

# Privacy Policy

We fully recognize the importance of protecting personal information. We believe that properly processing personal information is part of our social responsibility and declare that we strive to protect personal information in accordance with the following principles (hereinafter “this Privacy Policy”). The definitions of terms other than those defined separately in this Privacy Policy shall be in accordance with the definitions in the Personal Data Protection Act (2023) and other related laws and regulations (hereinafter "Personal Data Protection Laws").

## 1. Our Company Profile

Please refer to Company > Corporate Profile on Sojitz Corporation corporate website.

## 2. Compliance with Laws and Regulations

We will strictly comply with Personal Data Protection Laws, guidelines, industry self-regulation rules, and internal rules, etc. when carrying out operations in which personal data is collected, processed, used, and/or transferred cross border.

## 3. Collection of Personal Information

We will collect personal data by fair and legitimate means. In addition, unless permitted by Personal Data Protection Laws, we will not collect any personal data defined and listed in Article 6 Paragraph 1 of the Personal Data Protection Act without the written prior consent of the individual (data subject) to whom such personal data pertains.

## 4. Process and Use of Personal Information

1. We will process and use personal data only for the purposes of use officially announced in advance or within the scope of use informed at the time of collection and to the extent necessary to carry out business.
2. We will not process and use personal data in a manner that may encourage or induce illegal or unlawful activities.

3. In the case where we share personal data with a third party, or entrust the processing of personal data to a third party, we will examine such third party rigorously, and perform proper supervision to ensure that such third party keeps the personal data confidential.

## 5. Provision of Personal Data to Third Parties

Except as provided by Personal Data Protection Laws, we will not provide personal data to any third party without the prior consent of the individual (data subject) to whom such personal data pertains.

## 6. Provision of Cross-Border Transfer of Personal Data

When we carry out a cross-border transfer of personal data, we will comply with the rules of Personal Data Protection Laws, and in principle, we will obtain the consent of the individual (data subject) in question after providing the information required by Personal Data Protection Laws in advance.

## 7. Sharing of Personal Data

We will share personal data as follows:

1. Personal Data Items  
The data subject's address, name, postal code, telephone number, fax number, email address, organization to which the person belongs, position in the organization, and other information included on the person's business card, as well as related data such as the date, time, and location of the business card exchange, etc.
2. Scope of Shared Users  
Sojitz Corporation and Sojitz Group companies\*  
\* Refers to affiliated enterprises as defined in Article 369-1 of the Company Act of 2021.  
Please refer to Company > Operating Bases and Company > Major Group Companies on Sojitz Corporation's corporate website.
3. Purpose of Use  
Personal data will be used for the purposes defined separately in the Purposes of Use of Personal Information.
4. Information about the Company Responsible for Managing the Personal Data  
We are responsible for the personal data that we share. For our address and representative, please refer to Company > Corporate Profile on Sojitz Corporation's corporate website.  
If you have any questions about the sharing of personal data, please contact the Personal Information Inquiry Desk listed separately.

## 8. Safety Management Measures for Personal Data

1. We will work to store and manage personal data in an accurate and up-to-date manner, and will take the necessary safety control measures to prevent unauthorized access or leakage of personal data.
2. We will take the following specific security management measures.
  1. Formulation of a Basic Policy and Maintenance of Discipline Regarding the Processing of Personal Data  
In order to ensure the proper processing of personal data, we will establish a basic policy that includes compliance with Personal Data Protection Laws and the creation of a point of contact for related questions and concerns.
  2. Organizational Safety Management Measures  
In addition to appointing a manager responsible for processing personal data, we will clarify the employees involved with processing personal data as well as the scope of the data, and we will establish a system for reporting and contacting the manager if evidence or indications of violations of Personal Data Protection Laws or internal rules is detected. In addition to regular self-inspections regarding the processing of personal data, we will undergo audits conducted by outside departments and third parties.
  3. Human Security Management Measures  
We will provide training to employees regarding precautions when processing of personal data. Articles concerning the confidentiality of personal data are included in the employee regulations.
  4. Physical Safety Management Measures  
In regions where personal data is processed, we place restrictions on employee access and on equipment that can be brought into the office. We will also implement measures to prevent unauthorized persons from viewing personal data. We will take measures to prevent the theft, leakage, loss, or any unlawful disclosure of equipment, electronic media, and documents, etc., and takes measures to ensure that personal data is not easily revealed when such devices or electronic media are transported, including within our premises.
5. Technical Safety Control Measures  
We will implement access restrictions in order to limit the scope of employee access to the personal information database, and of the database itself. We have implemented a system to protect information systems that process personal data from unauthorized outside access or harmful software.
6. Understanding the External Environment  
We have outsourced the storage of information, including some personal data, to a cloud services provider. The personal data is stored in the United States of America under the management of the said provider. We are implementing safety management measures based on our understanding of the personal information protection system in the United States of America,

based on information provided by the Personal Information Protection Commission of Japan, and based on the Personal Data Protection Laws of Taiwan etc.

## **9. Inquiry, Review, Copy, Supplement, Correction, Suspension of Collection, Processing, or Use, and Deletion of Personal Data**

We will promptly respond to requests from the data subjects of personal data for “inquiry”, “review”, “copy”, “supplement”, “correction”, “cessation or suspension of collection, processing, or use”, and “deletion”, etc. of their own personal data as well as to complaints and inquiries, in an appropriate manner and to a reasonable extent in accordance with Personal Data Protection Laws. Please contact the Personal Information Inquiry Desk listed separately.

## **10. Compliance Program for the Protection of Personal Data**

To execute this Privacy Policy, we have formulated a compliance program for the protection of personal data (which includes this Privacy Policy, Personal Data Protection Regulations and other regulations and rules) and keep our employees and other interested parties fully informed of this program, and execute and maintain this program, as well as strive to properly manage personal information through ongoing review and improvement.

■ Personal Information Inquiry Desk : [adm-tai@sojitz.com](mailto:adm-tai@sojitz.com)

## Purposes of Use of Personal Data

Sojitz Taiwan Corporation (“the Company”) will use the personal data that it acquires for the following purposes.

### 1. Personal Data of Business Partners

- Negotiations, communications, consultations, order acceptance and placement, settlement or other processing relating to business transactions
- Receipt of goods or services, etc. relating to business transactions
- Company business-related surveys, research, or analysis
- Provision of information relating to Company business (including information regarding prizes/rewards, promotional campaigns, and lectures/seminars)
- Response to inquiries or opinions submitted to the Company
- Appropriate and smooth performance of other operations of the Company

### 2. Personal Data of Shareholders

- Exercise of rights and performance of duties as shareholders pursuant to the Company Act and other laws and regulations
- Provision of privileges to, and performance of other measures with regard to, shareholders in the capacity of shareholders
- Management of shareholders, such as preparation of shareholders’ roster and other information based on the standards specified by laws and regulations
- Appropriate and smooth performance of other operations of the Company

### 3. Personal Information of Job Applicants Acquired during Hiring Activities

- Provision of information and communications relating to hiring by the Company, screening of job applicants and hiring decisions

- Provision of documents and communications for hiring procedures after a provisional decision is made

- Other labor management and smooth performance of the operations of the Company.

#### 4. Personal Data of the Company's Officers, Employees, Former Employees and their Family Members

- Work-related communications, exchanges of information, and compliance with rights and duties relating to labor laws and regulations, tax laws and regulations and social welfare laws and regulations, including human resource policies (including transfers, evaluations, and career development such as education), payment of wages, attendance management, benefits and so on

- Performance of various procedures specified by internal regulations

- Communications with, and the provision of information to, the Sojitz Employees Union, Sojitz Health Insurance Union, Health Care Room, Shareholding Association, Alumni Club and group companies

- Notification and reporting to government offices, their auxiliary organizations or other organizations to which the Company belongs

- Provision of social welfare benefit services, referrals concerning various types of group insurance and related procedures

- Distribution of internal publications and so on

- Communications during emergencies

- Other labor management and smooth performance of the operations of the Company

# 隱私權政策主頁

- 關於個人資料保護

- **隱私權政策**

我們深知保護個人資料的重要性，並將妥善處理個人資料視為我們的社會責任，特此聲明，我們將根據以下政策（下稱「本隱私權政策」）致力保護個人資料。此外，除於本隱私權政策另行定義的用語，其餘用語的定義，均依個人資料保護法（最新修正於 2023 年）及其他相關法令（下稱「個人資料保護相關法令」）的定義。

## 1. 本公司的名稱

請參閱本公司官方網站「企業情報」中的「[公司簡介](#)」。

## 2. 法律規範的遵守

我們在進行涉及個人資料的業務時，將遵守個人資料保護相關法令、相關指導原則、產業自律規範、公司內部規定等規定。

## 3. 個人資料的蒐集

我們將透過合法、公正的方式蒐集個人資料。另外，除個人資料保護相關法令允許的情況外，未事先徵得資料主體書面同意，我們不會蒐集其明定於個人資料保護法第 6 條第 1 項之個人資料。

## 4. 個人資料的處理、利用

我們僅在事先公告的個人資料利用目的或蒐集個人資料時告知之利用目的之範圍內，且僅在執行業務所必需的範圍內，處理、利用個人資料。

我們不會以鼓勵或誘使可能涉及違法行為的方式，處理及利用個人資料。

我們與第三方共享個人資料或委託第三方處理個人資料時，將對第三方進行嚴格審查，並實施適當監督，以確保該第三方對個人資料善盡保密義務。

## 5. 向第三方提供個人資料

除個人資料保護相關法令規定的情況外，未事先徵得當事人（即資料主體）同意，我們不會向第三方提供個人資料。

## 6. 國際傳輸個人資料

我們從事個人資料之國際傳輸時，將遵守個人資料保護相關法令的規定，原則上在事先向資料主體提供個人資料保護相關法令所要求的資訊後，徵得資料主體的同意。

## 7. 共享個人資料

我們將於以下情況共享個人資料：

#### 個人資料項目

資料主體之地址、姓名、郵遞區號、電話號碼、傳真號碼、電子信箱網址、所屬組織、在組織中的職位、其他名片記載資訊、交換名片的日期、時間、地點等相關資訊。

#### 個人資料利用者的共享範圍

台灣双日股份有限公司及双日集團旗下公司（\*）

（\*）依據公司法（最新修正於 2021 年）第 369 條之 1 第 1 條規定之「關係企業」。請參閱台灣双日股份有限公司官網「企業情報」中的「國內外營運據點」與「主要集團公司」。

#### 使用目的

本公司另行制定的「個人資料使用目的」所記載之目的

#### 負責管理個人資料的公司名稱

我們對共享的個人資料負責。有關本公司的地址和負責人，請參閱台灣双日股份有限公司官方網站「企業情報」中的「公司簡介」。

若您對於資料共享有任何疑問，請聯絡官方網站上揭示的「個人資料保護諮詢窗口」。

### 8. 個人資料的安全管理措施

我們將致力維護個人資料的正確性與最新狀態，並採取必要的安全管理措施，以防堵個人資料遭未經授權之進用或外洩。

我們將採取以下安全具體管理措施：

①制定基本政策並建立處理個人資料的紀律為確保妥善處理個人資料，我們制定了遵守個人資料保護相關法令的基本政策，並設置處理諮詢與申訴的窗口。

#### ②組織安全管理措施

我們除任命經理專責處理個人資料外，還明定處理個人資料的員工及其處理個人資料的範圍，並建立了通報制度，一旦發現違反個人資訊保護相關法令或公司章程的事實或跡象時，即可與經理取得連繫。

除定期對個人資料處理情況進行自我檢查外，我們還將接受其他外部部門或第三方的查核監督。

#### ③人員安全管理措施

我們為員工提供有關處理個人資料注意事項的培訓。

個人資料保密的條款已列入工作規則。

#### ④物理安全管理措施

在處理個人資料的區域，我們對人員的進出與攜入的設備進行控管，並採取措施，以防止未經授權人員查看個人資料。

我們採取措施，以防止處理個人資料之設備、電子媒體和文件等遭竊取、外洩、遺失或其他非法揭露，並確保這些設備或電子媒體等在移動過程中（包含公司處所內移動），不會輕易洩漏個人資料。

#### ⑤技術安全管理措施

我們實施存取限制，以限制負責人以及其所處理之個人資料資料庫的範圍。我們建立一套機制，以保護個人資料處理系統免遭外部非法入侵或惡意軟體攻擊。

#### ⑥掌握外部環境

我們已將包含部分個人資料的資訊儲存業務委託外包給雲端服務供應者，這些個人資料存放於美國，並由上述雲端服務供應者進行管理。我們根據對美國個人資料保護制度的理解、日本個人資料保護委員會提供的資訊及臺灣個人資料保護相關法令等，實施安全管理措施。

### 9. 資料主體就其個人資料所提出之關於查詢、請求閱覽、製給複製本、補充、更正、停止蒐集處理或利用、刪除等

資料主體就其個人資料提出之關於查詢、請求閱覽、製給複製本、補充、更正、停止蒐集處理或利用、刪除等的要求，我們將依據個人資料保護相關法令，於合理範圍內迅速做出適當的回應。請聯絡官方網站揭示的「[個人資料保護諮詢窗口](#)」。

### 10. 個人資料保護相關法規遵循制度體系

為執行本隱私權政策，我們制定了個人資料保護相關法規遵循制度體系（包含本隱私權政策、個人資料保護規章以及其他規章與規則），確保我們的員工和其他相關人員充分了解該政策以及執行和維護該政策，並透過持續檢視與改進，致力妥善管理個人資料。

■個人資料保護諮詢窗口：[adm-tai@sojitz.com](mailto:adm-tai@sojitz.com)

## 個人資料使用目的

台灣双日股份有限公司（下稱「本公司」）將出於以下目的使用所取得的個人資料。若有不清楚之處，請您聯繫「個人資料保護諮詢窗口」。

### 1. 業務合作夥伴的個人資料

- 與商業交易有關的談判、溝通、協商、接受訂單、結算或其他處理
- 與業務交易有關的商品或服務等的收受
- 與公司業務相關的調查、研究或分析

- 提供與公司業務相關的資訊（包括有關獎品/獎勵、促銷活動、講座/研討會的資訊）
- 對向本公司提出的詢問或意見的回應
- 公司其他業務的正常、順利進行

## 2、股東個人資料

- 依據公司法及其他法律法規行使股東權利及履行股東義務
- 基於股東身分，公司向股東提供特殊權益或其他優惠措施。
- 股東的管理，例如根據法律法規規定的標準準備股東名簿及相關資訊
- 公司其他業務的正常、順利進行

## 3. 招聘活動中獲得的求職者個人資料

- 提供與公司招聘、篩選求職者和招聘決定相關的資訊和通訊
- 錄取後，提供報到所需的文件和通訊資料
- 其他勞動管理及公司營運順利進行。

## 4. 公司高階主管、員工、前員工及其家庭成員的個人資料

- 與工作相關的溝通、資訊交流以及遵守有關勞動法律法規、稅收法律法規、社會福利法律法規的權利和義務，包括人力資源政策（包括調動、評估、教育等職業發展）、工資發放、考勤管理、福利等
- 履行內部規定規定的各種手續
- 與双日工會、双日健康保險工會、保健室、股東會、退休人員聯誼會、集團公司等等的聯繫及資訊提供
- 向政府機關及其附屬機關或本公司所屬的其他機關進行申報、報告
- 提供社會福利服務、各類團體保險的轉介及相關手續
- 內部刊物的分發等
- 緊急情況下的通信
- 其他勞動管理及公司營運順利進行