PERSONAL DATA PROTECTION PROVISION

PART I. PERSONAL DATA PROCESSING OBLIGATIONS, PERSONAL DATA PROTECTION FAILURE, AND INDEMNITY

This provision in this document applies as an integral part of the Cooperation Agreement between the Parties.

All provisions and conditions set forth in Personal Data Protection Provision hereby apply and bind the Parties in connection to the collection, processing, disclosure, and/or transfer of data, including Personal Data, for the purpose of providing and using the Service, and seeking the opportunity of business cooperation between the Parties.

1. **Personal Data Processing Obligations of both Parties**
   a. The Parties agree to undertake and collaborate to fulfill all obligations of the applicable laws and regulations, including Personal Data Protection Laws, regarding the collection, processing, disclosure, and/or transfer of data, including Personal Data, for the purposes in accordance with Agreement.

   b. The Disclosing Party of Personal Data must:
      i. enter into supplemental data transfer terms with the Receiving Party, as may be required by the applicable laws and regulations, including Personal Data Protection Laws. In the event of any conflict between any such supplemental data transfer terms and Agreement, those supplemental data transfer terms shall prevail.

      ii. warrant and undertake that the data, including Personal Data, has been collected, processed, disclosed, and transferred to the receiving Party of Personal Data in accordance with the applicable laws and regulations, including Personal Data Protection Laws. If the disclosing Party of Personal Data breaches the provisions of this clause, such a Party shall be legally liable and shall release the receiving Party of Personal Data from liability for such negligence.

KETENTUAN TERKAIT PELINDUNGAN DATA PRIBADI

BAGIAN I. KEWAJIBAN PEMROSESAN DATA PRIBADI, KEGAGALAN PELINDUNGAN DATA PRIBADI, DAN JAMINAN

Ketentuan dalam dokumen ini berlaku sebagai bagian yang tidak terpisahkan dari Perjanjian Kerja Sama antara Para Pihak.

Seluruh ketentuan dan persyaratan yang diatur dalam Ketentuan Terkait Pelindungan Data Pribadi berikut ini berlaku dan mengikat bagi Para Pihak dalam kaitan terdapat pengumpulan, pemrosesan, pengungkapan dan/atau pemindahan data, termasuk Data Pribadi untuk tujuan pemberian dan penggunaan Layanan serta untuk penjajakan kerja sama bisnis di antara Para Pihak.

1. **Kewajiban Pemrosesan Data Pribadi Para Pihak**
   a. Para Pihak sepakat akan melaksanakan dan bekerjasama untuk memenuhi seluruh kewajiban peraturan perundang-undangan yang berlaku kepadanya, termasuk Hukum Pelindungan Data Pribadi sehubungan dengan pengumpulan, pemrosesan, pengungkapan dan/atau pemindahan data, termasuk Data Pribadi untuk tujuan sesuai dengan Perjanjian ini.
   b. Pemberi Data Pribadi wajib:
      i. menyepakati persyaratan pemindahan data tambahan dengan Penerima sebagaimana mungkin disyaratkan oleh peraturan perundang-undangan yang berlaku, termasuk Hukum Pelindungan Data Pribadi. Dalam hal terjadi pertentangan antara persyaratan pemindahan data tambahan tersebut dengan Perjanjian ini, maka persyaratan pemindahan data tambahan tersebut yang akan berlaku.
      ii. menjamin dan berjanji bahwa data, termasuk Data Pribadi telah dikumpulkan, diproses, diungkapkan dan dipindahkan kepada penerima Data Pribadi sesuai dengan peraturan perundang-undangan yang berlaku, termasuk Hukum Pelindungan Data Pribadi. Apabila pemberi Data Pribadi melanggar ketentuan ayat ini, maka Pemberi Data Pribadi wajib untuk bertanggung jawab secara hukum dan melepaskan tanggungjawab kepada

iii. take reasonable efforts to ensure that any of the to-be-transmitted Personal Data is accurate and complete as disclosed (as-is basis) and consented by the Data Subject before providing the Personal Data to the Receiving Party.

c. The Receiving Party of Personal Data must:
   i. warrant and undertake to maintain the confidentiality and security of any data, including Personal Data, obtained from the Disclosing Party by adhering to the applicable laws and regulations, including Personal Data Protection Laws, at all times when using and processing the Personal Data received from the Disclosing Party of Personal Data.

   ii. provide the Disclosing Party with such reasonable cooperation, information and assistance as required from time to time to enable the Disclosing Party to comply with its obligations under the applicable laws and regulations, including Personal Data Protection Laws.

   iii. not knowingly perform its obligations under Agreement in such a way as to cause the Disclosing Party to be in breach of any of its obligations under the applicable laws and regulations, including Personal Data Protection Laws.

   iv. not use the Personal Data for any purpose other than as necessary to fulfill the purpose of Agreement and shall not disclose the Personal Data to any third party without the prior written consent of the Disclosing Party, unless required by the applicable laws and regulations.

   v. remain fully liable to the Disclosing Party for:
      1) The Third Party's performance that is authorized by the Receiving Party to Access the Personal Data; and
      2) The costs and resources required for any additional monitoring or management of the Third Party.

Penerima Data Pribadi atas kelalaiannya tersebut.

iii. melakukan upaya yang wajar untuk memastikan bahwa Data Pribadi yang akan dikirimkannya akurat dan lengkap sesuai dengan yang diungkapkan dan selaras dengan persetujuan yang diberikan oleh Subjek Data sebelum mengirimkan Data Pribadi tersebut kepada Penerima Data Pribadi.

c. Penerima Data Pribadi wajib untuk:
   i. menjamin dan berjanji akan menjaga kerahasiaan dan keamanan setiap data, termasuk Data Pribadi yang diperoleh dari Pemberi Data Pribadi dengan cara mematuhi peraturan perundang- undangan yang berlaku, termasuk Hukum Pelindungan Data Pribadi, pada setiap saat ketika menggunakan dan memproses Data Pribadi yang diterima dari pemberi Data Pribadi.

   ii. bekerja sama secara wajar, untuk memberikan informasi dan bantuan yang diperlukan dari waktu ke waktu kepada Pemberi Data Pribadi untuk memungkinkan Pemberi Data Pribadi untuk memenuhi kewajibannya berdasarkan peraturan perundang-undangan yang berlaku, termasuk Hukum Pelindungan Data Pribadi.

   iii. tidak akan dengan sengaja melaksanakan kewajibannya berdasarkan Perjanjian ini sedemikian rupa sehingga menyebabkan Pemberi Data Pribadi melanggar kewajibannya berdasarkan peraturan perundang-undangan yang berlaku, termasuk Hukum Pelindungan Data Pribadi.

   iv. tidak akan menggunakan Data Pribadi untuk tujuan apa pun selain yang diperlukan untuk memenuhi tujuan Perjanjian ini dan tidak akan mengungkapkan Data Pribadi kepada pihak ketiga mana pun tanpa persetujuan tertulis sebelumnya dari Pemberi Data Pribadi, kecuali diminta oleh peraturan perundang-undangan yang berlaku.

   v. tetap sepenuhnya bertanggungjawab kepada Pemberi Data Pribadi untuk:
      i. Pelaksanaan kewajiban Pihak Ketiga yang diberikan wewenang oleh Penerima untuk Mengakses Data Pribadi; dan
      ii. Biaya dan sumber daya yang dibutuhkan untuk pemantauan atau manajemen tambahan dari Pihak Ketiga.

vi. identify to the Disclosing Party a contact point within its organization who is authorized to respond to enquiries concerning the processing of the Personal Data and will cooperate in good faith with the Disclosing Party, the Data Subject and the authorized government concerning all such enquiries within a reasonable time.

vii. implement reasonable technical, security and organizational measures to protect the Personal Data against unauthorized access, loss, destruction, alteration, and/or disclosure. For the purpose of Agreement, "technical, security and organizational measures" as referred to in this paragraph include the arrangements set out in this provision which shall not be varied without the Disclosing Party's prior written agreement.

viii. be able to provide evidence of said technical and organizational controls to the Disclosing Party in detail when required.

ix. have in place binding procedures and regulations so that any of its Representatives and/or Third Party authorized to Access the Personal Data from the Disclosing Party will respect and maintain the confidentiality, integrity, and security of such Personal Data.

x. In the event that the Receiving Party is a Processor or Sub Processor of Privy as the Data Controller, shall in accordance with the instructions of Privy, retain the Personal Data for a retention period of at least 5 (five) years for both electronic and non-electronic forms of Personal Data, and shall delete the Personal Data after the retention period has ended and/or in accordance with any applicable laws and regulations.

xi. upon any breach of any of provisions under Agreement by the Receiving Party, or upon the termination or expiry of Agreement, the Receiving Party shall, in accordance with the instructions of the Disclosing Party, either return (and cause to be returned) or destroy and erase (and cause to be destroyed and erased) any Personal Data provided by the Disclosing Party and provide a written confirmation (within thirty (30) days) to the

vi. mengidentifikasi narahubung dalam organisasinya kepada Pemberi Data Pribadi untuk menanggapi pertanyaan seputar pemrosesan dan penggunaan Data Pribadi dan akan bekerja sama dengan itikad baik bersama Pemberi Data Pribadi, Subjek Data, dan pemerintah yang berwenang mengenai pertanyaan tersebut dalam waktu yang wajar.

vii. menerapkan tindakan teknis, keamanan, dan organisasi yang wajar untuk melindungi Data Pribadi dari akses, kehilangan, penghancuran, perubahan, dan/atau pengungkapan yang tidak sah. Berdasarkan tujuan Perjanjian ini, "langkah-langkah teknis, keamanan, dan terorganisir" sebagaimana dimaksud dalam ayat ini termasuk pengaturan yang ditetapkan dalam ketentuan ini yang tidak akan berubah tanpa perjanjian tertulis sebelumnya dari Pemberi Data Pribadi.

viii. dapat menyediakan bukti kontrol teknis dan organisasi tersebut kepada Pemberi secara terperinci bila diperlukan.

ix. memiliki prosedur dan peraturan yang mengikat sehingga setiap Perwakilan dan/atau Pihak Ketiga yang diberikan wewenang untuk Mengakses Data Pribadi dari Pemberi Data Pribadi akan menghormati dan menjaga kerahasiaan, integritas, dan keamanan Data Pribadi tersebut.

x. dalam hal Penerima Data Pribadi adalah Prosesor atau Sub Prosesor dari Privy selaku Pengendali Data Pribadi, sesuai dengan instruksi dari Privy, menyimpan Data Pribadi selama masa retensi setidaknya 5 (lima) tahun untuk Data Pribadi dalam bentuk elektronik dan non-elektronik, serta menghapus Data Pribadi tersebut setelah masa retensi berakhir dan/atau sesuai dengan peraturan perundang-undangan yang berlaku.

xi. dalam hal adanya pelanggaran ketentuan manapun dalam Perjanjian ini atau setelah pengakhiran atau berakhirnya Perjanjian ini, sesuai dengan instruksi dari Pemberi Data Pribadi, baik mengembalikan (dan menyebabkan dikembalikan) atau menghancurkan dan menghapus (dan menyebabkan dihancurkan dan dihapus) setiap Pribadi Data yang diberikan oleh Pihak pemberi

Disclosing Party that it has returned or destroyed and erased (whichever applicable) all such Personal Data, provided that the Receiving Party may retain one (1) copy of such Personal Data if it is required to do so by any applicable laws and regulations. For the avoidance of doubt, the written confirmation as referred to in this Section includes the Minutes of Deletion as set out in this Agreement.

dan memberikan konfirmasi tertulis (dalam waktu tiga puluh (30) hari) kepada pihak pemberi bahwa pihaknya telah mengembalikan atau memusnahkan dan menghapus (mana saja yang berlaku) semua Data Pribadi tersebut, dengan ketentuan bahwa Penerima Data Pribadi dapat tetap menyimpan satu (1) salinan dari Data Pribadi jika diwajibkan oleh peraturan perundang-undangan yang berlaku. Untuk menghindari keraguraguan, konfirmasi tertulis sebagaimana dimaksud dalam Pasal ini meliputi Berita Acara Penghapusan yang ditetapkan dalam Perjanjian ini.

xii. cease to retain its documents containing the other party's Personal Data, or remove the means by which the other party's Personal Data can be associated with particular individuals as soon as it is reasonable to assume that:
   1) purpose is no longer being served by the retention of the Personal Data and;
   2) retention of the Personal Data is no longer necessary for any regulatory, legal, audit, or business purpose.

xii. berhenti menyimpan dokumennya yang berisi Data Pribadi pihak lain, atau menghapus cara yang dengannya Data Pribadi pihak lain dapat dikaitkan dengan individu tertentu segera setelah dianggap wajar bahwa:
   1) tujuannya adalah tidak lagi dilayani oleh penyimpanan Data Pribadi; dan
   2) penyimpanan Data Pribadi tidak lagi diperlukan untuk tujuan peraturan, hukum, audit, atau bisnis apa pun.

xiii. the Receiving Party is provided with anonymized Personal Data, the Receiving Party must not reverse-engineer, recreate, combine with any other dataset, or otherwise re-identify any Data Subject from the anonymized Personal Data.

xiii. jika Penerima Data Pribadi diberikan Data Pribadi yang dianonimkan, Penerima Data Pribadi tidak diperkenankan untuk merekayasa balik, membuat ulang, menggabungkan dengan kumpulan data lain, atau mengidentifikasi ulang setiap Subjek Data dari Data Pribadi yang dianonimkan tersebut.

2. Personal Data Protection Failure

a. The Parties agree to coordinate and cooperate in addressing and resolving/terminating the occurrence of the Failure of Personal Data Protection in accordance with their respective portions and responsibilities in the Failure of Personal Data Protection that has occurred.

b. In the event that either Party identifies indications of Failure of Personal Data Protection which affects Personal Data in relation to Agreement, said Party shall promptly notify the other Party upon discovery of such indications of the Protection Failure, or no later than 2x24 (twice twenty-four) hours from the moment the Party becomes aware of the occurrence of such indications of the Protection Failure.

2. Kegagalan Pelindungan Data Pribadi

a. Para Pihak sepakat untuk saling berkoordinasi dan bekerja sama untuk menangani dan menyelesaikan/menghentikan terjadinya Kegagalan Pelindungan Data Pribadi sesuai dengan porsi dan tanggung jawabnya masing-masing dalam Kegagalan Pelindungan Data Pribadi yang terjadi.

b. Apabila salah satu Pihak menemukan indikasi Kegagalan Pelindungan Data Pribadi yang mempengaruhi Data Pribadi sehubungan dengan Perjanjian ini, maka Pihak tersebut wajib memberitahukan kepada Pihak lainnya dengan segera sejak penemuan indikasi atas Kegagalan Pelindungan tersebut atau paling lambat 2x24 (dua kali dua puluh empat) jam sejak Pihak tersebut mengetahui terjadinya indikasi Kegagalan Pelindungan tersebut.

c. Notification stated in paragraph (a) above must contain at least:
   i. the impact of the Protection Failure, as well as the typology and amount of Personal Data affected by the Protection Failure;
   ii. when and how the Personal Data was impacted by the Protection Failure; and
   iv. efforts that have been and will be made in the context of handling and recovering from the Protection Failure.

d. The Party experiencing Protection Failure must limit the impact of the Protection Failure from spreading, at least by:
   i. cease the unauthorized access to the hacked Personal Data, systems, networks or applications;
   ii. isolate the hacked Personal Data, systems, networks, or applications;
   iii. take remedial action; and
   iv. take preventive action so that the Protection Failure Does not recur.

e. The Parties shall undertake actions required under the applicable laws and regulations, including relevant Personal Data Protection Laws, concerning the handling of the Failure of Personal Data Protection.

f. In the event of a Failure of Personal Data Protection, the grieving party has the right to make a temporary suspension of the implementation of the Purposes and request the breaching party to delete and/or destroy the Data that is provided by the grieving party to the breaching party to prevent further adverse effects.

g. In the event that the Failure of Personal Data Protection occurs due to failure, error, or negligence, whether intentional or unintentional, of either Party, said Party shall be fully liable for all consequences arising from the Failure of Personal Data Protection, including providing compensation to the affected parties (suffering losses due to being affected), such as, among others: the other Party, consumers, or affected users, in conformity with Article 3 of this provisions.

c. Pemberitahuan yang dimaksud pada paragraf (a) di atas wajib paling sedikit memuat:
   i. dampak dari Kegagalan Pelindungan, serta jenis dan jumlah Data Pribadi yang terdampak dari Kegagalan Pelindungan;
   iii. kapan dan bagaimana Data Pribadi terdampak oleh Kegagalan Pelindungan; dan
   ii. upaya yang telah dan akan dilakukan dalam rangka penanganan dan pemulihan atas Kegagalan Pelindungan.

d. Pihak yang mengalami Kegagalan Pelindungan wajib untuk membatasi dampak Kegagalan Pelindungan agar tidak meluas, paling sedikit dengan:
   i. menghentikan akses tidak sah ke Data Pribadi, sistem, jaringan, atau aplikasi yang diretas;
   ii. mengisolasi Data Pribadi, sistem, jaringan, atau aplikasi yang diretas;
   iii. melakukan tindakan pemulihan; dan
   iv. mengambil tindakan pencegahan agar Kegagalan Pelindungan tidak terjadi.

e. Para Pihak wajib untuk melakukan tindakan-tindakan yang diwajibkan berdasarkan peraturan perundang-undangan, termasuk Hukum Pelindungan Data Pribadi yang berlaku sebagaimana relevan terkait dengan penanganan Kegagalan Pelindungan Data Pribadi.

f. Dalam hal terjadi Kegagalan Pelindungan, pihak yang dirugikan berhak untuk melakukan penghentian sementara atas pelaksanaan Tujuan, dan meminta pihak yang melanggar untuk menghapus dan/atau memusnahkan Data yang disediakan oleh pihak yang dirugikan kepada pihak yang melanggar untuk mencegah dampak buruk lanjutan.

g. Apabila Kegagalan Pelindungan Data Pribadi terjadi karena kelalaian, kesalahan, atau kealpaan, baik disengaja atau tidak disengaja, dari salah satu Pihak, maka Pihak tersebut wajib bertanggung jawab penuh atas seluruh konsekuensi yang timbul dari Kegagalan Pelindungan Data Pribadi tersebut, termasuk memberikan ganti rugi kepada pihak-pihak yang terdampak (mengalami kerugian karena terdampak), seperti, antara lain: Pihak lainnya, konsumen, atau pengguna yang

h. The breaching Party of this Agremeent and/or Data Protection Laws shall, at its sole expense, indemnify, hold harmless and defend the grieving Party's personnel from and against all claims, suits, actions, losses, damages, settlements, penalties, fines, costs and expenses (including legal fees and costs on an indemnity basis) and liabilities, directly or indirectly, of any kind or nature arising from or in connection with any breach of the requirements herein by the breaching Party's personnel or any act, omission or negligence of the brieching Party's personnel that causes or results in the grieving Party being in breach of applicable Data Protection Laws.

3. Indemnity

Any breaching Party agrees to release and indemnify the non-breaching from and against any and all claims, suits, charges, settlement, penalties, fines, loss, expenses and/or liabilities, directly or indirectly, of any kind or nature, arising from or in connection with any breach of Agreement by the breaching Party, or any act, omission or negligence of the breaching Party's Representative that causes or results in the non-breaching Party being in breach of prevailing Data Protection Laws.

terdampak, sesuai dengan ketentuan dalam Pasal 3 ketentuan ini.

h. Pihak yang melanggar Perjanjian ini dan/atau Hukum Pelindungan Data harus, atas biayanya sendiri, mengganti rugi, membebaskan dan membela personel Pihak yang dirugikan dari dan terhadap semua klaim, gugatan, tindakan, kerugian, kerusakan, penyelesaian, hukuman, denda, biaya dan pengeluaran (termasuk biaya hukum dan biaya berdasarkan ganti rugi) dan kewajiban, secara langsung atau tidak langsung, dalam bentuk atau sifat apa pun yang timbul dari atau sehubungan dengan pelanggaran persyaratan di sini oleh personel Pihak yang melanggar atau setiap tindakan, kelalaian, atau kelalaian personel Pihak yang melanggar yang menyebabkan atau mengakibatkan Pihak yang dirugikan melanggar Hukum Pelindungan Data yang berlaku.

3. Jaminan

Setiap Pihak yang melanggar setuju untuk membebaskan dan mengganti kerugian Pihak yang tidak melanggar dari dan terhadap setiap dan seluruh klaim, tuntutan, kerugian, penyelesaian perselisihan, pinalti, denda, kerugian, biaya dan/atau tanggung jawab baik secara langsung atau tidak langsung, atau untuk setiap hal apapun, yang timbul dari atau terkait dengan pelanggaran atas Perjanjian ini yang dilakukan oleh Pihak yang melanggar atau setiap tindakan, pengabaian, kelalaian Perwakilan Pihak yang melanggar yang mengakibatkan dilanggarnya Hukum Pelindungan Data yang berlaku.

PART 2A. DESCRIPTION OF THE DATA PROCESSING

This Part and must be completed and signed by the Parties:

1. Purposes and Operations of the Processing

The Personal Data is transferred or disclosed by Disclosing Party to the Receiving Party for the purposes and the status of the Parties as set out in the Agreement.

Personal Data to be processed by the Receiving Party will be subject to the following processing activities:

a. acquisition and collection;
b. processing and analysis;
c. storage;
d. correction and updating;
e. appearance, announcement, transfer,
f. dissemination, or disclosure; and/or
g. deletion or destruction

2. Types of Personal Data

The Personal Data to be processed by the Receiving Party consist of the following types of Personal Data (Please note that the definitions of "General Personal Data" and "Specific/ Sensitive Personal Data" may refer to Parties' interpretation of any statutory classifications under applicable Personal Data Protection Laws):

General Personal Data

a. Full name;
b. National Identity Number;
c. Copy of ID Card and/or Supporting Documents (for Foreigner User);
d. Place and Date of Birth;
e. E-mail; and/or
f. Phone Number.

Specific/Sensitive Personal Data (if appropriate)

a. Biometric data.

3. Data Subjects

The Personal Data to be processed by the Receiving Party relate to the following categories of Data Subjects:

a. Privy users;
b. Individual acting as the person in charge of Merchant and Privy;
c. Privy's Director or Attorney in Fact, Commissioner; and/or

BAGIAN 2A. DESKRIPSI PENGOLAHAN DATA

Bagian ini wajib dilengkapi dan ditandatangani oleh Para Pihak:

1. Tujuan dan Kegiatan Pemrosesan

Data Pribadi dipindahkan atau diungkapkan oleh Pemberi kepada Penerima untuk tujuan dan berdasarkan status para pihak sebagaimana di atur pada Perjanjian.

Data Pribadi yang diproses oleh Penerima terbatas pada kegiatan pemrosesan sebagai berikut:

a. pemerolehan dan pengumpulan;
b. pengolahan dan penganalisisan;
c. penyimpanan;
d. perbaikan dan pembaruan;
e. penampilan, pengumuman, transfer,
f. penyebarluasan, atau pengungkapan; dan/ atau
g. penghapusan atau pemusnahan

2. Jenis Data Pribadi

Data Pribadi yang diproses oleh Penerima mengandung jenis Data Pribadi sebagai berikut (Harap perhatikan bahwa definisi "Data Pribadi Umum" dan "Data Pribadi Spesifik/Sensitif" dapat merujuk pada penafsiran Para Pihak atas klasifikasi menurut Hukum Pelindungan Data Pribadi yang berlaku):

Data Pribadi Umum

a. Nama lengkap;
b. Nomor Induk Kependudukan;
c. Salinan KTP dan/atau Dokumen Pendukung (untuk Pengguna WNA);
d. Tempat dan Tanggal Lahir;
e. Surel; dan/atau
f. Nomor HP.

Data Pribadi Spesifik/Sensitif (sebagaimana sesuai)

a. Data biometrik.

3. Subjek Data

Data Pribadi yang diproses oleh Penerima sehubungan dengan kategori Subjek Data sebagai berikut:

a. Pengguna Privy;
b. Individu yang bertindak sebagai narahubung dari Pelanggan dan Privy;
c. Direksi atau Kuasa Direksi, dan Komisaris Privy; dan/or

d. Merchant ’s Director or Attorney in Fact, and Commissioner.

4. Data Protection Officer Contact Information

If there is any inquiries and/or questions regarding Personal Data, the Merchant can contact Privy's contact person or Data Protection Officer with the following information:

Ardhitia Prawira R
Senior Legal Manager Data Privacy and Legal Commercial
dpo@privy.id

d. Direksi atau Kuasa Direksi, dan Komisaris Pelanggan.

4. Informasi Kontak Pejabat Pelindung Data Pribadi

Apabila terdapat keperluan dan/atau pertanyaan terkait Data Pribadi, Pelanggan dapat menghubungi narahubung atau DPO Privy dengan informasi sebagai berikut:

Ardhitia Prawira R
Senior Legal Manager Data Privacy and Legal Commercial
dpo @privy.id

PART 2B. MINIMUM STANDARD FOR TECHNICAL, SECURITY MEASURES

To ensure the confidentiality and security of the Personal Data during the reception, processing and use of the Personal Data for the Purpose set out in Agreement, the Parties agree that the Receiving Party must take reasonable technical, security and organizational measures with due observance of at least the following arrangements

1. Personal Data Access controls to ensure that Personal Data is not available to any unauthorized party other than any its Representatives and/or authorized Third Party under Agreement, and only to the extent necessary to enable such Representatives and/or Third Party to perform the Purpose in Agreement, including maintaining security, Access passwords and other means of Access, restricting unauthorized Access, modification or destruction of Data, physical and logical Access controls, multi-factor authentication and procedures for granting, reviewing, updating and revoking Access to systems, data and facilities. In particular, the Receiving Party should consider the following, namely:

a. <u>User Access Management:</u>

1) employ the authorised user access that controls the authentication to Personal Data Processing System(s).

2) has been reviewed periodically to ensure that users' access are appropriate for the authorised user.

b. <u>User Responsibilities:</u>

1) perform appropriate controls on the equipment that is not located in the safe area from unauthorized individuals.

2) use appropriate controls to protect such Personal Data contained in work areas, including but not limited to paper and and on display screens from unauthorized Access.

c. <u>Network Access Control:</u>

1) use standard network access controls.

2) not using Peer-to-Peer networking on Personal Data Processing System(s).

PART 2B. STANDAR MINIMUM UNTUK LANGKAH-LANGKAH TEKNIS KEAMANAN

Untuk menjamin kerahasiaan dan keamanan Data Pribadi selama penerimaan, pemrosesan dan penggunaan Data Pribadi untuk Tujuan yang ditetapkan dalam Perjanjian ini, Para Pihak sepakat bahwa Penerima harus mengambil langkah-langkah teknis, keamanan dan organisatoris yang wajar dengan memperhatikan sekurang-kurangnya pengaturan berikut ini:

1. Pengawasan terhadap Akses Data Pribadi untuk memastikan bahwa Data Pribadi tidak tersedia untuk pihak manapun yang tidak berwenang selain Perwakilan dan/atau Pihak Ketiga yang berwenang dalam Perjanjian ini, dan hanya sejauh yang diperlukan untuk memungkinkan Perwakilan dan/atau Pihak Ketiga tersebut memenuhi Tujuan dalam Perjanjian ini, termasuk menjaga keamanan, Akses kata sandi dan cara Akses lainnya, membatasi Akses tanpa izin dan pemberitahuan tanpa izin, perubahan atau penghapusan Data, kontrol Akses fisik dan logis dan prosedur untuk pemberian, peninjauan, pembaruan, dan pencabutan Akses ke sistem, data, dan fasilitas. Secara khusus, Penerima harus memperhatikan hal-hal berikut ini:

a. <u>Manajemen Akses Pengguna:</u>

1) menggunakan akses pengguna yang terotorisasi dengan kontrol otentikasi ke Sistem Pemrosesan Data Pribadi.
2) telah ditinjau secara berkala untuk memastikan bahwa hak akses tersebut sesuai untuk peran pengguna yang terotorisasi.

b. <u>Tanggung Jawab Pengguna:</u>

1) melakukan kontrol pada peralatan yang tidak berada pada area aman dari pihak yang tidak berwenang.
2) menggunakan kontrol yang sesuai untuk melindungi Data Pribadi yang terdapat di area kerja, termasuk namun tidak terbatas pada kertas dan layar tampilan dari Akses yang tidak sah.

c. <u>Kontrol Akses Jaringan:</u>

1) menggunakan kontrol akses jaringan standar.
2) tidak menggunakan jaringan Peer-to-Peer pada Sistem Pemrosesan Data Pribadi.

d. <u>Operating Systems Access Control:</u>

1) control Access to operating systems by use of access control procedure.

2) when technically possible, shut down inactive sessions after a defined period of time.

3) when technically possible, employ restrictions on connection times to high risk applications.

2. Secured channels to transfer and store Personal Data (such as secured file transfer protocol and encryption). In the case of Personal Data exchange, the Parties should consider the following, namely:

a. perform an inventory and risk assessment of all Personal Data exchange channels (including but not limited to SFTP, HTTPS, SMTP), and at a minimum for those Personal Data exchange channels used to transmit Personal Data and/or Confidential Information, with the purpose of identifying and mitigating risks to such Personal Data and/or Confidential Information from the use of these channels.

b. implement commercially reasonable effort to monitor the Personal Data exchange channels to detect unauthorized Personal Data releases.

c. use appropriate security controls and agreed upon Personal Data exchange channels when exchanging such Personal Data.

d. implement security measures in accordance with industry standards to protect Personal Data and/or Confidential Information, including using security protocols such as TLS (minimum of TLS 1.3 version), HTTPS, and SFTP, using trusted encryption algorithms such as AES-GCM, AES-CCM, RSA, ECDSA, and SHA-3, and/or transmit such Personal Data and/or Confidential Information through a secure network, either via the internet or wireless communication using mentioned security standards.

3. Safety and security procedures and safeguards that are no less rigorous than those safety and security procedures and safeguard maintain

d. <u>Kontrol Akses Sistem Operasi:</u>

1) mengontrol Akses ke sistem operasi dengan menggunakan prosedur pengendalian akses.

2) jika memungkinkan secara teknis, mematikan sesi tidak aktif setelah jangka waktu tertentu.

3) jika memungkinkan secara teknis, menerapkan pembatasan waktu koneksi ke aplikasi yang berisiko tinggi.

2. Jalur untuk memindahkan dan menyimpan Data Pribadi (seperti protokol keamanan pemindahan file dan enkripsi) yang aman. Dalam hal pertukaran Data Pribadi, Para Pihak harus memperhatikan hal-hal berikut ini, yaitu:

a. melakukan inventarisasi dan penilaian risiko atas semua saluran pertukaran Data Pribadi (termasuk namun tidak terbatas pada SFTP, HTTPS, SMTP), dan setidaknya untuk saluran pertukaran Data Pribadi yang digunakan untuk mengirimkan Data Pribadi dan/atau Informasi Rahasia, dengan tujuan untuk mengidentifikasi dan mengurangi risiko terhadap Data Pribadi dan/atau Informasi Rahasia tersebut dari penggunaan saluran-saluran ini.

b. menerapkan upaya yang wajar secara komersial untuk memantau saluran pertukaran Data Pribadi untuk mendeteksi pengungkapan Data Pribadi yang tidak sah.

c. menggunakan kontrol keamanan yang sesuai dan saluran pertukaran Data Pribadi yang disepakati saat bertukar Data Pribadi tersebut.

d. menerapkan langkah-langkah keamanan yang disesuaikan dengan standar industri untuk melindungi Data Pribadi dan/atau Informasi Rahasia, mencakup pemakaian protokol keamanan seperti TLS (minimal TLS versi 1.3), HTTPS, dan SFTP, menggunakan algoritma enkripsi yang disarankan seperti AES-GCM, AES-CCM, RSA, ECDSA, dan SHA-3, dan/atau mengirimkan Data Pribadi dan/atau Informasi Rahasia melalui jaringan dengan jalur aman, baik melalui internet maupun komunikasi nirkabel menggunakan standar keamanan tersebut.

3. Prosedur dan penjagaan keamanan yang tidak kurang dari standar prosedur dan penjagaan keamanan yang dilakukan dan dijaga oleh

by Merchant or Privy and vice versa in each of operations at the same time;

4. Compliance with industry best practices, standards and rules relating to security processes and controls of Personal Data. In relation thereto, the Receiving Party will establish, maintain and enforce, and periodically revise and improve its safety and security procedures and protections (including against the unauthorized use, destruction, loss or alteration of Personal Data in Receiving Party possession or control) that are consistent with current industry best practice from time to time; and

5. Implementation of technical and organizational controls around areas, such as:

   a. information security policies and procedures;
   b. human resource security;
   c. asset management;
   d. cryptography;
   e. physical and environmental security;
   f. operation security;
   g. communications security;
   h. system acquisition, development and maintenance;
   i. information security in supplier relationships.
   j. information security incident management;
   k. information security continuity and redundancies; and
   l. compliance with legal and contractual requirements.

Pelanggan maupun Privy dan sebaliknya dalam kegiatan operasionalnya pada saat yang sama;

4. Tunduk pada aturan, standar, dan aturan industri terkait dengan proses dan kontrol keamanan Data Pribadi. Sehubungan dengan itu, Penerima akan membangun, memelihara dan menjaga, serta secara bertahap melakukan perubahan dan meningkatkan prosedur keselamatan dan keamanan dan pelindungan (termasuk terhadap penggunaan, perusakan, kehilangan atau perubahan Data Pribadi yang tidak sah dalam kepemilikan atau kontrol Penerima) untuk mempertahankan keakuratan sesuai dengan standar terbaik dari waktu ke waktu; dan

5. Pelaksanaan teknis dan pengendalian pengorganisasian pada bidang-bidang, seperti:

   a. kebijakan dan informasi prosedur keamanan;
   b. keamanan sumber daya manusia;
   c. manajemen aset;
   d. kriptografi;
   e. keamanan fisik dan lingkungan;
   f. keamanan operasi;
   g. keamanan komunikasi;
   h. pengambilalihan sistem, pengembangan dan pemeliharaan;
   i. informasi keamanan dalam hubungan penyediaan;
   j. informasi pengaturan keamanan;
   k. informasi kelancaran dan kelebihan keamanan; dan
   l. tunduk pada hukum dan kontrak yang berlaku.

PART 3. MINUTES OF PERSONAL DATA DELETION AND EVIDENCE OF PERSONAL DATA DELETION BETWEEN THE PARTIES

After the Parties have deleted the Personal Data following the expiration of the retention period and/or in accordance with the applicable laws, the Party performing the deletion shall provide a Personal Data Deletion Report along with evidence of the Personal Data deletion to the other Party as proof that the deletion has been conducted in compliance with the applicable requirements, while considering at least the following provisions:

1. The Minutes of Personal Data Deletion shall at a minimum contain the following information:
   a. Details of the Cooperation Agreement serving as a reference (Agreement Number, Name, and Date);
   b. The Parties involved (Data Provider and/or Data Recipient) and the Type of Personal Data Exchange (Mutual or Unilateral);
   c. Details of Personal Data Storage (Shared Personal Data, Location of Personal Data Storage, Date of Personal Data Deletion, Name of the Responsible Party for Personal Data Deletion, and Reason for Personal Data Deletion); and
   d. Other evidence for before and after the deletion of Personal Data.

2. The format of the Minutes of Personal Data Deletion Report shall be further determined based on the mutual agreement of the Parties while adhering to the applicable laws.

BAGIAN 3. BERITA ACARA PENGHAPUSAN DATA PRIBADI DAN BUKTI PENGHAPUSAN DATA PRIBADI PARA PIHAK

Setelah Para Pihak melakukan penghapusan Data Pribadi setelah masa retensi berakhir dan/atau sesuai dengan peraturan perundang-undangan yang berlaku, Pihak yang melakukan penghapusan wajib memberikan Berita Acara Penghapusan Data Pribadi serta bukti penghapusan Data Pribadi kepada Pihak lainnya sebagai bukti bahwa penghapusan telah dilakukan sesuai ketentuan yang berlaku, dengan memperhatikan sekurang-kurangnya pengaturan berikut ini:

1. Berita Acara Penghapusan Data Pribadi sekurang-kurangnya harus memuat informasi mengenai:
   a. Detail Perjanjian Kerja Sama yang dijadikan rujukan (Nomor, Nama, dan Tanggal);
   b. Para Pihak (Pemberi dan/atau Penerima Data) serta Jenis Pertukaran Data Pribadi (Mutual atau Unilateral);
   c. Detail Penyimpanan Data Pribadi (Data Pribadi yang dibagikan, Tempat penyimpanan Data Pribadi, Tanggal penghapusan Data Pribadi, Nama penanggung jawab penghapusan Data Pribadi, Alasan penghapusan Data Pribadi); dan
   d. Bukti pendukung lainnya untuk menunjukkan sebelum dan setelah dilakukannya penghapusan Data Pribadi.
2. Format Berita Acara Penghapusan Data Pribadi akan ditentukan lebih lanjut berdasarkan kesepakatan Para Pihak dengan tetap mengacu pada peraturan perundang-undangan yang berlaku.