

## **CHOYOU PRIVACY AND DATA PROTECTION POLICY**

1. PURPOSE ..... 3

2. DEFINITIONS ..... 3

3. SCOPE..... 4

4. DATA PROTECTION PRINCIPLES ..... 4

5. TRANSFERS TO THIRD PARTIES ..... 5

6. SOURCES OF PERSONAL DATA ..... 5

7. DATA SUBJECT RIGHTS ..... 5

8. DATA RETENTION PERIOD ..... 5

9. INTRA-GROUP PROCESSING..... 6

10. THIRD PARTY PROCESSORS..... 6

11. WRITTEN CONTRACTS FOR THIRD PARTY PROCESSORS ..... 6

12. DATA SECURITY..... 6

## 1. PURPOSE

This Policy defines the requirements for compliance with the laws and regulations applicable to Choyou collection, use, processing and transfer of Personal Data throughout the world.

## 2. DEFINITIONS

**Consent:** means any freely given specific and informed indication of his/her wishes by which the Data Subject signifies agreement to Personal Data relating to him/her being processed.

Consent may be obtained by a number of methods. These may include click boxes on online forms in which Personal Data are entered.

**Data:** means information which:

- is being processed by means of equipment operating automatically in response to instructions given for that purpose; and/or
- is recorded with the intention that it should be processed by means of such equipment; and/or
- is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System; and/or
- does not fall within any of the above, but forms part of a readily accessible record covering an individual.

Data therefore includes any digital Data by computer or automated equipment, telephone recordings, and any manual information which is part of a Relevant Filing System.

**Data Controller:** means a person who (alone or with others) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed. Choyou will be the Data Controller in most cases.

**Data Exporter:** means the Data Controller or Data Processor who transfers the personal data abroad.

**Data Importer:** means the Data Controller or Data Processor who agrees to receive from the Data Exporter personal data for further processing in accordance with the terms of this Policy and the relevant Data Transfer Agreement.

**Data Processor:** means any person, other than an employee of the Data Controller, who processes the Data on behalf of the Data Controller. A company may be a Data Processor if defined as such in a contract with the Data Controller.

**Data Subject:** means the person to which Data refers. Data Subjects include clients and web users, individuals on contact /e-mailing lists or marketing databases, employees, contractors and suppliers.

**Personal Data:** means Data related to a living individual who can be identified from those Data or from those Data and other information in the possession of, or likely to come into the possession of, a Data Controller or Data Processor. Personal data does not include information that has been anonymized, encoded or otherwise stripped of its identifiers, or information that is publicly available, unless combined with other non-public personal information.

**Processing Data:** covers a wide variety of operations relating to Data, including obtaining, recording or holding the Data or carrying out any operation or set of operations on the Data, including:

- organisation, adaptation, or alteration;
- disclosure by transmission, dissemination, or otherwise; and
- alignment, combination, blocking, erasure, or destruction.

Any digital Database and/or organised manual files relating to identifiable living individuals fall within the scope of Data Protection laws and regulations, while a Database of pure statistical information (which cannot either directly or indirectly be related to any identifiable living individuals) will not.

**Technology :** includes any means of collecting or Processing Data, including, without limitation, computers and networks, telecommunications systems, video and audio recording devices, biometric devices, closed circuit television and the like.

### 3. SCOPE

- Choyou is committed to complying with the applicable Data Privacy and Protection requirements in the countries in which it operates.
- This policy is based on the General Data Protection Regulation (GDPR) within EU Regulation 2016/679 which provides a robust generic model for global Data Protection and privacy compliance.
- This Policy applies to ChoYou' full and part time employees, and all suppliers, prospects and partners who receive Personal Data from Choyou, have access to Personal Data collected or processed by ChoYou, or who provide information to EI- Technologies, regardless of geographic location.
- As a policy commitment Choyou will not process Personal Data without notification to the Data Protection authorities in any jurisdiction which requires such notification. To ensure compliance with the regulations Choyou will correctly establish its status for all Data Processing as either a Data Controller, or Data Processor acting for another Data Controller.

### 4. DATA PROTECTION PRINCIPLES

- Choyou has adopted the following principles to govern its use, collection, and transmittal of Personal Data, except as specifically provided by this Policy or as required by applicable laws:
- Personal Data shall only be processed fairly and lawfully;
- Personal Data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes;
- Choyou shall make reasonable efforts to ensure that Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or processed;
- Personal Data shall not be collected or processed unless one or more of the following apply:
  - The Data Subject has provided Consent;
  - Processing is reasonably necessary for the performance of a contract directly with the Data Subject, or to which the Data Subject is an employee of a party;

- Processing is necessary for compliance with an ChoYou legal obligation;
- Processing is necessary in order to protect the vital interests of the Data Subject;
- Processing is necessary for the legitimate interests of Choyou or by the third party or parties to whom the Data is disclosed, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject.
- Appropriate physical, technical, and procedural measures shall be taken to:
  - prevent and/or to identify unauthorised or unlawful Processing of Personal Data; and
  - prevent accidental loss or destruction of, or damage to, Personal Data.

## **5. TRANSFERS TO THIRD PARTIES**

- Personal Data shall not be transferred to another entity, country or territory, unless reasonable and appropriate steps have been taken to establish and maintain the required level of Data Security.
- All transfers of Personal Data to third parties for further Processing shall be Subject to written agreements.
- Subject to the provisions of the above, Personal Data may be transferred where any of the following apply:
  - The Data Subject has given Consent to the proposed transfer;
  - The transfer is necessary for the performance of a contract between the Data Subject (personally or via his employing company as an Choyou client) and Choyou;
  - The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between ChoYou and a Third Party;
  - The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise, or defence of legal claims;
  - The transfer is required by law;
  - The transfer is necessary in order to protect the vital interests of the Data Subject.

## **6. SOURCES OF PERSONAL DATA**

- Personal Data shall be collected only from the Data Subject unless the nature of the business purpose necessitates collection of the Data from other persons or bodies.
- If Personal Data are collected from someone other than the Data Subject, the entity collecting the Data must have confirmation, in writing, from the supplier of the Data that the Data Subject has provided Consent to the transfer to Choyou.

## **7. DATA SUBJECT RIGHTS**

- Data Subjects shall be entitled to obtain the information about their own Personal Data upon a request made in writing to Choyou.
- Data Subjects shall have the right to require Choyou to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

## **8. DATA RETENTION PERIOD**

- Personal Data must be kept only for the period necessary for permitted uses.

- Personal Data shall be deleted if their storage violates any Data Protection rules or if knowledge of the Data is no longer required by Choyou, or at the request of the Data Subject.

## **9. INTRA-GROUP PROCESSING**

- Where Choyou relies on another group company to assist in its Processing activities, it will enter into a Data Transfer Agreement based upon the EU Model Clauses with that other group company in order to ensure that responsibility for the data is clearly identified, as both parties may be considered as Data Controllers.
- The group companies involved in the Processing shall be known as a Data Exporter and a Data Importer respectively, although there may be more than one Data Importer involved in the Processing.

## **10. THIRD PARTY PROCESSORS**

Similarly where Choyou relies on third parties to assist in its Processing activities, Choyou will choose a Data Processor which provides sufficient security measures and take reasonable steps to ensure compliance with those measures.

## **11. WRITTEN CONTRACTS FOR THIRD PARTY PROCESSORS**

Choyou shall enter into a written contract with each Data Processor requiring it to comply with Data privacy and security requirements imposed on Choyou under local legislation.

## **12. DATA SECURITY**

- Choyou has a Data Security Management policy, under which it shall adopt physical, technical, and organisational measures to ensure the security of Personal Data, including the prevention of their alteration, loss, damage, unauthorised Processing or access, having regard to the nature of the Data, and the risks to which they are exposed by virtue of human action or the physical or natural environment. These measures will be documented within the Data Security Policy, which will be reviewed at least annually, or when necessary to reflect significant changes to security arrangements.
- Adequate security measures should include all of the following:
  - Prevention of unauthorised persons from gaining access to Data Processing systems in which Personal Data are processed.
  - Preventing persons entitled to use a Data Processing system from accessing Data beyond their needs and authorisations.
  - Taking all reasonable measures to ensure that Personal Data are protected against undesired destruction or loss.
  - Taking all reasonable measures to ensure that Data collected for different purposes can and will be processed separately.
  - Taking all reasonable measures to ensuring that Data are not kept longer than stipulated in the Data Retention Policy, including by requiring that Data transferred to third persons be returned or destroyed.