Live Assist for Microsoft Dynamics 365

GDPR Compliance Statement

Version 1.0.0

Document History

Author(s)	Version	Description
P. Nono	1.0.0	First Version

YRP 1-508, 3-4 Hikari-no-Oka Yokosuka-Shi, Kanagawa, 239-0847, Japan
tel.: + 81-(0) 46-821-3362 | **cba-japan.com**

Communication Business Avenue, Inc.

Live Assist for Microsoft Dynamics 365

GDPR Compliance Statement

Introduction

The EU General Data Protection Regulation ("GDPR") came into effect across the European Union on 25th May 2018 and brought the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the digital age requirements.

The 21st Century brings broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardize data protection laws and processing across the EU, affording individuals stronger, more consistent rights to access and control their personal information.

Our Commitment

Communication Business Avenue, Inc. or CBA ('we' or 'us' or 'our') is committed to ensuring the security and protection of the personal information that we process and providing a compliant and consistent approach to data protection. We have always had a robust and effective data protection program that complies with existing law and abides by data protection principles. However, we recognize our obligations to update and expand this program to meet the demands of the GDPR.

CBA is dedicated to safeguarding the personal information under our remit and developing a data protection regime that is effective, fit for purpose, and demonstrates an understanding of and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarized in this statement and include developing and implementing new data protection roles, policies, procedures, controls, and measures to ensure maximum and ongoing compliance.

How Did We Prepare for the GDPR?

CBA has a consistent level of data protection and security across our organization. Our preparation includes:

- **Information Audit** – carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed, and if and to whom it is disclosed.
- **Policies & Procedures** – revising data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including: –
    - **Data Protection** – our central policy and procedure document for data protection was overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities, with a dedicated focus on privacy by design and the rights of individuals.
    - **Data Retention & Erasure** – we have updated our retention policy and schedule to ensure that we meet the 'data minimization' and 'storage limitation' principles and that personal information is stored, archived, and destroyed compliantly and ethically. We have dedicated erasure procedures to meet the new 'Right to Erasure' obligation and know when this and other data subject's rights apply, along with any exemptions, response timeframes, and notification responsibilities.
    - **Data Breaches** – our breach procedures ensure that we have safeguards and measures to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and disseminated to all employees, making them aware of the reporting lines and steps to follow.
    - **International Data Transfers & Third-Party Disclosures** – where CBA stores or transfers personal information outside the EU, we have robust procedures and safeguarding measures to secure, encrypt and maintain the integrity of the data. Our procedures include a continual review of the countries with sufficient adequacy decisions and provisions for binding corporate rules, standard data protection clauses, or approved codes of conduct for those countries without it. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards to protect the information, ensure enforceable data subject rights, and have effective legal remedies for data subjects where applicable.

- **Subject Access Request (SAR)** – we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply, and a suite of response templates to ensure that communications with data subjects are compliant, consistent, and adequate.
- **Legal Basis for Processing** – we have reviewed all processing activities to identify the legal basis for processing and ensure that each basis is appropriate for the activity it relates to. We also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met, where applicable.
- **Privacy Notice / Policy** – we have revised our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, whom the information is disclosed to and what safeguarding measures are in place to protect their information.
- **Data Protection Impact Assessments (DPIA)** – where we process personal information that is considered high risk, involves large scale processing, or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity, and implement mitigating measures to reduce the risk posed to the data subject(s).
- **Processor Agreements** – where we use any third party to process personal information on our behalf (i.e., Payroll, Recruitment, Hosting, etc.), we have implemented new compliant Processor Agreements and due diligence procedures for ensuring that they (as well as we), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organizational measures in place, and compliance with the GDPR.
- **Special Categories Data** – where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition.

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information, via our compliance website, of an individual's right to access any personal information that CBA processes about them and to request information about:

- What personal data do we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long do we intend to store your personal data for
- The right to have incomplete or inaccurate data about them corrected or completed, and the process for requesting this
- The right to request the erasure of personal data (where applicable) or to restrict processing following data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and whom to contact in such instances

Information Security & Technical and Organizational Measures

CBA takes the privacy and security of individuals and their personal information very seriously and takes every reasonable measure and precaution to protect and secure the personal data that we process. We have robust security policies and procedures to protect personal information from unauthorized access, alteration, disclosure, or destruction and have several layers of security measures.

GDPR Roles and Employees

CBA understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans. We have implemented an employee training program provided to all employees and forms part of our induction and annual training program.

Subject Access and Right to be forgotten requests

Customers should send all subject access requests or right-to-be-forgotten requests should be sent to our compliance team at compliance@cba-japan.com.

Customer GDPR Addendum

Customers can enter an addendum to cover personal EU data processed by CBA and its sub-processors.

More Information

For more information about Live Assist for Microsoft Dynamics 365, you may contact us at global-sales@cba-japan.com.