South Korea Privacy Policy

All personal information handled by ComPsych through its partner in South Korea, Dain Co., Ltd., (hereinafter, "The Company") is collected, held and processed based on the relevant statutes or with the consent of the data subject. The Company's privacy policy is based on the current Personal Information Protection Act (the "Act").

The Company will process personal information, which is collected, held and processed under the regulations of the Act, lawfully and fairly to protect the right and interest of data subject and perform the business appropriately.

The Company will also guarantee the users' rights related to personal information that the Company maintains, such as the right to access their personal information and right to claim the correction of personal information.

Users can request administrative judgment as provided in the Administrative Appeals Act for infringement of rights and interests under these statutes, and apply for dispute settlement or consultation with the Personal Information Dispute Settlement Committee and the Personal Information Violation Reporting Center.

Purpose of Processing Personal Information

The Company shall utilize the personal information collected for providing EAP services.

Personal Information Processing and Retention Period

The Company shall process and hold personal information to the extent that it is based on statutes or agreed upon by the data subject.

Provision of Personal Information to the Third Parties

The Company will not provide personal information that the Company collects and holds to third parties unless for the provision of services without the consent of users, except in the following situations:

1. Where special provisions exist in other laws;
2. Where it is deemed necessary explicitly for protecting, from impending danger, life, body or economic profits of the data subject or third party where the data subject or his/her legal representative is not in a position to express his/her intention, or prior consent cannot be obtained owing to unknown addresses;
3. Where personal information is provided in a manner keeping a specific individual unidentifiable necessarily for such purposes as compiling statistics or academic research.

In all other situations, prior to providing personal information to the third parties, the Company shall inform the data subject of the following matters and receive consent:

♦ Name (Corporation or Title of Organization) and contact of recipient;
♦ The purpose of use of personal information (where personal information is provided, it means the purpose of use by the recipient) and particulars of the personal information to be used or provided;
♦ The period for retaining and using personal information (where personal information is provided, it means the period for retention and use by the recipient);

♦ The fact that the data subject is entitled to deny consent, and disadvantage affected resultantly from the denial of consent

Right, Duty and Exercising Method of Data Subject

Users can exercise the following rights as the data subject:

1. Request for Accessing to Personal Information: Access to personal information that the Company maintains can be requested under the Article 35 (Access to Personal Information) of the Act.

Provided, in any of the following cases, the request may be limited or denied after the Company notifies a data subject of the cause under Clause 5, Article 35 of the Act:

● Where access is prohibited or limited by Acts;
● Where access may probably cause damage to the life or body of a third party, or improper violation of property and other benefits of a third party;
● Where a public institution has grave difficulties in providing the information.

2. Correction or Erasure of Personal Information: A data subject may request the correction and erasure of personal information the Company maintains under the Article 36 (Correction or Erasure of Personal Information) of the Act.

3. Suspension, etc. of Processing of Personal Information: A data subject may request the relevant personal information controller to suspend the processing of his/her personal information under the Article 37 (Suspension, etc. of Processing of Personal Information) of the Act.

The request for access, correction/erasure/suspension of processing of personal information will be responded to in accordance with the Act. The request for access, correction/erasure/suspending processing of personal information are available to through the charged division.

The rights exercised according to the above can be performed through the legal representative of the data subject or through the representative of the person who receives the delegation.

Processed Personal Information Items

The Company shall collect and retain the personal information only through the consent of the data subjects and the provisions of the statutes. The types of personal information collected and held by the Company in accordance with the provisions of the statutes may be as follows:

ID, name, company/position, e-mail, contact, date of birth, address, consultation details, supervisor, etc.

Destruction of Personal Information

The Company shall destroy personal information without delay when the personal information becomes unnecessary to the purpose of processing the personal information. Provided, this shall not apply where the retention of such personal information is mandatory under law.

The user's personal information shall be destroyed within five days from the date of the end of the personal information retention period, and within five days from the date when the personal

information is deemed unnecessary, such as achieving the purpose of processing the personal information.

Electronic file will be destroyed by permanently deletion in a way that cannot be restored.
Records, printed materials, written or otherwise recorded media other than the form of electronic files shall be destroyed by shredding or incinerating

Measures for Ensuring Safety of Personal Information

The Company has taken the following technical and physical measures necessary for ensuring safety, in compliance with Article 29 of the Act.

1. **Regular Self-inspection**: The Company has executed self-inspection regularly (once a quarter) to secure the safety of processing personal information.
2. **Minimizing and educating personnel authorized to handle personal information**: The number of personnel authorized to handle personal information has been minimized and regular educational programs have been implemented for such personnel.
3. **Formulating and implementing internal management plans**: The Company has formulated and implemented internal management plans in accordance with the guidelines for ensuring the safety of personal information.
4. **Technical measures against hacking:** The Company has installed security programs and updates and inspects the programs to protect personal information from being leaked externally or destroyed by hacking or computer viruses and has installed its systems in an area with restricted access to technically and physically monitor and block external access.
5. **Encryption of personal information:** Passwords and identification numbers, among each user's personal information, are encoded for storage and management. Furthermore, additional means, such as encrypting essential data for storage and transmission, are used for security.
6. **Preserving access records and preventing forgery and alteration of access records**: Log data about access to the personal information processing system are retained and managed for at least six months, and access records are maintained properly to prevent forgery, alteration, theft, and loss.
7. **Restrictions on access to personal information**: Access to personal information is controlled by granting, amending, or cancelling the authority to access the database system that processes personal information, and unauthorized external access is controlled by operating firewalls for blocking and preventing invasion and intrusion, while personnel authorized to handle personal information are precluded from accessing the personal information processing system externally via information and communications networks.
8. **Using a lock for document security:** Documents containing personal information and secondary storage are kept in a secure location with a lock.
9. **Restricting access by unauthorized persons:** The space for the physical storage of the personal information system that keeps personal information, is separated from other areas, and a procedure for controlling access to the space, has been established and is implemented.

Managers and Officers in Charge of Managing Personal Information

Civil Application Service on Personal Information

The Company shall designate the managers and officers in charge of managing personal information as follows to protect consumers' personal information and process the complaints related to the personal information:

Name of Information Protection Officer: HONG, YOUNG MIN, Director of Headquarters
Contact: 02-6272-9015
(It will be connected to the division in charge of managing personal information)

Name of Person in Charge of Protecting Personal Information: PARK, HYUN GI, Deputy Head of Department
Contact: 02-6272-9019
E-mail: basquiat16@daincnm.co.kr

You may report any complaints regarding personal information protection that arise from using the Company's service to the personal information management manager or the department in charge. The Company will quickly provide sufficient answers to the users' reports.
If you need to report or discuss other personal information breaches, please contact the organization below:

1. The Personal Information Dispute Mediation Committee (www.1336.or.kr/1336)
2. ePRIVACY Mark Committee (www.eprivacy.or.kr/02-580-0533~4)
3. The Cyber Crime Investigation Team of the Supreme Prosecutors' Office (http://icic.sppo.go.kr/02-3480-3600)
4. The Cyber Terrorism Response Center of the National Police Agency (www.ctrc.go.kr/02-392-0330)