perform regular risk assessments to verify the design of controls that protect business operations and information technology.

12. VULNERABILITY AND PATCH MANAGEMENT

12.1) Vulnerability Scanning. Mirakl will perform routine vulnerability scans and will remediate them according to industry standards and associated security risks.

12.2) 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 to detect any material security weaknesses. In the event weaknesses are found, Mirakl will implement the commercially 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.

12.3) 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 AND DISASTER RECOVERY

Mirakl will maintain policies and procedures for responding to an emergency or a force majeure event that could damage the Customer Data or production systems that contain the 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 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 Cloud Services which includes requirements for the disaster plan to be tested on a regular basis.
- RPO: Recovery Point Objective is no more than twenty-four (24) hours for Mirakl Target2Sell and no more than one (1) hour for all other Cloud Services.
- RTO: Recovery Time Objective is no more than twenty-four (24) hours for all Cloud Services.

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 the Customer Data ("Data Breach"), Mirakl will promptly, at its own 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 customers.

15. REPORTING AND AUDIT

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

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

- Service Organization Control (SOC 2 Type II); or
- other similar industry recognized independent compliance assessments.

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

- ISO/IEC 27001; or
- other similar industry recognized independent compliance assessments.

16. CONTACT

For any security-related question or request, Customer will use Mirakl's support portal (https://help.mirakl.net) as a single point of contact.