Archiving (Data retention) Policy

Introduction

This Archiving policy sets out the obligations of Omni Sp. z o. o. (LLC) ("us/we/our/Company") and the basis upon which we shall retain, review and destroy data held by us, or within our custody or control. This policy applies to the Company, including its officers, employees, agents, sub-contractors, and sets out what the retention periods are and when any such data may be deleted.

Objectives

It is necessary to retain and process certain information to enable our business to operate. We may store data in the following places:

- our own servers;
- any third-party servers;
- potential email accounts;
- desktops;
- employee-owned devices (BYOD);
- potential backup storage; and/or
- our paper files.

This policy applies equally to paper, electronic media and any other method used to store personal data. The beginning of the retention period only commences from the moment of closing the record. We are bound by various obligations under the law in relation to this and therefore, to comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully in respect of their personal data under the General Data Protection Regulation ("the Regulation").

Security and Storage

All data and records are stored securely to prevent misuse or loss. We will take appropriate security measures against unlawful or unauthorized processing of personal data, and against accidental loss or damage to personal data. We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if there is an agreement by them to comply with these procedures and policies, or if there are appropriate measures in place.

We will maintain data security by protecting the confidentiality, integrity and availability of personal data, defined as follows:

a) Confidentiality means that only people who are authorized to use the data can access it.
b) Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
c) Availability means that authorized users should be able to access the data if they need it for authorized purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Archiving (Retention) Policy

Personal data that we are processing will be kept no more than 5 (five) years since the last data subject inactivity, ending of employment period or until the consent is revoke/you have objected to such processing.

Our specific data retention periods are set out below:

Type of data	Type of data subject	Type of processing	Purpose of processing	Retention period
Employees	First Name, Last Name, Email Address, Telephone number, Address, Device IP Address, Marriage status, Health, Credit/Debit Card Details, Bank Details, Date of Birth, Insurance, Other information mentioned in Employee Privacy Notice document	Stored in DE Falkenstein fsn1 (Germany), DE Nuremberg nbg1 (Germany), FI Helsinki hel1 (Finland)	Performing of necessary Employer's obligations	Employment period + 5 years
Customers	Contact person's First Name, Last Name, Email Address, Telephone number, Address, Website, Company Information, Device IP Address, Credit/Debit Card Details, Bank Details	Stored in DE Falkenstein fsn1 (Germany), DE Nuremberg nbg1 (Germany), FI Helsinki hel1 (Finland)	Provide Company's services	Inactive for 5 years*
Customer's clients/ employees/partners	First Name, Last Name, Email Address, Telephone number, Address, Device IP Address, Credit/Debit Card Details	Stored in DE Falkenstein fsn1 (Germany), DE Nuremberg nbg1 (Germany), FI Helsinki hel1 (Finland)	Provide Customer's information Communication (any content of such communication) with the customer and/or within its chats	Inactive for 5 years

* *Inactive* means data subject has not interacted (opened, clicked, replied emails, answered phone calls, responded to text messages that we have sent them) since the last activity. From time to time, it may be necessary to retain or access historical personal data under certain circumstances such as if we have contractually agreed to do so or if we have become involved in unforeseen events like litigation or business disaster recoveries.

Destruction and Disposal

Upon expiry of our retention periods, we may delete confidential or sensitive records categorized as requiring high protection and very high protection, and we may either delete or anonymize less important documents.

Our Responsible person is responsible for the continuing process of identifying the records that have met their required retention period and supervising their destruction if needed. The destruction of confidential, financial and personnel-related records shall be securely destroyed electronically or by shredding if possible. Non-confidential record may be destroyed by recycling.